

A MITEL
PRODUCT
GUIDE

MiCollab Administrator Guide (MiCollab Server Manager Web Help)

Release 9.8

April 2024

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 Getting Started..... 1

1.1 About MiCollab..... 1
1.2 What's New in this Release..... 1
1.3 Logging In..... 1
1.4 About the Documentation Set..... 2
1.5 About the MiCollab Administrator Portal..... 4
1.6 Contacting Technical Support..... 5
1.7 Disclaimer, Trademarks, and Copyright..... 5
1.8 About the Users and Services Main Page..... 6
1.9 Using the Navigation/Search Bar..... 7
1.10 Displaying Data..... 9
1.11 Button Icons..... 10
1.12 About Help and Versions..... 12

2 Performing Administration Tasks..... 14

2.1 Configure the Server Settings..... 14
2.2 Administer the Applications..... 15
2.3 Maintain the Server..... 15
2.4 Assign Local Administrator User..... 15

3 About the Users and Services Application..... 17

3.1 View User Directory..... 17
3.2 Add or Edit Location Information..... 20
3.3 Add, Edit or Delete Department Information..... 20
3.4 Initial Users and Services Provisioning..... 22
3.5 About Hot Desk Users..... 24
3.6 View User Directory..... 26
3.7 Configure Service Information E-mail..... 28
3.8 Manage Unassigned Services..... 32
3.9 Delete Services..... 33
3.10 Configure MiCollab Language..... 35

4 About Network Elements..... 39

4.1 Add or Edit Network Elements..... 39
4.2 MiVoice Business Network Element Field Descriptions..... 43
4.3 System Management Tool Access..... 50
4.4 MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400 Network Element Field Descriptions..... 52

5 UCC Licensing..... 55

5.1 UCC License Bundle Definitions....64
5.2 Manage MiVoice Business Subscription Ed.02 Licensing Bundles....66

6 About Roles and Templates....72

6.1 Default Roles and Templates....72
6.2 Guidelines for Using Templates....76
6.3 Manage User Templates....77
6.4 Enter Template Information for UCC Licensing....80
6.5 Manage Roles....110
6.6 Apply Roles....112
6.7 Template Migration....112

7 Flow Through Provisioning - Description....113

7.1 Flow Through Provisioning - Conditions and Limitations....113
7.2 Flow Through Provisioning - Management Capabilities....117
7.3 Flow Through Provisioning - Summary of Behaviors....118
7.4 Flow Through Provisioning - Configuration....118
7.5 Flow Through - Maintenance....119
7.6 Flow Through Provisioning - Events and Alarms....123

8 Reconcile Wizard - Description....127

8.1 Reconcile Wizard - Conditions....129
8.2 How Entries are Paired....129
8.3 Reconcile Wizard - Welcome....132
8.4 Reconcile Wizard - Analyze Reconcile Operations....134
8.5 Reconcile Wizard - Non-Sharing Network Elements....134
8.6 Reconcile Wizard - Sharing Network Elements....136
8.7 Reconcile Wizard - MiCollab Phones to be Reviewed....137
8.8 Reconcile Wizard - Execute Reconcile....138
8.9 Reconcile Wizard - Manually Reconciling Operations....139
8.10 Reconcile Wizard - Configure MiCollab Network Element Settings....143
8.11 Reconcile Wizard - Troubleshooting....143

9 Reach Through - Description....144

9.1 Reach Through - Conditions....149
9.2 Reach Through - Configuration....149
9.3 Using Reach Through....155

10 About SDS Distribution Errors....156

10.1 Resolving Distribution Errors....158
10.2 Exporting Error Data....160
10.3 Viewing Data Distribution Alarms....161

11 About the Bulk User Provisioning Tool....162

11.1 Bulk Import from File....167
11.2 Auto Fill Selection....173
11.3 Add User Entries....176

11.4 Correcting Errors 177

12 View User Directory 179
12.1 Enter User Information 181
12.2 Quick Add 194
12.3 Delete Users 196
12.4 Send Service E-mail 197

13 Enter Phone Information 198
13.1 Enter Speech Auto Attendant Information 221
13.2 Configure Groups 222
13.3 Enter NuPoint UM Information 227
13.4 Enter MiCollab Client Information 238
13.5 Enter MiCollab Audio, Web and Video Conferencing Information 244
13.6 Enter MBG Information 247
13.7 Enter Vidyo Information 249
13.8 Enable Google Integration Features 251
13.9 Add External Numbers 252

14 About MiTeam Classic 254
14.1 MiTeam Classic Licensing 256
14.2 MiTeam Classic Configuration 257
14.3 Provision MiTeam Classic 260

15 About MiTeam Meetings 263
15.1 Provision MiTeam Meetings 263

16 Generate User Summary or MiTeam Classic Status Report 266
16.1 Generate Report of MiCollab Client Accounts 267

17 Deploy Mobile Client for Mobile 271
17.1 Deploy Mobile Client for EHDU 271
17.2 Deploy MiCollab MAC or PC Client (without Softphone) 272

18 Correcting Errors 274
18.1 Managing Detained and Failed IDS Operations 275
18.2 Unable to Delete a User's Extension 277
18.3 Unable to Add Phone After Deletion 277
18.4 Pop-up Error in Chrome 278

19 MiCollab Audio, Web and Video Conferencing Introduction 279
19.1 What's New in this Release 280
19.2 VMware View 280

20 Configuration Guidelines for Secure Conferencing..... 281

20.1 Web Conferencing Settings..... 282
20.2 Port Reservation Settings..... 283
20.3 System Options..... 285
20.4 LDAP Configuration..... 294
20.5 Voice Prompts..... 297
20.6 Country Tone Plan..... 299
20.7 Music-On-Hold Settings..... 300
20.8 Licensing..... 300
20.9 User Interface Wizard..... 301
20.10 Edit DAS Rules..... 302
20.11 Google Apps Integration for MiCollab Audio, Web and Video Conferencing..... 305
20.12 Google Gadget Configuration..... 308

21 MiVoice Business SIP Server Configuration..... 309

21.1 Configure MiVoice Business for MiCollab Audio, Web and Video Conferencing..... 310
21.2 MiVoice Office 250 SIP Server Configuration..... 312
21.3 MiVoice 5000 or MiVoice MX-ONE SIP Server Configuration..... 313
21.4 MiVoice Office 400 SIP Server Configuration..... 314

22 Recording Retention Settings.....316

23 Client Only Delivery.....317

24 Two-Way Audio Settings..... 318

25 Manage or Delete a User Profile.....331

25.1 Add User..... 333
25.2 Add Guest User..... 333
25.3 Administer User.....334
25.4 View Scheduled Conferences.....335
25.5 View Call Activity Report.....335
25.6 Schedule a Reservationless Conference.....335
25.7 Add a Delegate.....336
25.8 Support for Apostrophes.....337
25.9 List Users..... 337
25.10 Bulk Provision Users.....338
25.11 Bulk Provision Reservationless Conferences.....339
25.12 Default User Settings.....340
25.13 Broadcast Email..... 342
25.14 Billing Codes..... 342
25.15 Active Calls.....343
25.16 Proxy Extension Status.....347
25.17 Manage Published Data.....351
25.18 Manage Recordings..... 352
25.19 License Usage.....353

25.20 SIP Logs....353
25.21 Call Activity Reports....356
25.22 VoIP Utilization Statistics....357
25.23 Scheduled Conferences....357
25.24 System Alerts Log....357
25.25 Install History Log....358
25.26 Port Reservations Report....358
25.27 Downloading Web Sharing Logs....359

26 About NuPoint Unified Messaging (For on-premise deployments only)....362

26.1 About the NuPoint UM Documentation Suite....367
26.2 About this Help System....369
26.3 Searching the Online Help....369
26.4 What's New in This Release....372
26.5 Accessing Documentation, Release Notes, Articles, and Downloads....372
26.6 Searching the Online Help....373
26.7 Documentation Conventions....375
26.8 Contacting Technical Support....376
26.9 Overview....376
26.10 The Web Console....378
26.11 The Text Console....380
26.12 Console Capabilities....384
26.13 Frequently Used Procedures....387
26.14 Introduction....388
26.15 About Configuration....389
26.15.1 About Configuration....389
26.15.2 View Active Configuration....392
26.15.3 Duplicate the Active Configuration....392
26.15.4 Activate the Inactive Configuration....392
26.15.5 Duplicate the Active Configuration....393
26.15.6 Activate the Inactive Configuration....393
26.15.7 About Line Groups....394
26.15.8 About Dialing Plans....396
26.15.9 About Mailboxes....399
26.15.10 About Class of Service (COS)....402
26.15.11 Media Service....402
26.16 About Network Elements....403
26.16.1 Add a Network Element....403
26.16.2 Modify a Network Element....406
26.16.3 Delete a Network Element....407
26.16.4 Log In to a Remote Network Element....407
26.17 What is a Mailbox?....408
26.17.1 Types of Mailboxes in a Typical Installation....409
26.17.2 About Distribution Lists....426
26.17.3 About Names and Greetings....431
26.17.4 Unplayed Messages and Message Receipts....432
26.18 Mailbox Configuration Summary....432
26.18.1 Mailbox Names with Accented Characters....433
26.18.2 Configure an Overflow Mailbox....434
26.18.3 Configure a Broadcast Mailbox....434
26.18.4 Configure a Shared Extension Mailbox....436
26.18.5 Configure a Chain Mailbox....437
26.18.6 Implement a Tree Mailbox....437

26.18.7 Implement a Rotational Mailbox System..... 439
26.18.8 Passcode Expiry..... 442
26.18.9 Assign Alternate Extensions to a Single Mailbox..... 442
26.18.10 Unplayed Messages and Message Receipts..... 444
26.18.11 Message Waiting Types..... 444
26.19 Distribution List Configuration..... 445
26.19.1 Configure for Name and Greeting Broadcast..... 447
26.19.2 Allow Broadcasting to a Broadcast Mailbox..... 447
26.19.3 Nest a Distribution List or Prevent Nesting..... 448
26.19.4 Overview..... 448
26.19.5 Create a Master Distribution List by Phone..... 449
26.20 Record Company Greetings..... 450
26.20.1 Record an Alternate Company Greeting..... 451
26.20.2 Allow a Transfer Automatically After a Greeting..... 452
26.20.3 Configure for Name and Greeting Broadcast..... 452
26.20.4 Configure for a Receipt Notice or Summary..... 453
26.20.5 Record the Message of the Day..... 454
26.20.6 Enable or Disable a Message of the Day..... 455
26.20.7 Extended Absence Greetings..... 456
26.20.8 Record a Site Tutorial..... 457
26.21 Managing Mailboxes..... 458
26.21.1 Mailbox Parameters - Web Console..... 459
26.21.2 Search for a Mailbox..... 496
26.21.3 Add Mailboxes..... 499
26.21.4 Edit Mailboxes..... 501
26.21.5 Delete Mailboxes..... 502
26.21.6 Unlock Mailboxes..... 502
26.21.7 Set or Clear Mailbox Passcode or Tutorial..... 503
26.21.8 Set Passcode Expiry..... 503
26.21.9 Managing Distribution Lists..... 504
26.21.10 Import/Export a Distribution List..... 504
26.21.11 Set Languages for Prompts..... 506
26.22 Mailbox Parameters - Text Console..... 506
26.22.1 Create a Standard Mailbox..... 516
26.22.2 Define an Administrator Mailbox..... 522
26.22.3 Define an Attendant Mailbox..... 523
26.22.4 Modify or Delete Mailboxes..... 524
26.22.5 Find Mailbox Information..... 525
26.22.6 Configure a Rotational Mailbox..... 530
26.22.7 Set or Clear Mailbox Passcode or Tutorial..... 531
26.22.8 Set Passcode Expiry..... 531
26.22.9 Test Mailbox Capabilities..... 532
26.22.10 Configure a Mailbox for Distribution Lists..... 533
26.22.11 Create or Modify a List for Mailbox Owners..... 534
26.22.12 Delete a Distribution List..... 535
26.22.13 Delete a Member from All Distribution Lists..... 535
26.22.14 View All Lists Containing a Specified Member..... 536
26.22.15 View Members of a Single List..... 536
26.23 Schedule Company Greetings..... 536
26.23.1 Enable an Alternate Company Greeting..... 537
26.23.2 Copy a Mailbox Greeting..... 537
26.23.3 Select Languages for Prompts..... 538
26.23.4 Disabling a Message of the Day..... 539
26.24 Overview..... 539
26.24.1 Hotel/Motel Mailbox Structure..... 540
26.24.2 How the Hotel/Motel Application Works..... 541

26.24.3 Billing Guests....542
26.25 Overview....543
26.25.1 Default FCOS....543
26.25.2 Suggested Additional FCOS....563
26.25.3 Customizing FCOS....565
26.25.4 Managing FCOS....567
26.25.5 Customize Your FCOS....571
26.25.6 Assign an FCOS to a Mailbox....572
26.25.7 Add or Delete Feature Bits for an Existing FCOS....573
26.25.8 View FCOS Information....574
26.26 Feature Bits by Category - Overview....576
26.26.1 Category 1: Greeting Feature Bits....576
26.26.2 Category 2: Login Feature Bits....577
26.26.3 Category 3: Logout Feature Bits....579
26.26.4 Category 4: Attendant Call Feature Bits....580
26.26.5 Category 5: Outside Caller Feature Bits....580
26.26.6 Category 6: Prompts Feature Bits....582
26.26.7 Category 7: Receive Messages Feature Bits....584
26.26.8 Category 8: Play Messages Feature Bits....586
26.26.9 Category 9: Answer Message Feature Bits....588
26.26.10 Category 10: Keep or Discard Messages Feature Bits....589
26.26.11 Category 11: Make Messages Feature Bits....590
26.26.12 Category 12: Give Messages Feature Bits....591
26.26.13 Category 13: Message Addressing Feature Bits....593
26.26.14 Category 14: User Options Feature Bits....594
26.26.15 Category 15: User Distribution Lists Feature Bits....597
26.26.16 Category 16: Master Distribution Lists Feature Bits....598
26.26.17 Category 17: Check In/Check Out Feature Bits....598
26.26.18 Category 18: Super User Feature Bits....598
26.26.19 Category 19....600
26.26.20 Category 20: NuPoint Fax Feature Bits....600
26.26.21 Category 21: Paging and Message Delivery Feature Bits....603
26.26.22 Category 22: Email Feature Bits....604
26.26.23 Category 23: Network and NP Forms Feature Bits....605
26.26.24 Category 24: Web View (NP PWG) Feature Bits....606
26.26.25 Category 26: Short Message Service Feature....607
26.26.26 Category 27: NP Talk Features....608
26.26.27 Category 28: Dial-back and CLI Features....608
26.27 Feature Bits 001 to 049....609
26.27.1 Feature Bits 050 to 099....620
26.27.2 Feature Bits 100 to 149....632
26.27.3 Feature Bits 150 to 199....641
26.27.4 Feature Bits 200 to 249....651
26.27.5 Feature Bits 250 to 306....661
26.28 Other Classes of Service - Overview....668
26.28.1 Limits Class of Service - Overview....669
26.28.2 LCOS Parameters and Default Values (Web Console)....669
26.28.3 Create a New LCOS from a Copy....701
26.28.4 LCOS Parameters and Default Values (Text Console)....701
26.28.5 Assign an LCOS to a Mailbox....703
26.28.6 View LCOS Information....704
26.29 Group Class of Service - Overview....705
26.29.1 How a GCOS Works....706
26.29.2 One-Way Communication Using an Empty GCOS....712
26.29.3 Managing GCOS....713
26.29.4 Define a Bitmapped GCOS....715

26.29.5 Modify a Bitmapped GCOS Group....716
26.29.6 Assign a GCOS to a Mailbox....716
26.29.7 View GCOS Information....717
26.30 Restriction Class of Service - Overview....719
26.30.1 Managing RCOS....720
26.30.2 Configure an RCOS....723
26.30.3 Set RCOS System-Wide Parameters....724
26.30.4 Modify the Absorption Table....724
26.30.5 Modify the Exact Match Table....724
26.30.6 Modify NPA/NXX Tables....725
26.30.7 Assign an RCOS to a Mailbox....725
26.30.8 View RCOS Information....726
26.30.9 Sequence of NPA/NXX Screening....727
26.30.10 Screening Examples....728
26.30.11 RCOS Worksheet Configuration....729
26.30.12 Default FCOS....731
26.31 Managing TCOS....750
26.32 Description - NuPoint Voice Application....751
26.33 Default Configuration Settings....761
26.34 Dial-by-Name....763
26.35 Dial-Back....767
26.36 NuPoint Voice Application Programming - Task List....769
26.36.1 Add a Line Group....770
26.36.2 Edit a Line Group....778
26.36.3 Delete a Line Group....778
26.36.4 Application Parameters....779
26.37 Configure a Dialing Plan....793
26.38 Transfer to System Attendant....794
26.39 Prevent Unaddressed Messages....794
26.40 Enable the Dial by Name Function....795
26.41 Configure Media Service (Packet Rate)....796
26.42 Verify Configuration Parameters....796
26.43 Define a Line Group....796
26.43.1 Configure a Dialing Plan....798
26.43.2 Transfer to System Attendant....800
26.43.3 Prevent Unaddressed Messages....801
26.43.4 Enable Multiple Messages for Outside Callers....802
26.43.5 Enable the Dial-by-Name Function....803
26.43.6 Configure Media Service (Packet Rate)....804
26.43.7 Verify Configuration Parameters....805
26.44 Add Caller ID to Voice Mail Headers....806
26.45 Description....806
26.45.1 Configuration Requirements....812
26.45.2 Line Groups for Outdial Functions....818
26.45.3 Dial Strings for Outdials....819
26.45.4 Class of Service for Pager Mailboxes....825
26.45.5 COS for Message Delivery....828
26.45.6 COS for Call Placement....830
26.45.7 Mailboxes for Paging....831
26.45.8 Preparing for Mailbox Programming for Pagers....835
26.45.9 Allow Mailbox Owners to Control Paging/Message Delivery....839
26.45.10 Allow Receipt of Urgent Messages Only....839
26.45.11 Configure a Tone or Voice Pager....839
26.45.12 Configure a Display Pager....841
26.45.13 Paging Instructions for Users....842
26.45.14 Billing Considerations for Paging....844

26.45.15 Add, Edit or Delete a Pager System..... 846
26.45.16 Configure a Mailbox for Paging..... 847
26.45.17 Add an Alternate Pager to an Existing Mailbox..... 847
26.45.18 Set Pager Start and Stop Times..... 848
26.45.19 Turn Pagers/Message Delivery Off for a Mailbox..... 848
26.45.20 Enable Call Placement..... 848
26.45.21 Define a Pager System..... 849
26.45.22 Configure a Mailbox for Paging/Message Delivery..... 850
26.45.23 Setting Start and Stop Times..... 852
26.45.24 Change Paging Schedules or Intervals..... 853
26.45.25 Enable Cascade Paging..... 853
26.45.26 Turn Pagers/Message Delivery Off for a Mailbox..... 854
26.45.27 View Pager Configuration..... 854
26.45.28 Enable Call Placement..... 855
26.46 Testing Overview..... 857
26.46.1 Test Pager Configuration..... 858
26.46.2 Test Call Placement..... 860
26.46.3 Test Message Delivery..... 860
26.46.4 Testing Primary Pager Configuration..... 862
26.47 Configure External Applications..... 862
26.47.1 External Application (RS232) Programmable Application Parameters..... 863
26.48 Descriptions..... 866
26.48.1 Assign Message Waiting Type to a Mailbox..... 867
26.48.2 DTMF-to-PBX Configuration Requirements..... 868
26.48.3 DTMF to PBX MWI Configuration..... 873
26.48.4 Configure Message Cancel Timer..... 874
26.48.5 Turn off MWI for Skipped Messages..... 874
26.48.6 Set DTMF-to-PBX Protocols..... 874
26.48.7 Set DTMF-to-PBX Protocols..... 875
26.48.8 Compensate for Different Directory and Mailbox Numbers..... 878
26.48.9 Refresh or Suppress MWI..... 879
26.48.10 Test DTMF-to-PBX MWI Configuration..... 879
26.48.11 Test Message Waiting Indication (Text Console only)..... 880
26.49 MiVoice Business ICP Programming for MiTAI MWI..... 881
26.49.1 MiVoice Business ICP Programming for MiTAI MWI..... 882
26.49.2 Configure NuPoint UM for MiTAI MWI..... 884
26.50 Introduction..... 884
26.50.1 Defining an RS-232 Serial Port..... 885
26.50.2 Programmable RS-232 MWI Interface..... 886
26.50.3 Configure Programmable RS-232 MWI..... 888
26.50.4 Creating a Programmable RS-232 Interface String..... 889
26.50.5 Programming RS-232 MWI Using a Modem..... 891
26.50.6 Define a Serial Port..... 894
26.50.7 Configure Programmable RS-232 MWI..... 895
26.50.8 Creating a Programmable RS-232 Interface String..... 895
26.50.9 Setting Delay Times for Programmable RS-232 MWI..... 898
26.50.10 Enabling/Disabling Light-on Requests for Successive Messages..... 898
26.50.11 Sending the Number of Unplayed Messages..... 899
26.50.12 Assigning Additional Serial Ports for Programmable RS-232 Interface..... 899
26.50.13 Testing the RS-232 MWI Configuration..... 900
26.51 Worksheets Index..... 900
26.51.1 NuPoint Voice Worksheet..... 902
26.51.2 Mailbox Worksheets..... 903
26.51.3 Mailbox Individual Worksheet..... 904
26.51.4 Mailbox Group Worksheet..... 905
26.51.5 FCOS Worksheet..... 906

26.51.6 LCOS Worksheet..... 907
26.51.7 GCOS Worksheet..... 908
26.51.8 RCOS Worksheet..... 909
26.51.9 Billing Worksheet (1 of 2)..... 910
26.51.10 Billing Worksheet (2 of 2)..... 911
26.51.11 Outdial Line Group Worksheet..... 912
26.51.12 Rotational Mailbox Worksheet..... 913
26.51.13 Tree Mailbox Worksheet..... 914
26.51.14 DTMF-to-PBX Worksheet..... 915
26.51.15 RS-232 Message Waiting Lights Worksheet..... 916
26.51.16 Mailbox Worksheet Examples..... 917
26.51.17 Sample LCOS Worksheet..... 918
26.51.18 Sample GCOS Worksheet..... 919
26.51.19 Sample RCOS Worksheet..... 920
26.52 Overview..... 921
26.52.1 System Maintenance - Overview..... 921
26.52.2 Passcode Maintenance..... 921
26.52.3 Alarm Manager..... 922
26.52.4 Message Purge - Overview..... 926
26.52.5 Backup and Restore..... 927
26.52.6 Configuring the Microsoft Network Share for LAN Backups and Restores..... 929
26.52.7 System Shutdown..... 930
26.52.8 Auto Purge..... 931
26.52.9 Auto Backup..... 931
26.52.10 Backup Parameters..... 932
26.52.11 Perform System Shutdown and Startup..... 935
26.52.12 Fax Download Settings..... 936
26.52.13 Enable Alarm Management..... 936
26.52.14 Automatic Message Purge..... 938
26.52.15 Manual Message Purge..... 939
26.52.16 Perform a USB Backup..... 940
26.52.17 Configure the FTP Server for LAN Backups and Restores..... 941
26.52.18 Back up the LAN using FTP..... 943
26.52.19 Perform a LAN Backup using MS Networking..... 944
26.52.20 Configure Scheduled LAN Backups..... 946
26.52.21 Restore Data..... 948
26.53 Hard Disk Utilities..... 951
26.54 Change Text Console Password..... 953
26.55 Set System Time and Date..... 954
26.56 Lights Test..... 954
26.57 Enable Alarm Management..... 955
26.58 Perform System Shutdown and Startup..... 957
26.59 Adjust Audio Stream..... 958
26.60 Security - Overview..... 958
26.60.1 Protection From Outside Abuse..... 959
26.60.2 Protection From Mailbox Owner Abuse..... 961
26.60.3 Security for System Administration..... 962
26.60.4 Security Reports and Audit Trails..... 965
26.60.5 Configure Mailbox Passcode Parameters by FCOS..... 966
26.60.6 Restrict Line Group Access..... 966
26.61 List of Current Users..... 967
26.61.1 Start an Audit Trail..... 967
26.61.2 Export an Audit Trail..... 968
26.61.3 Generate an Audit Trail Report..... 969
26.62 List of Authorized Users..... 970
26.62.1 Configure Mailbox Passcode Parameters by Line Group..... 970

26.62.2 Prevent Multiple Message In an Answering Session....971
26.62.3 Set Site Name, Site Banner, or Site Code....971
26.63 Start or Stop an Audit Trail....972
26.63.1 Format an Audit Trail Report....973
26.63.2 Generate an Audit Trail Report....974
26.64 Functionally Partitioned System Administration....974
26.64.1 Configure FPSA Password Parameters....978
26.64.2 Log In or Log Out of the Text Console....978
26.64.3 Add, Delete, Lock, or Unlock a User ID....979
26.64.4 Modify Permission Categories for Current User IDs....982
26.64.5 Reset a Password....982
26.64.6 Configure FPSA Password Parameters....983
26.64.7 Add, Delete, or Unlock a User ID....983
26.64.8 Modify Permission Categories for Current User IDs....985
26.64.9 Reset a Password....986
26.64.10 List of Authorized Users....986
26.65 Log In or Log Out of the Web Console....987
26.66 **Change a Password**....988
26.67 Change Text Console Password....988
26.68 Display Administrator Privileges....989
26.69 Overview....990
26.69.1 Configuration Requirements for Billing....990
26.69.2 Set Billing Rates....998
26.69.3 About Resource Counters....999
26.70 Gathering Data....1003
26.70.1 Perform a Manual Gather....1003
26.70.2 Configure an Automatic Gather....1004
26.70.3 Set Billing Rates....1004
26.70.4 Billing Gather Form....1004
26.70.5 Billing Rates Form....1006
26.71 Check Current Billing Rates....1013
26.71.1 Perform a Gather....1015
26.71.2 Auto Gather....1016
26.71.3 Set Base Rates....1017
26.71.4 Set Billing Rates for Connect Time....1018
26.71.5 Set Billing Rates for Messages Received....1018
26.71.6 Set Billing Rates for Mailbox Accesses....1019
26.71.7 Set Billing Rates for Pager Calls or Message Delivery....1019
26.71.8 Set Billing Rates for Disk Usage....1019
26.71.9 Set Billing Rates for Network Usage....1020
26.71.10 Bill Outdials to an Account or Long Distance Carrier....1021
26.72 Overview....1022
26.72.1 View System Information....1023
26.72.2 Configuration Report....1023
26.72.3 Call Director Database Report....1025
26.72.4 Feature Class of Service (FCOS) Report....1027
26.72.5 Group Class of Service (GCOS) Report....1029
26.72.6 Limits Class of Service (LCOS) Report....1031
26.72.7 Log File Report....1032
26.72.8 Mailbox Data Report....1035
26.72.9 Network Class of Service (NCOS) Report....1037
26.72.10 NP Receptionist Treatments Report....1038
26.72.11 Pager Access Codes Report....1041
26.72.12 Phonebook Report....1042
26.72.13 Pre-extension Dial Strings Report....1043
26.72.14 Show or Edit the History File....1044

26.72.15 System Information Report..... 1045
26.73 Overview - Statistics Reporting..... 1047
26.73.1 Run a Line Usage Report..... 1048
26.73.2 Run a Line Group Usage Report..... 1049
26.73.3 Run a Speech Block Usage Report..... 1050
26.73.4 Line Group Usage Report – All Trunks Busy Statistics..... 1051
26.73.5 Line Group Usage–Line–Statistics Report..... 1056
26.73.6 Line Usage Statistics Report..... 1059
26.73.7 Mailbox Statistics Reports..... 1062
26.73.8 Message Counts Usage Statistics Report..... 1067
26.73.9 Speech Blocks Usage Statistics Report..... 1070
26.73.10 Complete Summary Report..... 1073
26.73.11 Total System Statistics Report..... 1076
26.73.12 Virtual Drive Statistics Report..... 1077
26.73.13 Network Usage Statistics Report..... 1080
26.74 Overview - Billing Reports..... 1082
26.74.1 About Billing Reports..... 1083
26.74.2 Run a Billing Report..... 1083
26.74.3 Run the Billing Report..... 1084
26.74.4 Mailbox Blocked Report (Blocked Billing Report)..... 1086
26.74.5 Previous Billing Report..... 1087
26.75 Overview..... 1088
26.75.1 Access the Telephone Administration Menu..... 1088
26.75.2 Add a New Mailbox by Phone..... 1090
26.75.3 Delete a Mailbox by Phone..... 1091
26.75.4 Modify A Mailbox by Phone..... 1091
26.75.5 Change/Reset Mailbox Passcode or Enable/Disable Tutorial by Phone..... 1092
26.75.6 Set the System Date and Time..... 1092
26.75.7 Enable an Alternate Company Greeting..... 1093
26.75.8 Report System Usage Statistics by Phone..... 1093
26.75.9 Inquire About Mailboxes by Phone..... 1094
26.76 Overview..... 1094
26.76.1 DID Mailboxes..... 1095
26.76.2 The Message Attendant Application..... 1096
26.76.3 TAS Operator Procedures..... 1096
26.77 Installing an Optional Feature..... 1098
26.78 Direct Drop Overview..... 1099
26.79 About Call Detail Recorder..... 1101
26.79.1 CDR Disk Storage..... 1110
26.79.2 Line Numbers..... 1117
26.79.3 Configure CDR..... 1118
26.79.4 Starting and Stopping CDR..... 1119
26.79.5 Delete Existing CDR Records..... 1119
26.79.6 CDR Reports..... 1120
26.79.7 Set CDR Report Options..... 1125
26.79.8 Create CDR Report..... 1127
26.79.9 Run a Call Detail Record Report..... 1127
26.79.10 Interpreting Your Results..... 1129
26.80 Processing Each Call Type..... 1132
26.81 Hacker Detection..... 1144
26.82 Description..... 1144
26.82.1 Call Director - Configuration..... 1145
26.82.2 Call Director - Operation..... 1146
26.83 Competitive TUI Emulation - Description..... 1147
26.83.1 Competitive TUI Emulation - Configuration..... 1148
26.83.2 Competitive TUI Emulation - Operation..... 1148

26.84 Cut-Through Paging - Description..... 1149
26.84.1 Cut-Through Paging - Configuration..... 1150
26.84.2 Cut-Through Paging - Operation..... 1151
26.85 Overview - Language Prompts..... 1156
26.85.1 Activate Language Prompts..... 1158
26.85.2 Activate Language Prompts for Tenant Groups..... 1161
26.86 Overview..... 1162
26.86.1 About NuPoint UM Fax Applications..... 1163
26.86.2 Fax Scenarios..... 1165
26.86.3 NP Fax - Conditions..... 1170
26.87 Overview..... 1171
26.87.1 Fax Class of Service Parameters..... 1171
26.87.2 Adding NP Fax Options to COS..... 1179
26.87.3 Planning Fax Mailboxes..... 1183
26.87.4 Planning Outside Caller Access..... 1195
26.88 Overview..... 1199
26.88.1 Configuring Fax Applications..... 1200
26.88.2 Configuring Fax Applications..... 1203
26.88.3 Set Up a Fax Cover Page..... 1204
26.88.4 Viewing Fax Messages..... 1205
26.88.5 Managing Fax Groups..... 1206
26.88.6 Define a Fax Group..... 1208
26.88.7 Assign Fax Group to Line Group..... 1209
26.88.8 Set Limits for NuPoint Fax..... 1209
26.88.9 Configure a Mailbox for NuPoint Fax..... 1210
26.89 Introduction..... 1211
26.89.1 Billing Parameters..... 1212
26.89.2 Set Billing Rates for Fax..... 1214
26.89.3 Fax Statistics..... 1214
26.89.4 About the **Fax Group Usage Report**..... 1214
26.89.5 Run a Fax Group Usage Report..... 1216
26.89.6 Run a Fax Group Usage Report..... 1216
26.89.7 Troubleshooting..... 1217
26.90 Description..... 1218
26.90.1 Inside an NP Forms Application..... 1219
26.90.2 Playback and Transcription..... 1220
26.90.3 NP Forms Mailbox Interaction..... 1220
26.90.4 Tree Mailboxes and NP Forms..... 1221
26.90.5 NP Forms FCOS Configuration..... 1221
26.90.6 Configure an NP Forms Template Mailbox..... 1222
26.90.7 Create an NP Forms Application..... 1223
26.90.8 Configure a Rotational Mailbox for NP Forms..... 1223
26.90.9 Worksheet Index..... 1224
26.90.10 FCOS Worksheet..... 1225
26.90.11 NP Forms Diagram..... 1226
26.91 Introduction..... 1227
26.91.1 Configuration Task List..... 1229
26.91.2 NP Net TCP/IP Overview..... 1229
26.91.3 NP Net - Terms and Concepts..... 1230
26.91.4 Message Flow Through an NP Net Network..... 1231
26.91.5 Overview of NP Net Installation and Configuration Tasks..... 1234
26.92 About NP Net TCP/IP..... 1234
26.92.1 Configuring TCP/IP..... 1235
26.92.2 Configuring TCP/IP..... 1236
26.93 Network Node Table - Introduction..... 1237
26.93.1 Network Node Table Configuration Worksheet..... 1237

26.93.2 Create or Modify a Network Node Table Entry....1238
26.93.3 Delete a Network Node Table Entry....1240
26.93.4 View the Network Node Table....1240
26.94 Configuring Network Addressing - Overview....1241
26.94.1 Planning Network Addressing....1243
26.94.2 The Digits Translation Table....1244
26.94.3 Creating a Network Dialing Plan....1248
26.94.4 Using Broadcast Mailboxes for Transparent Network Messaging....1250
26.94.5 Network Addressing Examples....1252
26.94.6 Create New Prefix/Node Pairs....1254
26.94.7 Delete Prefix/Node Pairs....1255
26.94.8 View the Digits Translation Table....1255
26.94.9 Modify the Node Number for a Prefix....1256
26.94.10 Configuring the Network Queues - Overview....1256
26.94.11 Network Queues Worksheet....1257
26.94.12 Configure Network Queues....1261
26.94.13 Managing NCOS....1263
26.94.14 Configure a Network Class of Service....1265
26.95 Configuring Network Mailboxes....1266
26.95.1 Network Billing....1267
26.95.2 NP Net Reports....1271
26.95.3 Network Statistics Reports....1275
26.95.4 Worksheets - NP Net....1279
26.95.5 Network Addressing Planning Worksheet....1280
26.95.6 Network Queues Worksheet....1281
26.95.7 Network Class of Service Worksheet....1285
26.96 NP OnDemand - Description....1286
26.96.1 NP OnDemand - System Requirements....1286
26.96.2 Billing and Statistics....1287
26.96.3 Configure Call Detail Recorder for NP OnDemand....1287
26.96.4 NP OnDemand - Configuration Requirements....1288
26.96.5 Create a Template Mailbox....1290
26.97 NP RapidDial - Description....1292
26.97.1 Configuration Requirements NP RapidDial....1292
26.97.2 Create the NP RapidDial Table - Overview....1293
26.97.3 (A) Add New Records....1294
26.97.4 (C) Clear NP RapidDial Table....1295
26.97.5 (D) Delete existing record(s)....1296
26.97.6 (E) Export NP RapidDial Table....1297
26.97.7 (I) Import NP RapidDial Table....1297
26.97.8 (P) Purge Subscriber Group....1299
26.97.9 (R) Report on all Subscriber Groups....1299
26.97.10 (V) View Subscriber Group....1300
26.97.11 Configure Mailboxes for NP RapidDial....1300
26.98 NP Receptionist - Description....1300
26.98.1 NP Receptionist Features....1301
26.98.2 Call Flow and Call Processing....1303
26.98.3 NP Receptionist Configuration Overview....1305
26.99 Dialing Plan Options....1305
26.100 Flow Options....1310
26.101 PBX Dial String Definitions....1310
26.102 What is a Treatment Type?....1313
26.102.1 Extension Treatment Types....1313
26.102.2 Trunk Treatment Types....1316
26.102.3 Hidden (’Blind’) Mailbox Extension Number Programming....1316
26.102.4 Programming NP Receptionist to Dial an Outside Mailbox Extension Number....1317

26.102.5 Programming an Outside Attendant’s Extension Number 1319
26.102.6 Attendant's Dialing Sequence 1321
26.103 About NP Receptionist Worksheets 1321
26.103.1 NP Receptionist Worksheets 1323
26.103.2 NP Receptionist Configuration 1327
26.103.3 NuPoint Voice Configuration 1329
26.103.4 Create a Single-Digit Access Menu 1331
26.103.5 Set Up NP Receptionist Test Configuration 1332
26.103.6 Test Mailbox Treatment Types 1333
26.103.7 Test Intermediate Attendant Call Processing 1335
26.103.8 Test the NP Receptionist Setup 1336
26.103.9 Add NP Receptionist Extensions 1338
26.104 NP WakeUp - Description 1339
26.104.1 NP WakeUp - Description 1339
26.105 NP WakeUp - User Interface 1340
26.106 Call Records 1341
26.107 Overview of PMS Integrations 1341
26.107.1 Installation Using a Physical Serial Port 1342
26.107.2 To Restore NuPoint UM PPP Service 1343
26.107.3 Serial Port Settings 1343
26.107.4 Configure IP Connectivity 1344
26.107.5 Installation Using a Serial-to-IP Converter 1345
26.107.6 Install and Configure the Precidia iPocket232 1345
26.107.7 Configuration for PMS Integrations 1347
26.108 EECO Troubleshooting Guide 1349
26.108.1 HIS Troubleshooting Guide 1350
26.108.2 Hyatt Encore Configuration and Troubleshooting 1351
26.108.3 Marriott Troubleshooting Guide 1355
26.108.4 Reconnecting PMS to NuPoint 1364
26.108.5 Appendix - Diagnostic Specification 1364
26.109 Description 1383
26.109.1 Conditions 1383
26.109.2 Configuration 1385
26.109.3 Recorded Announcement Device (RAD) 1386
26.109.4 Softkeys - Description 1387
26.109.5 Softkeys - Conditions 1387
26.109.6 Configuring Softkeys on a MiVoice Business ICP System 1387
26.110 SMS Notification (UK Only) - Description 1388
26.110.1 Configure SMS 1388
26.110.2 External Application (RS232) Programmable Application Parameters 1389
26.110.3 Speech Auto Attendant - Description 1393
26.110.4 Speech Auto Attendant Users 1396
26.110.5 Speech Auto Attendant Features 1398
26.110.6 Speech Auto Attendant Installation 1401
26.110.7 Configuration Overview 1403
26.110.8 Planning and Licensing 1404
26.110.9 Mailbox Names and SAA Recognition 1407
26.110.10 Configure a Speech Recognition Line Group 1409
26.110.11 About User Data Source 1410
26.110.12 Define a NuPoint User Data Source 1411
26.110.13 Define an Active Directory User Data Source 1411
26.110.14 Define a MiCollab User Data Source 1412
26.110.15 Modify the User Data Source 1413
26.110.16 Update the User Data Source 1413
26.111 About Current Users 1414
26.111.1 Find Current Users 1415

26.111.2 Export Current Users....1415
26.112 About Departments....1416
26.112.1 Add a Department....1416
26.112.2 Edit a Department....1417
26.112.3 Delete a Department....1417
26.113 About Prompts....1418
26.113.1 Prompt Languages....1418
26.113.2 Record a Prompt....1419
26.113.3 Import a Prompt....1420
26.113.4 Play a Prompt....1421
26.113.5 Silence a Prompt....1421
26.114 About Dialing Policies....1422
26.115 About Miscellaneous Parameters....1426
26.115.1 Basic Speech Recognition Parameters....1426
26.115.2 Confidence Thresholds....1428
26.115.3 Dialing Policy Parameters....1429
26.115.4 User Data Source Schedule Parameters....1430
26.115.5 Presence Feature Parameters....1430
26.115.6 Administration Parameters....1431
26.116 Custom Pronunciations....1431
26.117 Troubleshooting SAA Name Recognition Problems....1433
26.118 Install Active Directory (AD) Snap-in....1434
26.119 Presence Overview....1436
26.119.1 Presence Installation....1437
26.119.2 LCS Configuration....1437
26.119.3 OCS Configuration....1442
26.119.4 Lotus Sametime Configuration....1447
26.119.5 Unified Communications Server Configuration....1449
26.120 SAA Backup and Restore....1450
26.121 Troubleshooting....1451
26.122 Speech to Text - Description....1452
26.122.1 Speech to Text - Installation....1455
26.122.2 Speech to Text Configuration....1455
26.122.3 Activating or Terminating Speech to Text....1459
26.122.4 Speech to Text Alarms....1460
26.123 Speech Navigation - Description....1461
26.123.1 Speech Navigation Installation....1462
26.123.2 Speech Navigation Configuration....1462
26.124 Unified Messaging - Description....1465
26.125 Basic Unified Messaging Features....1466
26.126 Optional Unified Messaging Features....1467
26.126.1 Configuring UM-SMTP, UM-Web View and Standard UM....1470
26.126.2 Configuring UM-SMTP, UM-Web View and Standard UM....1481
26.126.3 Mail Server Adapter Types....1486
26.126.4 Configuring Advanced UM....1487
26.126.5 Advanced Parameters Worksheet....1488
26.127 Configure IMAP Server Settings for Exchange or Office 365....1496
26.128 Configure a Superuser Account for Office 365....1502
26.129 Create a Superuser Account for Microsoft Exchange 2016 or 2019....1504
26.130 Troubleshooting Notes for IMAP for Exchange or Office 365....1507
26.131 Configure IMAP Server Settings for Google Apps....1516
26.132 Configure Advanced UM Parameters....1520
26.133 Configure Text to Speech....1526
26.134 Configure Advanced UM Parameters....1527
26.135 Configure Text to Speech....1528
26.136 Force Manual License Update....1529

26.137 Enable Advanced UM for User Mailbox....1529
26.138 Troubleshooting Standard UM....1531
26.138.1 Before You Call Mitel Product Support....1532
26.138.2 Troubleshooting Advanced UM....1533
26.138.3 Upgrading a System With Advanced UM....1538
26.139 Visual Voice Mail Support....1538
26.140 VPIM - Description....1539
26.140.1 Configuration Overview....1541
26.140.2 NuPoint-UM Configuration....1543
26.140.3 Exchange Server 2010 Configuration....1549
26.141 Web View - Description....1549
26.142 MiVoice Office 250 Integration Overview....1550
26.142.1 Prerequisites for the MiVoice Office 250 Integration....1552
26.142.2 MiVoice Office 250 Integration Configuration Overview....1553
26.142.3 MiVoice Office 250 Integration Task Summary....1554
26.142.4 MiVoice Office 250 Integration Troubleshooting....1559
26.143 About Call Director....1560
26.144 About the NuPoint UM Documentation Suite....1562
26.145 What's New in This Release....1563
26.146 About the Call Flow Page....1564
26.147 About the Configuration Page....1567
26.148 Finding online Help Quickly....1574
26.149 Accessing Documentation, Release Notes, Articles, and Downloads....1575
26.150 Contacting Mitel....1576
26.151 Disclaimer, Trademarks, Copyright....1577
26.152 Personal Call Flow Example....1577
26.153 Corporate Call Flow Example - Main Auto Attendant....1582
26.154 System Templates....1586
26.155 Voicemail RADs....1592
26.156 Tutorials....1594
26.157 Override....1594
26.158 Schedule....1597
26.159 Message....1599
26.160 Menu....1601
26.161 Call Transfers....1604
26.162 Voicemail....1612
26.163 Dial-by-Name....1614
26.164 Internal/External Call Handling....1616
26.165 Caller ID Filter....1617
26.166 Daily Greeting....1618
26.167 Message Center....1620
26.168 Language Router....1621
26.169 Call Flow Authoring Procedures - Overview....1623
26.170 Starting with a template....1625
26.171 Adding an action....1626
26.172 Deleting an action....1626
26.173 Reusing an action....1627
26.174 Copying a call flow....1628
26.175 Deleting a call flow....1630
26.176 Inserting an action....1630
26.177 Setting action properties....1631
26.178 Setting the prompt language....1632
26.179 Recording and Importing Messages....1632
26.180 Viewing call flow paths....1635
26.181 Printing call flows....1636
26.182 Call Flow Authoring Procedures - Overview....1637

26.183 Starting with a template.... 1639
26.184 Adding an action.... 1640
26.185 Deleting an action.... 1640
26.186 Reusing an action.... 1641
26.187 Copying a call flow.... 1642
26.188 Deleting a call flow.... 1644
26.189 Inserting an action.... 1644
26.190 Setting action properties.... 1645
26.191 Setting the prompt language.... 1646
26.192 Recording and Importing Messages.... 1646
26.193 Viewing call flow paths.... 1649
26.194 Printing call flows.... 1650
26.195 About Call Director Reports.... 1650
26.195.1 View a Call Flow Report.... 1651
26.195.2 Reset a Call Flow Report.... 1652
26.195.3 Run a System Report.... 1652
26.196 About Call Flow Reports.... 1653
26.196.1 Viewing a Call Flow Report.... 1654
26.196.2 Resetting a Call Flow Report.... 1655
26.197 About MiCollab Client.... 1655
26.197.1 What's New in MiCollab Client.... 1664
26.197.2 Requirements.... 1664
26.197.3 About Licensed Features.... 1668
26.197.4 Teamwork Mode.... 1678
26.197.5 Provisioning MiCollab Client.... 1679
26.197.6 Maintaining MiCollab Client.... 1680
26.197.7 Troubleshooting MiCollab Client.... 1681
26.197.8 Contacting Technical Support.... 1681
26.198 Enterprise Tab.... 1681
26.198.1 Adding and Editing Corporate Locations.... 1701
26.198.2 Adding and Editing Trusted Servers.... 1702
26.198.3 Creating an Enterprise.... 1703
26.198.4 Advanced Calendar Integration Settings.... 1705
26.199 Synchronization Tab.... 1711
26.199.1 Adding and Editing AD/LDAP Synchronizers.... 1715
26.200 PBX Nodes Tab.... 1720
26.200.1 Adding and Editing PBX Nodes.... 1724
26.201 Accounts Tab.... 1753
26.201.1 About Login IDs.... 1757
26.201.2 Adding and Editing Accounts.... 1759
26.202 Corporate Directory Tab.... 1771
26.202.1 Adding Corporate Contacts.... 1773
26.202.2 ACD Settings Tab.... 1774
26.203 Collaboration Tab.... 1777
26.203.1 Adding and Editing Collaboration Servers.... 1778
26.204 Features Tab.... 1781
26.204.1 Adding and Editing Feature Profiles.... 1784
26.204.2 Adding and Editing Feature Profile Members.... 1785
26.205 Peering Tab.... 1786
26.205.1 Adding and Editing Peer Servers.... 1787
26.206 Federation Tab.... 1789
26.206.1 Federation Tab.... 1790
26.207 View Licensing Information.... 1792

27 Install and Upgrade Applications 1793
27.1 View ServiceLink Status 1803

28 Administration 1806
28.1 MSL Web Services 1806
28.2 Backup Server Data 1807
28.3 View Log Files 1813
28.4 View Event Logs 1816
28.5 About SDS Distribution Errors 1819
28.6 View System Information 1821
28.7 Access System Monitoring Tools 1821
28.8 System Users 1822
28.8.1 Manage User Accounts for Remote VPN Access 1822
28.8.2 Manage Multiple Admin Accounts 1822
28.8.3 Digital Certificates for VPN Connections 1824
28.8.4 Password Quality Requirements 1826
28.9 Shutdown or Reboot 1828
28.10 Mitel Virtualization Diagnostics Tool 1828
28.11 Applications 1839

29 About Remote Access 1840
29.1 PPTP Settings (Client-to-Server VPN) 1840
29.2 Configure Port Forwarding 1844
29.3 Configure Syslog 1844
29.4 About SSL Web Server Certificates 1846
29.5 Manage Third-Party Certificates from Let's Encrypt 1847
29.6 Manage Third-Party Certificates from an Alternate Certificate Authority 1850
29.7 Manage Self Signed SSL Certificates 1860
29.8 Manage TLS Protocol 1863
29.9 Certificate Authority Trust 1864

30 About Integrated Directory Services 1865
30.1 Supported IDS Configurations 1868
30.2 Guidelines and Limitations 1875
30.3 Configure MiCollab or MiVoice Business Express System with IDS 1878
30.4 Configure MiCollab IDS for MiVoice MX-ONE 1882
30.5 Configure MiCollab IDS for MiVoice 5000 1883
30.6 Configure Active Directory Authentication 1886
30.7 Manage IDS Connections 1889
30.7.1 IDS Connection for MiVB Users and Contacts from Active Directory 1903
30.7.2 IDS Connection for MiVoice 5000 Contacts from Active Directory 1904
30.7.3 IDS Connection for MiVoice 5000 with contacts synchronized from a MiVoice 5000 Directory Service 1906
30.7.4 IDS Connection for MiVoice MX-ONE Contacts 1907
30.7.5 IDS Connection for Mitel MetaDirectory 1908
30.7.6 IDS Connection for Mitel InAttend 1909
30.8 Set Default IDS Attribute Mappings 1910
30.8.1 Conditions 1910
30.8.2 Attribute Mapping Descriptions 1912

30.9 Set Custom IDS Attribute Mappings....1918
30.10 Attribute Mappings for Mitel MetaDirectory....1919
30.11 Attribute Mappings for Mitel InAttend (BluStar)....1920
30.12 Disable IDS on MiCollab....1920
30.13 Configure Access to External (Off-board) Directory....1921
30.14 Partitioning the External (Off-board) Directory....1927
30.15 Migrate MiCollab with MiVoice Business IDS to MiCollab IDS....1929
30.16 Migrate MiCollab with MiCollab Audio, Web and Video Conferencing IDS to MiCollab IDS....1932
30.17 Migrate MiCollab with MiCollab Client IDS to MiCollab IDS....1935
30.18 IDS Synchronization Overview....1939
30.19 Scheduling IDS Synchronizations....1940
30.20 Add, Edit and Delete Entries using IDS....1941
30.21 Non-Corporate Contacts....1943
30.22 **Teamwork Mode Users**....1947
30.23 Partitioning the External (Off-board) Directory....1949
30.24 Add External Numbers....1951
30.25 Viewing IDS Detained Operations....1953
30.26 Managing LDIF Files....1953
30.27 LDAP Query Basics....1954
30.28 Filtering out Disabled AD Users from IDS....1954
30.29 Managing Detained and Failed IDS Operations....1954
30.30 IDS Synchronization Error Handling....1956
30.31 Troubleshooting LDAP Authentication....1957
30.32 Integrating MiCollab Client Database with USP....1958
30.32.1 Importing User Data from MiVoice Business Platforms....1959
30.32.2 Resolving MiCollab Client PBX Sync Errors....1960
30.33 Configure MiCollab Settings....1962
30.33.1 Change Password Strength....1962
30.33.2 Configure Service Information E-mail....1963
30.33.3 Collect Logs and Diagnostic Data....1966
30.33.4 Set Default Deployment Profile for EHDU....1967
30.33.5 CloudLink Integration....1968
30.34 Configure MiCollab Language....1977
30.35 Vidyo Tenant Credentials....1979
30.36 Configure Networks....1981
30.37 Configure E-mail....1985
30.38 Configure DHCP Server....1986
30.39 Configure Server Date and Time....1988
30.40 Add or Delete Hostnames and Addresses....1992
30.41 Manage Domains and DNS Settings....1993
30.42 Configure IPv6 in IPv4 Tunnel....1994
30.43 Configure SNMP Support....1996
30.44 Configure Network Interface Card Settings....2005
30.45 Review Server Configuration....2006
30.46 Support and Licensing....2007
30.47 Panel Requires Upgrade....2008

31 Cloud Service Provider....2009

31.1 Google....2009
31.1.1 Google Gadget Configuration....2009
31.1.2 Google Apps Integration for MiCollab Audio, Web and Video Conferencing....2010
31.1.3 Configure OAuth 2.0 for Service Accounts....2013
31.1.4 Configure OAuth 2.0 for Installed Applications....2015

31.1.5 About Google Apps Integration..... 2024
31.2 Microsoft..... 2025
31.2.1 Configure Microsoft Identity..... 2025

32 Glossary..... 2027

Getting Started 1

This chapter contains the following sections:

- About MiCollab
- What's New in this Release
- Logging In
- About the Documentation Set
- About the MiCollab Administrator Portal
- Contacting Technical Support
- Disclaimer, Trademarks, and Copyright
- About the Users and Services Main Page
- Using the Navigation/Search Bar
- Displaying Data
- Button Icons
- About Help and Versions

1.1 About MiCollab

MiCollab is a software and hardware solution that allows you to

- install multiple Mitel applications on a single server, and
- manage the server and the installed applications from this web-based administrator portal.

MiCollab and the installed applications provide services (voice mail, for example) to the users on a Mitel MiVoice Business, MiVoice Office 250, MiVoice Office 400, MiVoice 5000, or MiVoice MX-ONE communication platforms. In addition, MiCollab provides users with a personal web-based end-user portal (MiCollab End User Portal) that allows them to modify the settings of their installed applications.

Several configurations of MiCollab are supported. Refer to the *MiCollab Engineering Guidelines* for details about these configurations. The server settings that you need to configure from this administrator portal depend on your application requirements and your network configuration.

1.2 What's New in this Release

For a list of new functionality, see What's New in This Release on the Mitel Customer Documentation site.

1.3 Logging In

The Username and Password for the administrator portal are set from the server console during installation. The *MiCollab Installation and Maintenance Guide* provides complete instructions.

Instructions for logging into the administrator portal are also provided below:

1. Open your browser.

> **Note**:
> The following browsers are supported: Microsoft Edge 115 or higher, Google Chrome version 115 or higher, and Mozilla® Firefox® 115 or higher. Note that Flow Through Provisioning and Reach Through functionality are only supported in Firefox browser.

2. Enter the following URL:

   https://<Fully Qualified Domain Name of the MiCollab server>/server-manager
3. A security alert may appear. Click **Yes** to accept the security certificate.
4. Enter your Username and Password and click **Login**.

   - Default Username is "admin"
   - Password is set during installation

> **Note**:
> The default timeout for a Server Manager session is two hours.

5. You will be prompted to change the password immediately on first login. Enter and verify the new password and click **Change Password**.
6. Click **OK** to login to the Server Manager.

Click the Help link in the administrator portal for instructions about performing administration tasks and adding users. When you add a new user, the system is configured to automatically send a Welcome e-mail to the user's e-mail address. The Welcome e-mail provides the user with his or her account information and the URL of the MiCollab End User Portal :

https://<Fully Qualified Domain Name of the MiCollab server>/portal

> **Note**:
> For more information about the End User Portal, refer to the online help provided in the portal interface.

1.4 About the Documentation Set

All Mitel product documentation is available at Mitel Online. You must be a registered user.

To access product and technical documentation on Mitel Online:

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From the left menu, select **Docs Center**.
3. Click **Applications** > **Collaboration** and then select **MiCollab**.
4. To view a document, click the document title.
5. To download a document, right-click on the name of the document, and click **Save Target As**.

Note:
To view online help, ensure that Compatibility view is enabled for your browser.

MSL Documentation

- **MSL Installation and Administration Guide**: provides platform requirements, software installation instructions and maintenance and troubleshooting procedures
- **Server Manager Online Help** (this online help): provides the administrator with instructions for configuring the MSL server

MiCollab Documentation

- Installation and Maintenance Guide: provides platform requirements, software installation instructions and maintenance and troubleshooting procedures.
- Platform Integration Guide*:* provides instructions on how to configure the MiVoice Business, MiVoice Office 250, MiVoice 5000, and MiVoice MX-ONE communication platforms to support the MiCollab applications.
- Engineering Guidelines: highlight specific areas of the product that you must consider before installation. Use them to plan site installations.
- Administrator Portal Online Help: (this online help) provides the administrator with instructions about configuring the MiCollab server and maintaining the applications.
- MiCollab End User Portal Online Help: provides end users with instructions about setting up and using their MiCollab applications.

End-User Guides

- Messaging User Guide
- TUI Quick Reference Guide
- Competitive TUI Voice Mail User Guide
- Competitive TUI Quick Reference Guide

MBG (formerly Mitel Border Gateway)

- Remote Phone Configuration Guide

Speech Auto Attendant

- See the NuPoint UM User Guide

MiCollab Client

Engineering and Administrator Documentation

- MiCollab Client Advanced Engineering Guidelines: provides system requirements, configuration information, network diagrams, virtualization information, performance recommendations, system capacities.
- MiCollab Client Administrator Guide: includes PBX configuration information, Unified Communications specifications and hardware configuration information, and configuration information for integrated applications.
- MiCollab Client Administrator Online Help: provides a high-level overview of the provisioning process with links to task-related instructions. The task-related instructions provide detailed descriptions for fields and options.

End-user documentation

- MiCollab Client end-user online help: provides basic feature and usage information for the PC Client, Web Portal, MAC Client, and Mobile Client.
- Online Help for supported clients: embedded in the user interfaces, the help systems describe the interface elements, supported features, and provide task-related instructions

MiCollab Audio, Web and Video Conferencing (formerly Mitel Collaboration Advanced)

- Web Conferencing and Remote Support Installation Manual: provides installation instructions and maintenance procedures.
- MiCollab Audio, Web and Video Conferencing User Guide: contains end user information and procedures for Mitel Collaboration Advanced.
- MiCollab Audio, Web and Video Conferencing Online Help: provides administration and programming procedures.

Application Management Center (AMC)

- See the online help in your AMC Account

1.5 About the MiCollab Administrator Portal

This web-based portal allows you to

- configure server settings
- administer the Mitel applications that are installed on the MiCollab server
- maintain the server

1.6 Contacting Technical Support

Contact Mitel Technical Support if you require technical assistance. Before you call, check this Help system for tips and solutions. If you are unable to find a solution, please have the following information ready when you call:

- The MiCollab MSL software revision
- The nature of the problem
- What you were doing with the application when the problem occurred
- Troubleshooting results

For information about contacting Mitel Technical Support, access Mitel Online at http://www.mitel.com.

1.7 Disclaimer, Trademarks, and Copyright

Disclaimer

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Copyright

™, ® - Trademark of Mitel Networks Corporation

© Copyright 2020, Mitel Networks Corporation

All rights reserved

1.8 About the Users and Services Main Page

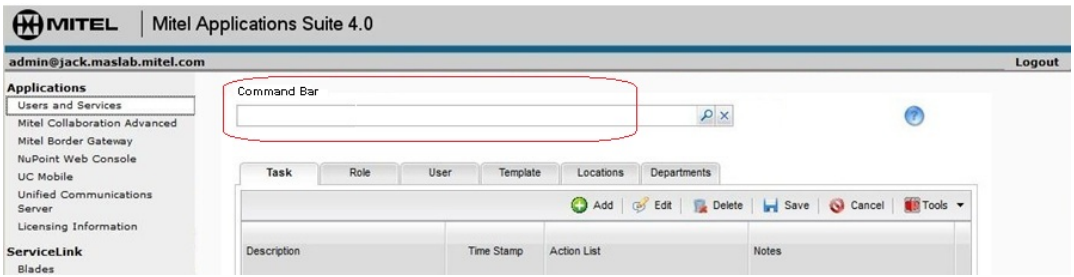
Overview

From the main page, you can perform the following operations on the data:

- perform tasks, such as display and search data records
- add, edit, and delete data records
- save or cancel your operations
- access import, export, reporting, and printing functions.

Command/Search Bar

The Command Bar is located at the top of the Main Page:



Use the Command Bar to perform the following operations:

- perform searches
- display database information
- generate reports
- list information with common characteristics (for example, all users without an email address)
- perform bulk imports or exports of user data

The command bar supports auto-completion capabilities. As you type a command, the commands that best match your entered text are displayed. If a command is not supported or recognized by the system, it is highlighted with red text.

To use the Command Bar simply enter your command in the bar in the form of a simple request. For example:

- Search for phone number <#####>
- Show all users with first name <first name>
- Show all users with Login ID <login id>
- List users without mailbox
- Import user data
- Export user data
- Print list of MiCollab Audio, Web and Video Conferencing users
- Generate report of unassigned services

Also, see Searching the Database.

Note:
The Command Bar does not support boolean operators such as "and" or "or".

Data Tabs

The Users and Services main page organizes the system user and application data under the following tabs:

- **Task**:
- **Role**: allows you to create roles. Roles define different user groups within your business, for example sales executives or product support. You then associate the roles with user templates that define the phone and application services for the user group. A user role can be associated to multiple different user templates.
- **User**: displays a list of the MiCollab user accounts. From the **User** tab, you can add or edit a user account and enter the following information:
  - personal information, such as first name and last name
  - assign phones
  - assign group membership
  - assign services, such as Speech Auto-Attendant, MiCollab Mobile Client , and NuPoint UM
- **Template**: allows you to create, edit, or delete user templates. Use templates to define phone and application service data for a user role. Then, whenever you create a new user, you can apply the template data to the user record to save time and minimize data entry.
- **Locations**: allows you to assign a location to a user.
- **Departments**: allows you to enter a department name, for example "Sales", to a user.

Software Version

The MiCollab software release versions are listed at the bottom of the main page.

1.9 Using the Navigation/Search Bar

Navigating the Users and Services Application

When performing administrations tasks, such as adding a user, creating a template, or adding MiCollab Client service, you can use the Navigation/Search bar to quickly access the required application page.

1. Type the task that you want to perform in the Navigation/Search bar. The following examples show the format that you should use when entering tasks:

   - Bulk import data from file
   - Manage deferred queue
   - Download example bulk import CSV file
   - Quick add a user
   - Add phone
   - Modify template
   - Create role
   - Add mailbox to last name smith
   - Add mca to user with first name john

2. Click on  . The application page that you use to perform the operation is displayed.

Searching the Database Using Quick Search

By default, the search function finds matches in specific fields on the selected tab. It searches for the data that you enter in the Command line in the following fields:

Tab	Fields searched
None (Empty)	Fields (as listed below) for the current tab are searched.
Task	Task Description
Role	Role Name
User List	First Name, Last Name, Number
Templates	Template Name
Locations	Location, Location Description
Departments	Department, Department Description

For example, if you select the **User** tab, enter 1001 in the Command line, and click on  . The search function displays any records that have the number 1001 in the following fields:

- First Name
- Last Name
- Number

Searching the Database Using Advanced Search

To search records in each of the tabs of the main page:

1. Select the desired tab (for example, Task or User). Note that your search is restricted to the data records contained under the current tab.
2. Type your search query in the Find field. To search efficiently, include a field name in your command query. For example:
   - Find phone number <#####>
   - Show all users with first name <first name>
   - Show all users with Login ID <login id>
   - Find users with phone number <number>
   - Search users with department <department name>
   - Display users with email address <email address>
   - Search users with last name similar to <first name>
   - Search users with location <location name>
   - List users without mailbox
   - Show all users with mca service
3. Click on  . The results are displayed in the main window.
4. Click on  to clear the Task line.

1.10 Displaying Data

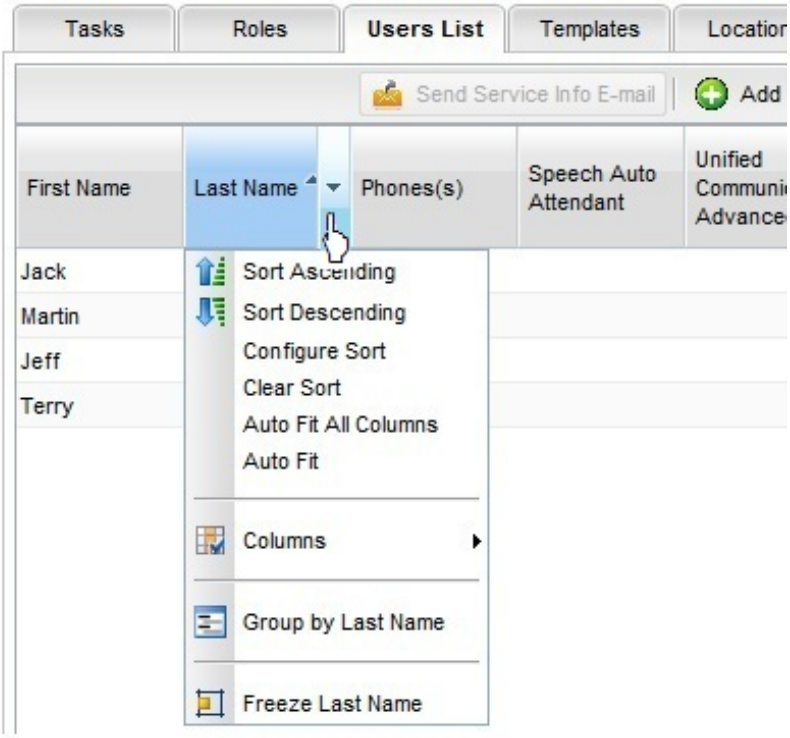
Sorting

You can customize the way data records are displayed in each tab. For example, in the **User** tab:

- To sort the First Name or Last Name column alphabetically, right-click in the column header.
- To sort the Phone numbers in either ascending or descending order right-click the Phone(s) column header.



- To create a customized sort using multiple columns, select **Configure Sort**, define the sort criteria and click **Apply**.
- To adjust a column, left-click in the column header and select the desired action.



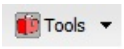
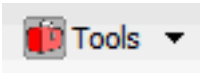
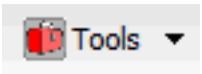
Viewing the Window Tabs

If a window supports more tabs than can appear in the window viewing area, you can click the tab tool in the top right corner of the window and select to view the hidden tab.

1.11 Button Icons

In the USP application, you perform operations by clicking the following buttons:

Button Icons	Click to . . .
	send a user a service information e-mail
	add a new record

Button Icons	Click to . . .
	edit or reuse an existing record
	delete one or more records
	save your edits in the active tab or window
	cancel your edits in the active tab or window
	assign an orphan record
 Import Export	launch bulk user import or export tool
 Report	save a report of the user data as an .dita file
 Print	print a report of the data in the current tab

Button Icons	Click to . . .
	identifies a phone's ring group service level as Full Service. A Full service phone belongs to a Personal Ring Group.
	identifies the pilot number for a Personal Ring Group.
	identifies a phone's ring group service level as Multi-Device Service. A Multi-Device Service phone belongs to a Multi-Device User Group.
	identifies the pilot number for a Multi-Device User Group.
	identifies a warning condition
	identifies an error condition
	access help

1.12 About Help and Versions

This help file is designed to provide information and instructions for the administrator Web portal and uses the following conventions:

- **Links**: Most of the Help topics link to other additional resources. When you click a link, you jump to another help topic or URL in your Web browser. Click your browser's **Back** button to return to the previous topic. You can identify a link by the blue unlined text. For example, here is a link to the MiCollab Audio, Web and Video Conferencing Introduction topic.
- **Print option**: To print the active topic using your default printer, use the **Print** option on your browser window.

For sales, service, or technical support, contact your local authorized Mitel provider. If you don't know the contact info for your local provider, use the “Partners – Mitel Partner Locator” link at the top of the Mitel Home page to locate a nearby office.

For information on how to contact Mitel Technical Support outside of North America, please refer to your Channel Support Agreement.

Performing Administration Tasks 2

This chapter contains the following sections:

- Configure the Server Settings
- Administer the Applications
- Maintain the Server
- Assign Local Administrator User

2.1 Configure the Server Settings

1. Configure Server Date and Time
2. Configure Remote Access Settings
3. Install and Upgrade Applications
4. Install Blades
5. Grant Network Privileges
6. Configure Port Forwarding
7. Add Hostnames and Addresses
8. Configure Email settings
9. Configure Internal DHCP server
10. Configure Proxy Settings
11. Manage Client Certificates
12. Install Web Server Certificate (optional)
13. Manage TLS Protocol
14. Configure PPTP Settings (Client-to-Server VPN)
15. Add ICPs
16. Change LDAP Directory Settings
17. Configure SNMP support
18. Manage Domains
19. Set System Information Access
20. Configure Traffic Shaping
21. Review Server Configuration
22. Configure MiCollab Settings
23. Set MiCollab Language
24. Run MiCollab Client Integration Wizard (if required)
25. Configure Flow Through Provisioning or Add or Edit Network Elements if Flow Through Provisioning is not supported
26. Run the Reconcile Wizard (if required)
27. Configure IDS on MiCollab (optional)

2.2 Administer the Applications

1. Provision Users and Services
2. Perform MiCollab Audio, Web and Video Conferencing Administration
3. Perform MBG Administration

   or Remote MBG Administration
4. Perform NuPoint UM Administration (includes Speech Auto Attendant)
5. Perform MiCollab Client Service Administration
6. Configure Vidyo Settings
7. Configure Service Info E-mail

Note:
For details on MBG administration, navigate to the online help from the MBG application.

2.3 Maintain the Server

1. Configure MSL Web Services
2. View ServiceLink Status
3. View Log Files/Collect Log Files
4. View Event Logs
5. View System Information
6. Access System Monitoring Tools
7. Manage System User Accounts for Remote Access
8. Backup or Restore Server Data
9. Shutdown or Reconfigure Reboot

2.4 Assign Local Administrator User

You can assign the "Local Administrator" login to a single system user who can then perform a subset of the MiCollab administrative functions. Local Administrator permission allows adding/editing users, phones, and services. The account name " local-admin" is created when MiCollab is installed. To assign a user to this account, modify the existing information.

Two email pseudonyms are automatically created for the Local Administrator user: < firstname.lastname> and < firstname_lastname>.

The Local Administrator will access the Administrator Portal in the same way as the System Administrator, but will see a limited subset of administrative tasks.

To assign Local Administrator privileges:

1. In the server manager menu, under **Administration**, click **System users**.
2. Click the Modify link associated with the local-admin account.
3. Enter the name and address information for the Local Administrator user. (Note: Department information is not linked to the "Department" field in the User Services and Provisioning application.)
4. Click **Save**.

> **Note**:
> Newly-created accounts are locked until the password is entered/changed.

To set or reset the Local Administrator password:

1. In the server manager menu, under Administration, click **System users**.
2. Click the Reset password link associated with the local-admin account. Passwords must contain at least one upper case letter, one lower case letter, one number, and one non-alphanumeric character, and be at least 7 characters long.
3. Enter the new password and then confirm by entering again.
4. Click **Save**.

To lock the Local Administrator from account access:

1. In the server manager menu, under Administration, click **System users**.
2. Click the Lock account link associated with the local-admin account.
3. Click **Lock** to confirm.

> **Note**:
> A locked account is unable to log in or collect email. You can unlock the account by resetting the password.

To view local-admin user's access logs:

1. In the server manager menu, under Administration, click **View log files**.
2. In the **Choose a log file to view** list, select **httpd/ admin_access_log**.
3. In the **Filter Pattern** field, enter **local-admin** and then click **Next**. There may be multiple httpd/ admin_access_log.yyyymmddhhmmss files. The timestamp indicates the ending timestamp for the logs in that file.

About the Users and Services Application

3

This chapter contains the following sections:

- View User Directory
- Add or Edit Location Information
- Add, Edit or Delete Department Information
- Initial Users and Services Provisioning
- About Hot Desk Users
- View User Directory
- Configure Service Information E-mail
- Manage Unassigned Services
- Delete Services
- Configure MiCollab Language

3.1 View User Directory

Overview

The Users and Services directory allows you to manage user data and assign or remove application services, such as MiCollab Audio, Web, and Video Conferencing or NuPoint UM. The directory lists user names and office numbers for MiCollab users and shows the services that are assigned to each user. Above the directory list, the "Unassigned services" and "Total number of users" are displayed.

View Directory Entries

1. Under **Applications**, click **Users and Services**.
2. Click the **User** tab.
3. Click **Show all**. Users are listed alphabetically by their last names. Services appears as column headings along the top of the directory.

Field/Column	Description
Last Name First Name	Displays the name of the user. The name fields can be blank, but you must assign a Login ID. Duplicate names are allowed. Although the Last Name and First Name can be the same, the combination of "Last Name, First Name" and "Office Phone #1" must be unique. Click a user's last name to display the information for that user.

Field/Column	Description
Phone(s)	The user's extension number(s) on the communications platform. This field can be blank.
	Indicates that a service (for example, Teleworker) that is hosted on the local node is assigned to the user. A blank cell indicates that the service is not assigned. The MiCollab Client service is available to all users. However, the service is not active unless it's assigned to one or more of the user's phones.
	Identifies data elements that are being shared via Flow Though Provisioning.

Note:
To display e-mail addresses, perform a search on an e-mail address.

Note:
If AWV and NP-UM ports are listed in the MiCollab USP directory, do not delete them from USP. They should not be assigned any services.

Locate an Existing User in the Directory

1. In the Search field, enter one of the following for the user:
   - First Name
   - Last Name, or
   - Phone extension number

Note:
Entering a partial name or number broadens your search and typically returns more results.

2. In the View field, set the number of results that you want to display per page.
3. Click on **Search**.

Directory Tasks

From the Users directory, you can perform the following tasks:

- Quick Add
- Edit a user's information
- Reset a user's login password and TUI passcode
- Add a new service to a user
- Delete a service from a user
- Delete users
- Send a user a welcome email
- Send CloudLink Welcome Email
- Deploy Mobile Client for Softphone
- Deploy MiCollab Clients for EHDU
- Generate Reports
- Connect to MiVB System Tool

About Unassigned Services

Unassigned services or mailboxes are services that have been registered with an application but have not yet been assigned to a user. Click the **View** link to display a list of available services (for example, unassigned mailboxes). See Managing Unassigned Services for more information.

Note:
When you add or delete services through any of the applications, it can take up to 5 minutes before the numbers are updated. For example, if you add a mailbox through the NuPoint UM Web Console, it can take up to 5 minutes before the number of "Unassigned mailboxes" is increased.

3.2 Add or Edit Location Information

You can populate the "Location" drop-down lists in the interface by adding or editing the location information. This entry is optional.

1. On the Users and Services main page, click the **Locations** tab and then click **Add**.
2. Enter location information as described below.
3. Click**Save**.

Field	Description	Value
Name	Enter the name of the location.	If Remote Directory Number Synchronization is enabled on the MiVoice Business , names can be up to 128 characters in length; otherwise, the maximum length is 10 characters. This field supports ASCII characters.
Description	Enter a location description (optional).	Up to 255 characters.

To edit a location name:

1. On the Users and Services main page, click the **Locations** tab.
2. Double-click on the Location name.
3. Modify the information as required.
4. Click on **Save**.

To delete a location name:

1. On the Users and Services main page, click the **Locations** tab.
2. Select the Location name.
3. Click on **Delete**.
4. Click on **Save**.
5. Click on **Yes**.

3.3 Add, Edit or Delete Department Information

Use the **Departments** tab to

- populate the "Department" drop-down lists in the interface
- to add a Department name for Speech Auto Attendant recognition (only required if you want to have a spoken Department name recognized by the auto attendant).

Add a Department

1. On the Users and Services main page, click the **Departments** tab and then click **Add**.
2. Enter Department information as described below and then click **Save**.

Field	Description	Value
Name	Enter the name of the department (for example, "Sales") in text only. Numbers and special characters are not permitted.	If Remote Directory Number Synchronization is enabled on the MiVoice Business , names can be up to 128 characters in length; otherwise, the maximum length is 10 characters. This field supports ASCII characters. **Note**: This value must contain ONLY pronounce-able text. Numbers and special characters are not supported by text-to-speech software. (For example, to add a number to a Department name, enter the text representation of the number ("Department Five") or to represent the "&" character, enter the word "and".)
Description	Enter a department description.	Up to 255 characters. (Optional).

Field	Description	Value
Number	Enter the phone number of the department, if applicable.	

Note:
New department names will not be added to the SAA directory immediately. To see an updated list, you can wait for the nightly (NuPoint UM) Auto Update or you can force an update using the NuPoint UM Data Source sync function. For more information, refer to the *Update the User Data Source* topic in the NuPoint UM online help.

Edit a Department

1. On the Users and Services main page, click the **Departments** tab
2. Double-click on the department name.
3. Modify the information as required.
4. Click **Save**.

Delete a Department

If you delete a department from MiCollab, the department is also removed from the user entries. If Flow Through Provisioning is enabled to MiVoice Business elements, the department is also removed from the MiVoice Business Department form and user entries.

However, the behavior on the MiVoice Business is slightly different. Before you can delete a department from the MiVoice Business Department form, you must first remove all references to that department name from the MiVoice Business user entries. After you delete a department from the MiVoice Business, the department is also removed from MiCollab if Flow Through Provisioning is enabled.

1. On the Users and Services main page, click the **Departments** tab
2. Select the department name.
3. Click **Delete**.
4. Click **Save**.
5. Click **Yes**.

3.4 Initial Users and Services Provisioning

Note:
Users must be provisioned using only one browser tab at a time.

Note:
For MiVoice MX-ONE and MiVoice 5000 users, User and services provisioning is performed from the respective communication platform administration interface and not from the MiCollab Users and Services application. See the respective communication platform in *MiCollab Platform Integration Guide* for more details.

1. Add the communication platforms as network elements:

   - Under **Applications**, click **Users and Services**.
   - On the **Network Element** tab, click **Add**.
   - Complete the fields as required.
   - Click **Save**.

   Note:
   If MiCollab is to be integrated with one or more MiVoice Business communication platforms using Flow Through Provisioning, do not add the network elements. They will be added automatically during the start sharing and sync operation.

2. View your available licenses in the Licensing Information page.
3. Configure the Applications Suite Language.
4. Define Locations for the site.
5. Define the Departments for the site.
6. Optionally add custom user templates and roles that define the user and service data that is common to user groups.

   Note:
   You can use the default templates by the system. The default templates are mapped to default UCC roles.and default UCC license bundles.

7. Provision the MiCollab user and service data using the method that is most suitable to your site:

For integrations with MiVoice Business communication platforms:

- Flow Through Provisioning **:** If you are configuring MiCollab with MiVoice Business servers, the recommended "best practice" is to configure Flow Through Provisioning and then add, edit and delete users from the MiCollab Users and Services application..

- Bulk Import from File: If you are installing MiCollab on a site with an existing MiVoice Business , export the user data to a comma separated (. csv) file and then import the file into MiCollab using the Bulk User Provisioning tool. For sites with a directory server, export the user data in LDAP Interchange Format (LDIF) and then import the LDIF file using the Bulk User Provisioning tool.
- Provisioning with IDS: If the site supports Integrated Directory Services (IDS), you can seed the USP database with entries from your corporate directory service database.
- Manually provision users: If this is a new site without an existing user database, you can provision users manually from the Users and Services application.

For integrations with MiVoice Office 250 or MiVoice Office 400 communication platforms:

- Bulk Import from File: If you are installing MiCollab on a site with an existing MiVoice Office 250or MiVoice Office 400 system , export the user data to a comma separated (. csv) file and then import the file into MiCollab using the Bulk User Provisioning tool. For sites with a directory server, export the user data in LDAP Interchange Format (LDIF) and then import the LDIF file using the Bulk User Provisioning tool.
- Manually provision users: If this is a new site without an existing user database, you can provision users manually from the Users and Services application.

For integrations with MiVoice 5000 or MiVoice MX-ONE communication platforms:

- Provision from management platform: provision users with MiCollab services from the MiVoice 5000 or MiVoice MX-ONE management interface by assigning a MiCollab role to the user entry. Refer to the *MiCollab Installation and Maintenance Guide* for integration instructions
- Provisioning with IDS: If the site supports Integrated Directory Services (IDS), you can seed MiCollab Client Corporate Directory with contacts from the MiVoice 5000, MiVoice MX-ONE, or Active Directory database.

3.5 About Hot Desk Users

Hot Desk Users (Internal)

Hot Desking allows anyone who is assigned as a "Hot Desk User" to log in to any available hot desk-enabled telephone. When a user logs into a hot desk device, the system associates that user's settings (such as directory number, COS/COR settings, display preferences (such as language), and button programming) with that device.

Once logged in, the user can

- Receive incoming calls at the set
- Place outgoing calls
- Retrieve voice messages
- Program and use feature keys

For information about programming the Hot Desk feature on the MiVoice Business , see the MiVoice Business System Administration Tool Help.

ACD Hot Desk Users

This feature allows an agent to log into any hot desk enabled set or ACD set and the system re-registers the set with the agent's personal phone profile and ACD functionality. After the agent logs into the set, the

agent has access to his or her own personal speed calls, features, and phone settings as well as the ACD agent functions. If you use hot desk ACD agents in a call center, you do not have to provide agents with separate phones for their personal use. Instead, you can make a pool of shared phones available to many agents and any hot desk enabled set or ACD set that a hot desk ACD agent logs into will also function as the agent's personal phone.

After a hot desk ACD agent logs in, the MiVoice Business system associates the user's personal phone settings, such as directory number, COS/COR settings, language display, and button programming with the set.

For information about programming the ACD Hot Desk users on the MiVoice Business , see the MiVoice Business System Administration Tool Help.

External Hot Desk Users

External Hot Desking extends hot desking capabilities to an external device, which makes it appear as an extension on the system. When the external hot desk user (EHDU) is logged into the MiVoice Business , a caller only needs to dial the extension number assigned to the user and the system automatically rings the user's cell phone, home phone or other device of choice—including an extension on another private network or PBX.

As a PBX extension, the external device user has access to extension dialing along with select PBX features and enterprise CLID. CLID enables the telephone number of the calling party to be displayed on the display screen of the receivers telephone.

For information about programming the External Hot Desk users on the MiVoice Business , see the MiVoice Business System Administration Tool Help.

SIP Softphone Hot Desk Users

This feature extends hot desking capabilities to a softphone, so that the user only need to perform one login and can attend calls on the go using user's cell phone, home phone, or other device of choice. The primary extension number entered while adding a new user using this feature will become the softphone number for the user. A user having Hotdesk SIP Softphone can also avail Teleworker service.

Note:
If the client is registered to a Hotdesk extension and the Hotdesk gets logged out, the softphone is disabled automatically. If the user wants to use the softphone again, the softphone must be enabled using the softphone toggle from the client.

After a SIP softphone user logs in, the MIVB system associates the user's personal phone settings, such as directory number and other settings to the softphone.

Note:
In MiVB there is no SIP Softphone Hot Desk User. Its only a user who logs into devices which supports Hot Desking, for example, like a SIP Softphone.

3.6 View User Directory

Overview

The Users and Services directory allows you to manage user data and assign or remove application services, such as MiCollab Audio, Web, and Video Conferencing or NuPoint UM. The directory lists user names and office numbers for MiCollab users and shows the services that are assigned to each user. Above the directory list, the "Unassigned services" and "Total number of users" are displayed.

View Directory Entries

1. Under **Applications**, click **Users and Services**.
2. Click the **User** tab.
3. Click **Show all**. Users are listed alphabetically by their last names. Services appears as column headings along the top of the directory.

Field/Column	Description
Last Name First Name	Displays the name of the user. The name fields can be blank, but you must assign a Login ID. Duplicate names are allowed. Although the Last Name and First Name can be the same, the combination of "Last Name, First Name" and "Office Phone #1" must be unique. Click a user's last name to display the information for that user.
Phone(s)	The user's extension number(s) on the communications platform. This field can be blank.
✓	Indicates that a service (for example, Teleworker) that is hosted on the local node is assigned to the user. A blank cell indicates that the service is not assigned. The MiCollab Client service is available to all users. However, the service is not active unless it's assigned to one or more of the user's phones.

Field/Column	Description
	Identifies data elements that are being shared via Flow Though Provisioning.

Note:
To display e-mail addresses, perform a search on an e-mail address.

Note:
If AWV and NP-UM ports are listed in the MiCollab USP directory, do not delete them from USP. They should not be assigned any services.

Locate an Existing User in the Directory

1. In the Search field, enter one of the following for the user:
   - First Name
   - Last Name, or
   - Phone extension number

   Note:
   Entering a partial name or number broadens your search and typically returns more results.

2. In the View field, set the number of results that you want to display per page.
3. Click on **Search**.

Directory Tasks

From the Users directory, you can perform the following tasks:

- Quick Add
- Edit a user's information
- Reset a user's login password and TUI passcode

- Add a new service to a user
- Delete a service from a user
- Delete users
- Send a user a welcome email
- Send CloudLink Welcome Email
- Deploy Mobile Client for Softphone
- Deploy MiCollab Clients for EHDU
- Generate Reports
- Connect to MiVB System Tool

About Unassigned Services

Unassigned services or mailboxes are services that have been registered with an application but have not yet been assigned to a user. Click the **View** link to display a list of available services (for example, unassigned mailboxes). See Managing Unassigned Services for more information.

Note:
When you add or delete services through any of the applications, it can take up to 5 minutes before the numbers are updated. For example, if you add a mailbox through the NuPoint UM Web Console, it can take up to 5 minutes before the number of "Unassigned mailboxes" is increased.

3.7 Configure Service Information E-mail

You can configure MiCollab to automatically send Service Information e-mails to your system users. This e-mail feature provides users with communication settings information, such as:

- Login ID
- Password
- Passcode
- Phone Type and Number

The system sends an e-mail, whenever you

- select a user in the Users and Services Directory page and click the **Send Service Info E-mail** button
- create a new user (either from MiCollab USP or from the directory server if MiCollab IDS is enabled)
- create an MiCollab Audio, Web and Video Conferencing user, or
- reset a user's password or passcode.

If you select a user in the Users and Services Directory page and click the **Send Service Info E-mail** button, the system sends a user a Service Information E-mail that contains all of the user's service information.

If you create a new user, the system automatically sends an e-mail to the user that contains the user's login ID, password, and a link to the MiCollab Web Client .

If you reset a user's password in the Users and Services application, the system sends the user an e-mail that contains only the new password.

You can send the e-mail with a default or custom greeting message. With the exception of the custom greeting, the information can be sent in two languages.

Conditions

- The Service Information e-mail feature is enabled by default.
- The Service Information e-mail is sent to the user's primary e-mail address that is entered in the User tab of Users and Services application.
- MiCollab sends a Service Information e-mail whenever any of the following methods are used to create a new user or reset a user's password:
    - Users and Services Add, Edit, or Quick Add User
    - Mitel Integrated Configuration Wizard
    - Users and Services Bulk Import
- The password is only included in the e-mail during the initial creation of a user or whenever the administrator resets the user’s password.
- If you create a user without an e-mail address, the system does not send a Service Information e-mail.
- If you disable the Service Information e-mail feature, all Service Information e-mails sent prior to the disabling of this feature are still delivered to the users.
- If you modify a user's password, a Service Information e-mail is sent with the new password. Note that an e-mail is not sent if a user modifies his or her own password.
- If you select a user in the USP directory and click the **Send Service Info E-mail** button, an e-mail is sent regardless of whether or not services are assigned to the user, providing the user is assigned an E-mail address.
- If you click the **Send Service Info E-mail** button in the USP directory page, all service information for the user is provided in a single e-mail. If you want the MiCollab Speech Auto Attendant Pilot/Access number numbers to be listed in the Service Information e-mail, you must enter these numbers in the Network Elements tab of the Users and Services application. The system takes the pilot/access numbers that you enter in the Network Elements tab and lists them in e-mail for the end users. If you do not enter the numbers in the Network Element tab, they will not be included in the e-mail.
- If MiCollab services are added to users who were originally created in a MiVoice Business system administration tool, a Service Information e-mail is not sent automatically, even if an e-mail address is provided for the user.

Configure Service Information E-mails

1. Configure the MiCollab server e-mail settings.
2. Under **Configuration**, click **MiCollab Settings**.
3. Click the **Welcome E-mail** tab.
4. Ensure that the **Send Welcome E-mail** option is **Enabled**.
5. By default, the MiCollab for Mobile deployment e-mail is sent to that application's users. Click the link if you do not want to distribute that e-mail. See *Mobile Client deployment e-mail* in **MiCollab Client Deployment** help for information about configuring the MiCollab for Mobile welcome e-mail.

6. Enter a valid e-mail address for the Sender account. This address appears in the "From:" header of the e-mail. It is recommended that you enter an e-mail address that will not be monitored (for example: do_not_reply@example.com).
7. By default, the **Append Do Not Reply Closing Message** option is set to **Enabled**. This option includes a note at the end of the Welcome e-mail that instructs users not to reply to the e-mail. If you want to receive replies from users at the Sender e-mail account, set this option to **Disabled**.
8. You can include a default greeting or a custom greeting in the Service Information e-mail:

   To use a the default greeting message, click **Default**.

   or

   To create a custom message, click **Custom** and enter a greeting message up to 2000 characters in length. Note that it is recommended that you include a link to the MiCollab Web Client at https://<host name of MiCollab server>/portal in your custom message. If the e-mail is required in multiple languages, you must enter the greeting message in each required language.

Note:
If you select the **Default** option while you have text entered in the Custom Message box, your text will be cleared.

Note:
To include a hyperlink in a custom message, you must include a space before and after the hyperlink, even if the hyperlink is on a separate line. Otherwise, the link may not function for all users.

9. Specify the service information that you want included in the e-mail by clicking the associated check boxes. If a service is checked, but the user does not have that particular service, no information for that service is included in the welcome e-mail. By default, all service information is checked.

   - The check boxes are available for MiCollab Microsoft Outlook Plugin, Legacy MiVoice for Skype for Business Plugin, MiCollab for Microsoft Client, and End User Portal Link.
   - MiCollab for PC Client download link will be included in the deployment e-mail. For MiCollab Servers that are upgraded from an older version to 8.0 or higher, the administrator must load the default deployment text or add the link **[####winpc####]** manually in the custom deployment text.
   - If you select the **Legacy MiCollab PC Client** checkbox, MiCollab Desktop Client download link will be included in welcome e-mail. By default, this checkbox will be selected in case of an upgrade or a new installation.

Note:
Select the **MiCollab Client Service** checkbox, to enable the **Legacy MiCollab PC Client** option.

10. Select up to two languages (First and Second Language). The e-mail information will be sent in both languages (sequentially in the selected order).

Note:
The system does not translate custom greeting messages.

11. Enter a valid destination e-mail address in the **Test E-mail Address** that you can access (for example your work e-mail address). To enter multiple addresses, separate each address with a semi-colon. After you click **Save**, an e-mail is automatically sent to the address or addresses that are entered in this field.
12. Click **Save**.
13. Open the e-mail account and check that the e-mail was received. Ensure that the e-mail contains the desired information.

Send Service Information

To send a Service Info E-mail that contains all of the user's service information from the Users and Services application directory:

1. Under **Applications**, click **Users and Services.**
2. Click **Users**.
3. Search for a specific user or click **Show all.**
4. Select the check boxes of the desired users.
5. Click **Send Service Info E-mail**.
6. Click **Ok**.

Disable Service Info E-mails

1. Under **Configuration**, click **MiCollab Settings.**
2. Click the **Welcome E-mail** tab**.**
3. Set **Send Welcome E-mail** option to **Disabled**.

3.8 Manage Unassigned Services

When you open the Users and Services application, the main page contains a summary listing the total number of users and the number of unassigned services for each application. An unassigned service is one that has been provisioned (possibly in another application or by use of bulk import), that does not have enough information for automatic assignment to a user (for example, a NuPoint UM mailbox, a teleworker phone, or an MiCollab Audio, Web and Video Conferencing service).

To view unassigned services:

1. Under **Applications**, click **Users and Services**.
2. Click the **View** link. The Unassigned Services Summary window opens.
3. Click the application tabs to view the unassigned services.

Manual Assignment

To manually assign unassigned services:

1. On the Users tab, search for the user to whom you want to assign the service (or click **Show all** .)
2. Select the user and then click **Edit** .
3. Select the tab for the service you want to assign.
4. Click **Assign Existing <service>** . A dialog box appears with a drop-down list of unassigned services.

> **Note**:
> This button is only available if there are unassigned services in the database.

5. Select the service to assign and then click **Assign** .
6. Click **Save** .

Assigning Teleworker Services

Another possible source of unassigned services is data migration. When teleworker phone data is migrated into the MiCollab environment from a previous standalone deployment, all phone services appear in the Users and Services application as "unassigned". If the phone has a Directory Number (DN) associated with it, it can be assigned as described above. If no DN is attached to the phone, it will appear in the list but you will be unable to assign it.

To manually assign a teleworker phone that has no DN:

1. Under **Applications**, click **MiVoice Border Gateway**.
2. Ensure that the teleworker service is enabled.

3. Register the telephone with the MiVoice Business to obtain a DN. (For information about registration, refer to the *Register IP Telephones* topic in the *MiVoice Business System Administration Tool Help* available at Mitel OnLine.)
4. Wait for the MiCollab database to update during its regular audit. (Maximum update interval is five minutes.)
5. Assign the service as described in "To assign unassigned services" above.

Automatic Assignment

In some cases, MiCollab will automatically assign an unassigned service to a user when it has enough information to do so.

For example:

- when a user has a phone with a DN and MAC address that match those of an unassigned service, the unassigned teleworker service is automatically assigned to that user.
- when a user has an email address that matches that of an unassigned service, the unassigned MiCollab Audio, Web and Video Conferencing service is automatically assigned to the user.

3.9 Delete Services

If Flow Through Provisioning is enabled, when you delete services on MiCollab the corresponding service is also deleted on the associated MiVoice Business system. See the table below for an explanation of configuration changes.

To delete a service from a user:

1. Locate the user in the directory.
2. Click the check box next to the user's Last Name.
3. Click **Edit**.
4. Click the tab of the service that you want to delete. For example, to delete a phone, click the **Phone** tab.

> **Note**:
> When you delete a MiVoice IP Phone , all the services associated with that phone including the voice mailbox messages are deleted. If replacing a set, ensure that you go to the "" tab for that user and remove the association with the Mitel phone in the **Extension** field of the **NuPoint Unified Messaging** tab before you delete the set. Otherwise, the user's voice mailbox messages will be deleted when you delete the phone.

5. Click **Delete <service>** where <service> is the name of the tab.
6. Click **Yes** to confirm the deletion.

When you delete this service in MiCollab :	You also change these settings in the MiVoice Business :
Phone	The phone device is deleted along with Tel Dir entry. Phone deletions are cascading, meaning that a deletion of associated services (mailbox and NuPoint UM services) is automatically performed. **Note**: Deleting a phone that is set as the Registered Phone for MiCollab Audio, Web and Video Conferencing service does not delete the MiCollab Audio, Web and Video Conferencing service, just the Registered Phone. **Note**: You cannot delete the primary phone from a user who has multiple phones. Also see Unable to Delete a User's Extension.
NuPoint UM Mailbox	When a mailbox is deleted from a user, the phone service associated with that mailbox has Call Forwarding removed and its COS value adjusted to reflect the remaining services.
MiCollab Client	MiCollab Client service has no effect on MiVoice Business settings.
Audio, Web and Video Conferencing	MiCollab Audio, Web and Video Conferencing service has no effect on MiVoice Business settings.
Teleworker Service	MBG teleworker service has no effect on MiVoice Business settings.
Vidyo Service	Vidyo service has no effect on MiVoice Business settings.

If a Delete Phone operation fails . . .

If MiCollab fails to delete a phone's services on the MiVoice Business , you will receive an error. You must manually delete all references to the phone's directory number/Remote Directory Number from the MiVoice Business System Administration Tool forms before you can complete the deletion.

Log into the MiVoice Business System Administration Tool and delete references to the phone's Directory Number/RDN from the following forms:

1. ACD Express Groups
   - Interflow Point Directory Number
   - Unavailable Answer Point Directory Number
2. ACD Path
   - Primary Agent Skill Group ID
   - Overflow 1 Agent Skill Group ID
   - Overflow 2 Agent Skill Group ID
   - Overflow 3 Agent Skill Group ID
   - Interflow Directory Number
   - Path Unavailable Answer Point Directory Number
   - DTMF Receiver Unavailable Answer Point Directory Number
3. Call Rerouting Always Alternative - Directory Number
4. Call Rerouting First Alternative - Directory Number
5. Call Rerouting Second Alternative - Directory Number
6. Hotel Options
   - Wake-Up Call - Expiration Routing
   - Wake-Up Call - Wake-Up Directory Number
7. Hunt Group - Hunt Group Member
8. Intercept Handling - any Directory Number field (14 in total)
9. Multiline Set Keys - Button Directory Number
10. Pickup Groups - Member
11. Remote Busy Lamps - Remote Host Set Directory Number
12. System Access Points
    - Night Bell Directory Number
    - MNMS: Event Indication Routing Number
    - MNMS: Event Indication Number
13. Telephone Directory - Number
14. Call Forwarding Profile - Forwarding Destination

3.10 Configure MiCollab Language

This page allows you to configure the following settings:

- **System Language**: Select the language of the Telephone User Interfaces (TUIs) for the MiCollab application end-users. End-users can also set their own prompt language on the Settings page of their MiCollab End User Portal. After the initial installation of a new system, the System Language defaults to US English.
- **NuPoint UM Prompt Languages**: Select the other languages for the NuPoint UM prompts. When users call into the NuPoint UM system through the Message Center auto attendant or Receptionist application, they are asked to select the language of the NuPoint UM prompts for the duration of their call. Users can select either the primary prompt language or one of the other languages. The primary (first) language is determined by the System Language setting above; the other languages are determined by the settings in these fields. For example, the primary system language could be English (United Kingdom); the second language; French (Canada), the third language Swedish (Sweden), and so on.

  You must record your corporate "Welcome" greeting in all the selected languages for incoming calls to the NuPoint UM system. When an external caller connects with the voice mail hunt group pilot number, the system plays your bilingual or multi-lingual corporate greeting and then prompts the caller to select the desired language. For example:

  System "Welcome" Greeting:"Welcome to Mitel Networks, Bienvenue à Mitel Networks".

  System Prompt: "For Service in English press 1; Pour le service en français, appuyez sur 2”.

  Users should also record their mailbox greetings in the required languages. When a caller reaches a user's mailbox, the system plays the mailbox greeting. For example:“You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message”.
- **Use NuPoint UM Mnemonic English Prompt**: When the System Language or Secondary NuPoint UM Prompt Language is set to English (United States), check this box if you want the NuPoint UM voice mail system to use English mnemonic prompts. By default, the system uses English numeric prompts.

Change System Language

To change the system language:

1. Under **Configuration**, click **MiCollab Language**.
2. Select the desired language from the **System Language** drop-down box.
3. If you set the system to use "English (United States)", you can choose to use numeric (default) or mnemonic prompts for NuPoint UM voice mail:

   - Check the **Use NuPoint Mnemonic English Prompt** box if you want the voice mail system to prompt users to enter letters to select actions. For example, "Press P to play";
   - Clear the box if you want the voice mail system to prompt users to enter numbers to select actions. For example "Press 7 to play".

Note:
The **Use NuPoint Mnemonic English Prompt** box is only presented if the NuPoint UM application is installed.

4. Click **Save**.

The following conditions apply to the System Language:

- The Line Group language setting and LCOS language setting use the MiCollab system default language. In the interface, the Line Group language setting is set to "undefined" and the LCOS language setting is set to "default". If you set the system language in the Line Group, it overrides the MiCollab system language setting and the MiCollab secondary NuPoint UM prompt language setting. Note that the LCOS language overrides the Line Group language and the MiCollab System language.
- The language of the Call Director application is not controlled by the system language setting.
- MiVoice Business phone displays are not controlled by the system language setting.
- For MiCollab Audio, Web and Video Conferencing , the Telephone User Interface language (TUI) is set on a system-wide basis for all users (that is, each user cannot set his or her own TUI language for MiCollab Audio, Web and Video Conferencing).
- The MiCollab End User Portal login page is displayed to the user in the language of the user's browser. If the browser language is not supported, the login page is displayed in the system language.
- The prompt language for call flows in Call Director default to the MiCollab language setting. However, users can set the prompt language for a call flow independently of the MiCollab language setting through the **Action** menu in the Call Director application.
- The System Language setting does not control the language used by the MiCollab End User Portal or Speech Auto Attendant application. The MiCollab Speech Auto Attendant only supports two languages: UK English and NA English. To change the Speech Auto Attendant language:

  1. Under **Applications**, click **NuPoint Web Console**.
  2. Under **Auto Attendant**, click **Misc. Parameters**.
  3. Select the desired **Primary Language**, and then click **Save**.
  4. Under **Auto Attendant**, click **Data Source**.
  5. Click **Force Update**.
- The **Use NuPoint Mnemonic English Prompt** box is displayed only when either System Language or Secondary NuPoint UM Prompt Language is set to English (United States).
- MiCollab Client supports additional languages that are not supported by MiCollab. However, MiCollab Client users can use these additional languages when MiCollab Client is deployed as an application on MiCollab , even though these languages are not supported by MiCollab .

Configure NuPoint UM Prompt Language

To configure a prompt language for the NuPoint UM system:

1. Ensure NuPoint UM FCOS feature bit 51 "Do Not Switch Languages for Outside Caller" is assigned to the users' voice mailboxes.
2. Under **Configuration**, click **Application Suite Language**.

3. Select the desired languages from the **NuPoint Prompt Language** drop-down box.
4. Record a bilingual or multilingual corporate greeting for the NuPoint UM system hunt group pilot number though the NuPoint UM administrator mailbox. Record the greeting in the "System Language" followed by the same greeting in the other selected languages; for example: “Welcome to Mitel Networks, Bienvenue à Mitel Networks; Bienvenido a Mitel Networks; Willkommen bei Mitel Networks”
5. Call into the NuPoint UM system hunt group pilot number and ensure that the prompts are played correctly.
6. Instruct mailbox users to record bilingual (or multilingual) greetings for their mailboxes as required. Again, users should record their mailbox greetings in the "System Language" followed by the same greeting in the other languages; for example: “You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message; Usted ha llegado al buzón de voz de Jean Julian , por favor deje un mensaje; Sie sind auf der Sprachmailbox von Jean Julian erreichen, hinterlassen Sie bitte eine Nachricht”.

The following conditions apply to the other NuPoint UM prompt languages:

- NuPoint UM FCOS feature bit 51 "Do Not Switch Languages for Outside Caller" must be assigned to the users' voice mailboxes.
- The NuPoint UM Line Group language setting and LCOS language setting use the MiCollab system default language. In the interface, the Line Group language setting is set to "undefined" and the LCOS language setting is set to "default". If you set the system language in the Line Group, it will override MiCollab system language setting and the MiCollab NuPoint UM prompt language.
- The "NuPoint Prompt Language" field is only displayed if NuPoint UM is installed.
- This prompt language feature does not apply to Speech Auto Attendant (SAA).

- Callers select the desired language for NuPoint prompts at the system-level only, not at the mailbox level.
- The system plays the languages in the order of the language choices. For example, if you selected the English as the "System Language" and then French, the system generated prompt plays: *"For service in English, press 1; Pour le service en français, appuyez sur 2."*
- This feature applies to calls to the NuPoint UM voice mail hunt group pilot number. The caller only selects the prompt language once, before the first system prompt is played.
- Mailbox owners are not prompted to select a prompt language when they log into their mailboxes.
- In MiCollab , the language selection prompts are system generated. MiCollab does not provide you with the ability to record and import a custom language selection prompt.
- An "SAA Warning" is displayed in the server manager interface if the "System Language" or one of the other language selections is not English.

About Network Elements 4

This chapter contains the following sections:

- Add or Edit Network Elements
- MiVoice Business Network Element Field Descriptions
- System Management Tool Access
- MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400 Network Element Field Descriptions

IMPORTANT: **Do not use this screen for MiCollab deployments using the Mitel MiVoice Business ICP. You must configure Network Elements in the MiCollab Users and Services application. You must also configure Network Elements before you configure line groups.**

Network Elements configuration must be done using the **Web Console**.

For standalone NuPoint UM, and for MiCollab deployments of NuPoint UM with the MiVoice Office 250 , you can use the Network Elements page of the NuPoint UM Web Console (only) to configure and manage various elements including multiple NuPoint servers, ICPs, and Digital Media Gateways (formerly PIMG/TIMG).

The local NuPoint UM server is automatically added to the Network Elements table and is identified by a padlock icon. The properties of the local server are configured at installation in the MSL server console so they are not configurable from the Network Elements page.

4.1 Add or Edit Network Elements

Overview

Use the Create Network Element page to perform the following tasks (System Administrator only):

- view a summary of current network elements
- add a new network element
- change existing ICP information
- reach through to the system administration tool of MiVoice Business elements or launch
- the management interface of a MiVoice 5000 element.

Note:
If an element's software version is not listed on this tab, the MiCollab system was unable to retrieve the version information from the element. To allow MiCollab to obtain the element software version from an MiVoice Business element, the "SNMP Read Only Community" field in the MiVoice Business SNMP Configuration form must be set to "Default".

Adding a Network Element

You cannot configure a mixture of MiVoice Business, MiVoice 5000, MiVoice Office 400 communications platforms, and MiVoice MX-ONE Service Nodes in the MiCollab network element page. The network elements must all be of the same type.

IMPORTANT: If you add a MiVoice Business server manually to this page, Flow Through Provisioning is not enabled. Although you can add phone services to users, the data is not shared. Sharing must be enabled from a MiVoice Business in the cluster.

Note:
You cannot modify the network element Type field. Therefore, if you add an element with the incorrect network element Type, for example if you add a MiVoice Business element when you intended to add a MiVoice 5000 element, you must delete the incorrect element and then add it correctly.

Note:
Do not create a network element when provisioning users on MiVoice Office 250.

To add a network element:

1. On the **Network Element** tab, click **Add**.
2. Complete the network element fields for the MiVoice Business, MiVoice 5000, MiVoice MX-ONE Service Node, or MiVoice Office 400.

Note:
The **Network Element Type** lists all the available PBXs. You must choose the PBX type you specified in the **Install Applications** tab while configuring the server.

1. If you are adding the first network element to the list, you are prompted to associate the element with the default UCC templates. If you select **Yes**, the network element field for the primary phone in the default templates is automatically set to the name of this network element. If you select **No**, you must create custom templates and associate them with this element.
2. Click **Save**.

3. If you are adding a MiVoice Business network element, you must enter the MiVoice Business System login credentials in the **Credentials** field. If the credentials are incorrect, PBX synchronization from MiCollab Client Service will not work, and the MiTAI Authentication in MiCollab Client and NuPoint Unified Messaging does not work.

Note:
MiTAI authentication is supported on MiVoice Business release 9.0 and later. It is recommended to turn OFF the authentication for earlier releases of primary and secondary MiVoice Business versions.

1. If you are adding a MiVoice 5000 or MiVoice MX-ONE Service Node, you must also
   - add the network element within the NuPoint Unified Messenger application, and
   - add the network element as a SIP Server in the MiCollab Audio, Web and Video application.
2. If you are adding a MiVoice Office 400 network element, you must also configure the network element as a SIP Server in the MiCollab Audio, Web and Video application.

Note:
By default, the first network element added to the form will be noted as the default SIP ICP for Teleworker service.

Editing a Network Element

1. On the **Network Element** tab, select the element to edit.
2. Click **Edit** or click the System Name link.
3. When edits are complete, click **Save**.
4. If you are editing a MiVoice 5000 or MiVoice MX-ONE service node, you must also
   - modify the network element within the NuPoint Unified Messenger application, and
   - modify the network element as a SIP Server in the MiCollab Audio, Web and Video application.
5. If you are modifying a MiVoice Office 400 network element, you must also modify the network element as a SIP Server in the MiCollab Audio, Web and Video application.

Deleting a Network Element

Delete any users and services that are associated with the network element from the MiCollab Users and Services directory.

1. On the **Network Element** tab, select the element(s) to delete.

2. Click **Delete**. A confirmation message appears.
3. Click one of the following:

   - **Yes**: deletes the selected, currently active network element.
   - **No**: skips the currently selected network element and moves to the next selected element, if applicable.
   - **Yes to All**: deletes all network elements after, and including, the currently selected element.
   - **Close**: closes the dialog without deleting.

Note:
If you are deleting a MiVoice 5000 or MiVoice MX-ONE service node that is associated with a custom template, then the template is also deleted.

4. If you are deleting a MiVoice 5000 or MiVoice MX-ONE service node, you must also
   - delete network element within the NuPoint Unified Messenger application, and
   - delete the SIP Server network element from the MiCollab Audio, Web and Video application.
5. If you are deleting a MiVoice Office 400 element, you must also delete the SIP Server network element in the MiCollab Audio, Web and Video application.

Note:
Deleting network elements from the MiCollab server does not automatically delete the associated application programming (for example, line groups and ports) that are provisioned on the communications platform.

4.2 MiVoice Business Network Element Field Descriptions

Field	Description	Values
Type	Select the PBX type. Mandatory.	MiVoice Business, MiVoice 5000, MiVoice MX-ONE Service Node, or MiVoice Office 400. **Note**: The MiVoice Business system identifies a MiCollab Server as Type "MSL Server" in the system administration tool.
System Name	Enter the unique network element name. For example, "MiVB3". Mandatory. This field is read-only for the local MiCollab Server network element.	Enter a unique name of between two and eight characters in length for the network element. The name can consist of alphanumeric and certain special characters. Spaces are not allowed.
IP Address	Enter the IP address of the network element. Mandatory. This field is read-only for the local MiCollab Server network element	Mandatory. Standard IP address notation of four sets of one to three digits separated by periods. For example, 192.168.0.1
Zone	Enter a number to identify the Network Zone. The MiVoice Business platform uses Network Zones • for compression and bandwidth management • to associate the zones to time zones for the display of local time on IP sets • to configure the zone's Location Based Number (LBN) prefix for Location Base Call Routing (optional), and • to define the zone's CESID (optional).	Number from 1 to 999. Default is blank. If this field is left blank, the MiVoice Business defaults this setting to Zone 1.

Field	Description	Values
FQDN	Enter a Fully Qualified Domain Name for the MiVoice Business network element. Optional. **Note**: For MiVoice Business FQDN to work, the host file must have the FQDN entry in MiCollab.	Optional

Network Element Settings

Field	Description	Values
SIP Conference FAC:	If MiCollab Client is in integrated mode, this field defines the Feature Access Code that MiCollab Client users dial to establish a 3-party conference. If MiCollab Client is in integrated mode, the system copies the code from this field to the PBX Node details page of the MiCollab Client Service. If MiCollab Client is in co-located mode, this field is not used and you must enter the code in the PBX Node details page. This field is not shared via Flow Through Provisioning.	Default is *40. Limit of 16 telephony characters (0-9, *, #)

Credentials

Field	Description	Values
System Login	Enter the MiVoice Business System Administration Tool Login ID. This field is mandatory.	Up to 20 alphanumeric characters. Must be a valid Login ID for a MiVoice Business user profile with Application access.

Field	Description	Values
Password	Enter the password associated with the MiVoice Business System Administration Tool Login ID. This field is mandatory.	MiVoice Business password. **Note**: Ensure that you enter the MiVoice Business System Login and Password correctly. If either are incorrect, the users will be unable to use the telephony services or change their Telephone User Interface (TUI) passcodes, and the MiTAI Authentication in MiCollab Client and NuPoint Unified Messaging will not work.
Confirm Password	Re-enter the password to confirm.	

System Properties

Note:
If you create a new MiVoice Business network element in the MiVoice Business cluster and start sharing it with MiCollab, you must add the element's Set Registration Code and Set Replacement Code in these fields, because SDS does not share them with MiCollab.

Field	Description	Values
Set Registration Code	Enter an access code to register a new IP telephone into the system. The access code consists of digits to add at the beginning of a PIN when registering an IP telephone.	May be 3 to 10 digits in length, including * or # (for example: ###). Cannot be the same as Set Replacement Code.
Set Replacement Code	Enter an access code to override an already registered IP telephone. The access code consists of digits to add at the beginning of a PIN when registering an IP telephone.	May be 3 to 10 digits in length, including * or # (for example: ***). Cannot be the same as Set Registration Code.

Field	Description	Values
Voice mail server type	Click on **NuPoint** or **EMEM** radio button to select the required server type and then save the **Network Element Settings**. **Note**: If a **Voice mail server type** is selected and the Network Element is saved, then the **Voice mail server type** cannot be changed. For EMEM feature to work, ensure that: • MiVoice Business is configured with **EMEM**. Refer to *Program the MiVoice Business Embedded Voice Mail* section in *MiVoice Business - System Administration Tool Online Help* • MiVoice Business is configured with **FQDN** instead of an IP address under **Controller Registry** in **System Administration Tool**. For more information, refer to *Controller Registry* section in *MiVoice Business - System Administration Tool Online Help*. • MiVoice Border Gateway is configured with **MiVB Embedded Visual Voice Mail** LAN Server using **Split DNS** under **Remote Proxy**. For more information, refer to *Configure LAN Servers on the Web Proxy* section in *MiVoice Border Gateway - Installation and Maintenance Guide*. To release **NuPoint**, click on **Release Licenses** checkbox and save the settings. **CAUTION**: If the **NuPoint** license is released, even then the **Voice mail server type** cannot be configured as **EMEM**.	If **NuPoint** is configured, then: • In MiCollab Server, under **MiCollab Client Service** > **Configure MiCollab Client Service** > **Enterprise** > **Settings** > **Voice mail server type**, the server type is automatically updated and cannot be changed. • In MiVoice Business, under **Users and Devices** > **User and Service Configuration**, a **Add voicemail** option is created for the Administrator to configure Voicemail for the user under **Deskphone**. If **EMEM** is configured, then: • In MiCollab Server, under **Users and Services** > **Users** tab, **NuPoint Unified Messaging service** would not be displayed and there will be no services displayed for **EMEM**. • In MiCollab Server, under **Users and Services** > **User Templates** > **Add New User Template** and **Edit User Template**, **Include EMEM VoiceMail Service** and **Forward to Email** are enabled. For the **Forward to Email** feature to work in MiCollab Server, ensure that MiVoice Business is configured with **Forward Voice Mail to E-Mail**. For more information, refer to *Forward Voice Mail to E-Mail* section in *MiVoice Business - System Administration Tool Online Help*. • In MiCollab Server, under **MiCollab Client Service** > **Configure MiCollab Client Service** > **Enterprise** > **Settings** > **Voice mail server type**, the server type is automatically updated and cannot be changed. • In MiVoice Business, under **Users and Devices** > **User and Service Configuration**, a **Voicemail** is configured automatically for the user under **Deskphone**.

Field	Description	Values
Use NuPoint UM IP Integration Licenses This checkbox will be displayed only if **NuPoint** server is selected.	You must activate this change in the NuPoint UM application from the activation link at the top of the page. **Note**: You can have maximum of 4 IP integration licenses in one MiCollab. One license comes integrated with the UCC licensing and three licenses need to be purchased separately from the AMC.	If **NuPoint** server is selected, select the **Use NuPoint UM IP Integration Licenses** checkbox. After you click **Save**, the Network Element (ICP) is configured in the NuPoint UM application. If **EMEM** server is selected, then **Use NuPoint UM IP Integration Licenses** checkbox is not displayed.

Application Data

Voicemail

Field	Description	Values
Call Reroute First Alternative (CRFA) Number **(On-premise deployments only)**	This setting allows you to configure call rerouting for devices at the system level. Enter the CRFA index number for call rerouting. Ensure that a destination extension (for example, voice mail hunt group number) is programmed against the index number in the Call Reroute First Alternative form of the MiVoice Business platform.	Number from 1 to 336 digits in length. When you create a phone with a mailbox, or add a mailbox to an existing phone, the system automatically applies the CRFA programming to the device. **Note**: Prior to MiCollab Release 6.0, Call Forwarding was used to direct calls to the voice mail hunt group number. Call Forwarding takes precedence over CRFA. Defaults to Call Reroute First Alternative index number 2 with the voice mail hunt group number set to extension 7000.
Call Forward Destination Directory Number **(On-premise deployments only)**	Enter the NP-UM voice mail hunt group number to be used by MiCollab Client.	7-digit number maximum. (Default applied by MiCW is 7000).
HCI Reroute Hunt Group Number for MiTai MWI **(On-premise deployments only)**	Enter the hunt group number for the HCI Reroute Hunt Group. (This hunt group is used to enable MWI lamp on stations with mailboxes via the MiTAI application interface).	7-digit number maximum. (Default applied by MiCW is 6400).

Field	Description	Values
Voicemail HuntGroup Number (MiCloud Flex deployments only)	Enter the voicemail hunt group number created on the MiVoice Business portal. After the Initial Configuration Wizard (ICW) is complete (in **Flex Solution Manager**), the administrator must add the voicemail hunt group number manually on the MiCollab portal.	

Speech Auto Attendant

Field	Description	Values
Pilot/Access Number	Enter the pilot number of the Speech Auto Attendant (SAA). This number is listed in the Welcome E-mail that the system sends to new users. For MiVoice Business systems, enter the "Speech Auto Attendant" Hunt Group directory number that is listed in the Telephone Directory form of the System Administration Tool. **Note**: MiCollab does not verify that the entered number is a valid entry in the MiVoice Business database. **Note**: This field is only present if the SAA application is licensed and installed on MiCollab.	7-digit number maximum. (Default applied by MiCW is 6800).

4.3 System Management Tool Access

Accessing a MiVoice Business System Administration Tool

To reach through to the MiVoice Business System Administration Tool interface from the MiCollab server:

1. Click the **Network Element** tab.

Note:
Elements that are sharing data with the MiCollab system have the following icon next to the element name:  and a  appears in the Sharing column. You can only reach through to elements that are sharing.

2. Click **Connect to MiVB System Tool.**The MiVoice Business System Administration Tool login interface opens in a new window.
3. Close the window to return to the MiCollab server.

Note:
When Flow Through Provisioning (Sharing) is enabled for MiVoice Business elements, changes made to the MiCollab user and phone services data are also updated in the MiVoice Business databases. In addition, changes made in the MiVoice Business database are propagated back to the MiCollab database. Flow Through Provisioning is only supported for MiVoice Business elements.

Accessing the MiVoice 5000 Management Interface

To access the MiVoice 5000 management interface from the MiCollab server:

1. Click the **Network Element** tab.
2. Click **Connect to AMB.**The MiVoice Business System management login interface opens in a new window.
3. Log into the management interface.
4. Close the window to return to the MiCollab server.

Note:
Access to the MiVoice 5000 Manager (AM7450) and MiVoice MX-ONE management interfaces are not supported from the Network Element page.

4.4 MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400 Network Element Field Descriptions

Field	Description	Values
Type	Select network element type required. Mandatory.	MiVoice Business, MiVoice 5000 , MiVoice MX-ONE Service Node, or MiVoice Office 400.
System Name	Enter the unique network element name. For example, "MiV5000_3". Mandatory. This field is read-only for the local MiCollab Server network element.	Enter a unique name of between two and 64 characters in length for the network element. The name can consist of alphanumeric and certain special characters. Spaces are allowed.

Field	Description	Values
IP Address	Enter the IP address of the network element. Mandatory. This field is read-only for the local MiCollab Server network element. **Note**: For most MiVoice MX-ONE deployments, without SNM Redundancy, enter the IP address or FQDN of LIM1 (this will be the alias IP address of LIM1, if MX-ONE Service Node redundancy is in use). MX-ONE Service Node Manager Redundancy does not influence this setting in MiCollab, but in Provisioning Manager Subsystem, the SNM alias Address should be used. Optionally it is possible to configure further Network Elements referring to other LIMs – might be one Network Element for each LIM or selected number of LIMs. In this case it is needed to create User Templates/ Roles for each Network Element. When assigning for a user in MiCollab Configuration in MX-ONE Provisioning Manager, the Provisioning Manager will try to fetch from MiCollab a Role which has configured as Network Element the LIM IP where the user's extension is initiated. If there is no Role configured with Network Element for this LIM, the Provisioning Manager will try to fetch the Role having Network Element with LIM1 IP. If none of this match, no Role will be shown in Provisioning Manager's MiCollab Configuration.	Standard IP address notation of four sets of one to three digits separated by periods. For example, 192.168.0.1
Zone	Enter a number to identify the Network Zone.	Number from 1 to 999. Default is blank.
FQDN	Enter a Fully Qualified Domain Name for the network element.	Optional

Field	Description	Values
Outgoing Dialing Prefix	Enter the outgoing dialing prefix to be used by MiCollab Client.	Enter a number up to 32 digits in length. Valid digits are 0 to 9. This field is optional.
Call Forward Destination Directory Number	Enter the NP-UM voice mail number to be used by MiCollab Client.	10-digit number maximum.
Call Take FAC	This field defines the Feature Access Code that MiCollab Client users dial on a device to which they want to shift an ongoing call from another device and continue the call without interruption. The system copies the code from this field to the PBX Node details page of the MiCollab Client Service. **Note**: This FAC does not apply to MiVoice Office 250 platform.	MiVoice 5000 default is #70. MiVoice MX-ONE default is *8#. MiVoice Office 400 default is blank. Limit of 16 telephony characters (0-9, *, #)
SIP Conference FAC:	This field defines the Feature Access Code that MiCollab Client users dial to establish a 3-party conference. The system copies the code from this field to the PBX Node details page of the MiCollab Client Service. **Note**: This FAC does not apply to MiVoice Office 250 or MiVoice Office 400 platforms. A FAC is not used to establish 3-party conferences on these communication platforms.	MiVoice 5000 default is *40. MiVoice MX-ONE default is 3. Limit of 16 telephony characters (0-9, *, #)

UCC Licensing 5

This chapter contains the following sections:

- UCC License Bundle Definitions
- Manage MiVoice Business Subscription Ed.02 Licensing Bundles

Unified Communications & Collaboration (UCC) licensing simplifies the selling and ordering process because it bundles the platform and application user licenses together. Instead of ordering a MiCollab license or multiple individual applications licenses for each user, you just order a single UCC license per user. Although you can order licenses individually (“à la carte”) we recommend that you use UCC licensing because it offers the following benefits:

- simplifies the licensing of a MiCollab user by bundling a MiVoice Business user license with a specific set of application user licenses
- offers a significant pricing discount over “à la carte” licenses
- provides tiered functionality with progressive discounts.

The following UCC user bundles are available:

- UCC Basic - Not a purchasable user bundle
- UCC Entry license
- UCC Standard license

Note:
You use *Enterprise* UCC V4.0 licenses with all MiCollab Release 7.0 and later systems.

UCC Licensing Rules

The following rules apply to UCC Licensing:

- UCC V4.0 licensing is supported with MiCollab Release 7.0 and above. Providing that you have active Software Assurance, all earlier UCC licenses are automatically converted to UCC V4.0 licenses during an upgrade to Release 7.0. The MiCollab server only updates the users' license bundles with the new service entitlements. It does not automatically assign new services to the user. After an upgrade, you must update the services for each user. If your system had UCC V2.0 or V3.0 licenses that were converted to UCC V4.0 licenses, it is recommended that you assign the newly converted bundles to the same users who were previously using the UCC V2 or V3 licenses.
- After licenses have been converted, you update the users' MiCollab Client Profiles using the Edit User functionality. New users are provisioned based on UCC V4 template definitions available on the system after the upgrade to MiCollab 7.0.
- UCC licensing is not supported for standalone applications and MiVoice Office 250 systems.
- Hardware (controllers, phones), base system software, service provider interconnect licenses, and certain system options remain separately purchasable licenses.
- “à la carte” licenses remain available. Installed platform user licenses can be converted to the UCC Basic designation (process depends on the Call Manager that MiCollab is deployed against). This change facilitates upgrades to Entry or Standard bundles.

- You can add UCC licenses to an existing MiCollab system. UCC licensing can be applied to a system that has existing "à la carte" licenses.
- There is no migration of existing "à la carte" licenses to UCC licenses.
- MiCollab licenses in the UCC license bundle can only be applied to one MiCollab application record in the AMC.
- In the SLS license server, the UCC group license manager (ULM) option does not exist.
- You cannot split a UCC license bundle and deploy the application licenses across different users within a system. Nor can you split a UCC license bundle across multiple MiCollab systems that have the same user.
- Only add phone and applications services from USP. Do not add them from the application interfaces. This could result in license violations.
- When a UCC license bundle is assigned to a user, all the services provided in that bundle are consumed by that user, even if the services are not configured.
- When you configure a new user with a UCC license bundle, MiCollab fully configures the user's phones and groups on the MiVoice Business (if Flow Through Provisioning is enabled). However, if you change a bundle for a user, you may be required to update the user's ring group programming on the MiVoice Business. When MiCollab is deployed with a MiVoice 5000 or MiVoice MX-ONE, the administrator provisions MiCollab users with licenses from the call manager administrator interface by assigning a role to the user.
- If all the available UCC license bundles for a specific bundle type (Basic, Entry, or Standard) are in use, you will receive an error message if you attempt to assign another one of those license bundles (that is, you cannot assign a bundle to a user if the in-use bundle count is already equal to the licensed bundle count). The system displays licensing information in the server-manager interface under **Applications** on the **Licensing Information** page.
- **For MiVoice Business integrations**: If you downgrade the UCC license bundle of an existing user (for example, from Entry to Basic, or from Standard to Entry) from the USP application, the system will not delete any of the services. Instead, MiCollab attempts to apply any available "al la carte" licenses to support the extra services. If "à la carte" licenses are not available, then a license violation is generated.
- **For MiVoice 5000 or MiVoice MX-ONE integrations**: If you downgrade the UCC license bundle of an existing user (for example, from Entry to Basic, or from Standard to Entry from the platform's call manager interface, the user's services are reduced to those supported by the lower licensing level. To upgrade the UCC license bundle of an existing user, you must delete the user and then recreate the user with the higher level UCC license from the management platform.
- If you have different types of upgrade licenses (for example, "Basic to Entry" and "Entry to Standard") available on the system, apply for the highest upgrade licenses first. For example, upgrade the Entry users to Standard licenses first, before you upgrade the Basic users to Entry licenses.
- To use the MBG Teleworker licenses that are included in the UCC Standard License, the MiCollab and MBG servers must be clustered. Refer to the MiCollab Installation and Maintenance Guide for instructions.
- During all deployments, two Teleworker phones, that is the primary phone and the other phone will be enabled in the default UCC Standard template. Old users created with this template would not be impacted, but the new users which are created from the Standard template would have Teleworker phones created by default.

UCC License Bundle Definitions

There are three tiers of UCC licensing: Basic, Entry, and Standard.

UCC license bundles map to default UCC roles and templates. To assign a UCC license bundle to a user, you assign the associated default role to the user. The role references a default user template that applies the licensing to the user.

The following table lists the licenses included in each tier. Refer to the *MiCollab Licensing Guide* for the latest information.

Note:
The licensing definitions in the following table are subject to change.

Licenses included	UCC Licenses		
	Basic (only applicable to MiVoice Business)	**Entry (Note 1)**	**Standard (Note 1)**
MiVoice Business user license only	Entitles user to MiCollab Basic Client	No	No
MiVoice Business multi-device user licenses (Not applicable to MiVoice 5000 or MiVoice MX-ONE)	No	Yes (Multi-device user group up to 8 devices)	Yes (Multi-device user group up to 8 devices)
MiVoice 5000 or MiVoice MX-ONE multi-device user licenses (Not applicable to MiVoice Business)	No	Yes (Multi-device user group up to 2 devices)	Yes (Multi-device user group up to 4 devices)
NuPoint mailbox license with call director (See **Note 3**)	No	Yes	Yes
Standard and Advanced UM license	No	Yes	Yes
MiCollab Desktop Client with Instant Messaging Presence	No	Yes Also includes full presence capability (IM, Voice, Video) and Dynamic Status (see **Note 8**)	Yes Also includes full presence capability and Dynamic Status

Licenses included	UCC Licenses		
	Basic (only applicable to MiVoice Business)	Entry (Note 1)	Standard (Note 1)
MiCollab Web Client with Instant Messaging Presence	Yes	Yes Also includes full presence capability (IM, Voice, Video) and Dynamic Status (see **Note 8**)	Yes Also includes full presence capability and Dynamic Status
MiCollab Audio, Web and Video Conferencing audio and collaboration access	No	No	Yes
MBG Teleworker license, MiCollab Client MiNET, and SIP softphone license	No	No (see **Note 4**)	Yes
MiCollab Client deskphone license	No	No	Yes
MiCollab Client web license (see **Note 1**)	Yes (Basic features only)	Yes (Entry features only)	Yes
MiCollab Client softphone license (see **Note 1**)	No	No	Yes
MiCollab Client Mobile SIP for Softphone	No	No (See **Note 5**)	Yes (See **Note 6**)
MiTeam Classic	No	No	Yes (See **Note 7**)
MiTeam Meetings	No	Yes	Yes

Note 1: With an additional MiVoice Business user licence, you can configure a UCC Entry user with a Multi-device User Group.

Note 2: Basic and Entry licenses also include the MiCollab Client desktop and web client with just the Instant Messaging Presence feature. Entry licenses provide IM and Voice presence. Standard licenses provide MiCollab Client desktop and web client with full MiCollab Client feature functionality.

Note 3: With UCC V4.0 and later licensing, new versions of the Entry and Standard licenses, specific to MiVoice MX-ONE platforms, are available. These licenses are for users with MiCollab Advanced Messaging (AVST) mailboxes. Separate roles and user templates are also provided. The new roles and templates are only available with MiVoice MX-ONE UCC licenses on newly licensed platforms. The new templates do not have the NuPoint Voicemail box enabled. Platforms that already have UCC V4.0 licensing are not updated with the new roles and templates.

Note 4: Optional license PN54006550 adds MiCollab Client Mobile functionality to an Entry bundle.

Note 5: Optional license PN54006551 adds MiCollab Client Softphone functionality to an Entry bundle.

Note 6: A Standard license provides video functionality. Vidyo provides higher resolution video as well as some advanced features. Vidyo and MiCollab integration also requires the Vidyo Portal API License PN5130264.

Note 7: Refer to the *MiCollab Client Administration Guide* for Classic Streams configuration.

Note 8: UCC Entry users who have Legacy MiCollab Desktop Client R7.3 can view their Dynamic Status but cannot manage their Dynamic Status. UCC Entry users who have MiCollab for PC Client R8.0 and later can view and manage their Dynamic Status.

Upgrading a UCC Licensed User to the Next Bundle Level

You can upgrade an existing UCC licensed user to a higher level license by changing the UCC licensing bundle in the User tab. For example, you could upgrade a user from Basic to Standard. After you upgrade, the existing UCC Standard licensing count increases by one license and the UCC Basic Licensing count decreases by one license. After you upgrade the license, you must assign the additional services to the user.

Note:
The following procedures assume that the UCC licensed services have not been modified (for example, by the addition of "à la carte" licenses or the deletion of services).

Note:
If you have different types of upgrade licenses (for example, "Basic to Entry" and "Entry to Standard") available on the system, apply the highest upgrade licenses first. Upgrade the Entry users to Standard licenses, before you upgrade the Basic users to Entry licenses.

The different types of upgrades that can be performed on licenses are:

- Upgrade from Entry to Standard
- Upgrade from Basic to Standard
- Upgrade from Basic to Entry

Upgrade from Entry to Standard

1. In the Users and Services page, select the user and click **Edit**.
2. In the **User** tab, set the UCC Bundle field to UCC Standard User (for Enterprise) and click **Save**.
3. In the **MiCollab Client** tab, assign one of the phones as a Desk phone extension and assign the other as a Soft phone extension. Note that the Soft phone extension must be assigned with a device type of UCA Endpoint, App Server Port, or a SIP phone device type in the **Phones** tab.
4. In the **Teleworker** tab, click **Add Teleworker Service** and select the Deskphone or Softphone extension.
5. In the **MiCollab Client** tab, enter the Desk phone and Softphone extensions and set the Feature Profile to "UCC (Vx.0) Standard".
6. In the **Audio, Web and Conferencing** tab, click **Add Service** and select the Desk phone extension.
7. Reach through to the MiVoice Business and change the user's group programming from Multi-device Group - "External Twin" to "Standard".

Note:
The Standard bundle supports MiTeam.

Upgrade from Basic to Standard

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the UCC Bundle field to UCC Standard User (Enterprise) and click **Save**.
3. In the **Phones** tab, add up to eight phones with Service Levels set to "Multi-device". Enable one phone with an "External Hot Desk License". The other phones must have "External Hot Desk License" disabled. In the **MiCollab Client** tab, assign one of the phones as a Desk phone extension and the other as a Soft phone extension. Note that the Soft phone extension must be assigned with a device type of UCA Endpoint, App Server Port, or a SIP phone device type in the **Phones** tab.

4. In the **NuPoint Unified Messaging** tab, click **Add New Mailbox**, set the Feature COS field to 14 and check one or both of the Standard and Advanced Unified Messaging boxes. Enable 3300 Record-A-Call if applicable.
5. In the **Teleworker** tab, click **Add Teleworker Service** and select the Deskphone or Softphone extension.
6. In the **MiCollab Client** tab, enter the Soft phone extension and set the Feature Profile to "UCC (Vx.0) Standard".
7. Reach through to the MiVoice Business and configure the user's group programming to use Multi-device Group - "Standard".

Upgrade from Basic to Entry

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the UCC Bundle field to UCC Entry User (Enterprise) and click **Save**.
3. In the **Phones** tab, add up to eight phones with Service Levels set to "Multi-device". Enable one phone with an "External Hot Desk License". In the **MiCollab Client** tab, assign another phone as a Desk phone extension.
4. In the **Phones** tab, add up to eight phones with Service Levels set to "Multi-device". Enable one phone with an "External Hot Desk License". In the **MiCollab Client** tab, assign the other phone as a Desk phone extension.
5. In the **MiCollab Client** tab, enter the softphone extension and set the Feature Profile to "UCC (vx.0) Entry".
6. Reach through to the MiVoice Business and configure the user's group programming to use Multi-device Group - "External Twin".

Downgrading a UCC Licensed User

You can downgrade an existing UCC licensed user to a lower level by changing the UCC licensing bundle in the User tab. For example, you could downgrade a user from Standard to Basic. After you downgrade, the existing UCC Basic licensing count increases by one license and the UCC Standard Licensing count decreases by one license. After you downgrade a license, you must delete the unlicensed services from the user.

Note:
The following procedures assume that the UCC licensed services have not been modified (for example, by the addition of "à la carte" licenses or the deletion of services).

Note:
In MiCollab Release 7.0 and later, you manage a user's Multi-Device User Group from the MiVoice Business system administration tool. If you downgrade a user, you may need to modify or delete the user's multi-device user group on the MiVoice Business.

Downgrade from Entry

To downgrade a user from Entry to Basic:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the UCC Bundle field to UCC Basic User (Enterprise) and click **Save**.
3. In the **Phones** tab, click **Delete Phone** and select the External Hot Desk User extension.
4. In the **NuPoint Unified Messaging** tab, click **Delete Mailbox** to the delete the mailbox.
5. If applicable, reach through to the MiVoice Business and delete the Multi-Device User - Standard group.

Downgrades From Standard

To downgrade a user from Standard to Basic:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the UCC Bundle field to UCC Basic User (Enterprise) and click **Save**.
3. In the **Phones** tab, delete the Soft phone (see the **MiCollab Client** tab to identify the Soft phone extension). Delete the External Hot Desk User extension.
4. In the **NuPoint Unified Messaging** tab, click **Delete Mailbox** to delete the mailbox.
5. In the **MiCollab Client** tab, set the Feature Profile to "UCC (Vx.0) Basic".
6. In the **Audio, Web and Conferencing** tab, click **Delete Service**
7. In the **Teleworker** tab, delete the **Teleworker** if present.

To downgrade a user from Standard to Entry:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the UCC Bundle field to UCC Entry User (Business or Enterprise) and click **Save**.
3. In the **Phones** tab, delete the Soft phone (see the **MiCollab Client** tab to identify the Soft phone extension).
4. In the **MiCollab Client** tab, set the Feature Profile to "UCC (Vx.0) Entry". Remove the MiCollab Client Desk phone or Soft phone if it is not required.
5. In the **Audio, Web and Conferencing** tab, click **Delete Service**.
6. In the **Teleworker** tab, delete the **Teleworker** if present.

Swapping UCC Bundles Between Two Users

If you have available licenses, you can simply change the UCC licensing bundles of both users. However, if your system does not have any available licenses.

1. Set the license bundle of one user to <None>.
2. Apply the available license to the other user. This action makes the previously assigned license available.
3. Apply the available license to the currently unlicensed user.
4. Adjust the services for both users (see upgrading and downgrading UCC bundle procedures above).

Configuring Existing MiVoice Business UCC Basic Users on MiCollab

If Flow Through Provisioning is Enabled

If Flow Through Provisioning is enabled, the MiCollab directory will be populated with the MiVoice Business users and their phone services. In this case, you just need to enable the applications for the users from the Users and Services application.

If Flow Through Provisioning is NOT Enabled

If you have configured UCC Basic users on MiVoice Business that are not configured in the MiCollab database (that is, the phone users were only configured on the MiVoice Business system), you can add these users to the MiCollab Users and Services application using the following procedure

1. Log into the MiVoice Business System Administration Tool.
2. Access the User and Device Configuration form.
3. Use the sort functionality to display a listing of the UCC Basic Users.
4. Export the user and device information into a CSV file.
5. Create copies of the Basic User template for the different device types.
6. Assign the templates to roles. See Manage Roles.
7. Copy the communication platform user data from the exported CSV file into the import file spreadsheet columns of the Bulk User Provisioning tool and include role (see Bulk Import from File).
8. Import the CSV file data.

Range Programming MiCollab Client Profiles

If UCC licenses are converted (for example from V2 to V3) during an upgrade, you must assign the new services to the users. If the users' MiCollab Client Profiles require updating, you can use range programming to complete this task:

1. In the MiCollab server manager, under **Applications**, click **MiCollab Client Service**.
2. Click **Configure MiCollab Client Service**.
3. Click the **Features** tab.
4. Click the "People" icon of the feature profile that you want to apply, for example: (UCC V3 Standard).
5. Click the **Add Members** link and select the users that you want to apply this feature profile to.
6. Click **Add to Profile** at the bottom of the page. You return to the "Feature Profile Members" page.
7. Click **Save**. A bar displays the progress.
8. When the profiles are updated, click **Done**.

Identifying UCC License Usage

If MiCollab is configured in Integrated Mode, you can identify the types of UCC licenses that are assigned to each user through the MiCollab Client administration interface:

1. In the MiCollab server manager, under **Applications**, click **MiCollab Client Service**.
2. Click **Configure MiCollab Client Service**.
3. Click the **Features** tab.
4. Select the default "Entry" or "Standard" default feature profile.
5. Click the "Edit profile members" button  to see which users are currently using the selected profile.

5.1 UCC License Bundle Definitions

There are three tiers of UCC licensing: Basic, Entry, and Standard.

UCC license bundles map to default UCC roles and templates. To assign a UCC license bundle to a user, you assign the associated default role to the user. The role references a default user template that applies the licensing to the user.

The following table lists the licenses included in each tier. Refer to the *MiCollab Licensing Guide* for the latest information.

Note:
The licensing definitions in the following table are subject to change.

Licenses included	UCC Licenses		
	Basic (only applicable to MiVoice Business)	Entry (Note 1)	Standard (Note 1)
MiVoice Business user license only	Entitles user to MiCollab Basic Client	No	No
MiVoice Business multi-device user licenses (Not applicable to MiVoice 5000 or MiVoice MX-ONE)	No	Yes (Multi-device user group up to 8 devices)	Yes (Multi-device user group up to 8 devices)
MiVoice 5000 or MiVoice MX-ONE multi-device user licenses (Not applicable to MiVoice Business)	No	Yes (Multi-device user group up to 2 devices)	Yes (Multi-device user group up to 4 devices)
NuPoint mailbox license with call director (See **Note 3**)	No	Yes	Yes
Standard and Advanced UM license	No	Yes	Yes

Licenses included	UCC Licenses		
	Basic (only applicable to MiVoice Business)	Entry (Note 1)	Standard (Note 1)
MiCollab Desktop Client with Instant Messaging Presence	No	Yes Also includes full presence capability (IM, Voice, Video) and Dynamic Status (see **Note 8**)	Yes Also includes full presence capability and Dynamic Status
MiCollab Web Client with Instant Messaging Presence	Yes	Yes Also includes full presence capability (IM, Voice, Video) and Dynamic Status (see **Note 8**)	Yes Also includes full presence capability and Dynamic Status
MiCollab Audio, Web and Video Conferencing audio and collaboration access	No	No	Yes
MBG Teleworker license, MiCollab Client MiNET, and SIP softphone license	No	No (see **Note 4**)	Yes
MiCollab Client deskphone license	No	No	Yes
MiCollab Client web license (seeNote 1)	Yes (Basic features only)	Yes (Entry features only)	Yes
MiCollab Client softphone license (see Note 1)	No	No	Yes
MiCollab Client Mobile SIP for Softphone	No	No (See **Note 5**)	Yes (See **Note 6**)
MiTeam Classic	No	No	Yes (See **Note 7**)

Licenses included	UCC Licenses		
	Basic (only applicable to MiVoice Business)	Entry (Note 1)	Standard (Note 1)
MiTeam Meetings	No	Yes	Yes

Note 1: With an additional MiVoice Business user licence, you can configure a UCC Entry user with a Multi-device User Group.

Note 2: Basic and Entry licenses also include the MiCollab Client desktop and web client with just the Instant Messaging Presence feature. Entry licenses provide IM and Voice presence. Standard licenses provide MiCollab Client desktop and web client with full MiCollab Client feature functionality.

Note 3: With UCC V4.0 and later licensing, new versions of the Entry and Standard licenses, specific to MiVoice MX-ONE platforms, are available. These licenses are for users with MiCollab Advanced Messaging (AVST) mailboxes. Separate roles and user templates are also provided. The new roles and templates are only available with MiVoice MX-ONE UCC licenses on newly licensed platforms. The new templates do not have the NuPoint Voicemail box enabled. Platforms that already have UCC V4.0 licensing are not updated with the new roles and templates.

Note 4: Optional license PN54006550 adds MiCollab Client Mobile functionality to an Entry bundle.

Note 5: Optional license PN54006551 adds MiCollab Client Softphone functionality to an Entry bundle.

Note 6: A Standard license provides video functionality. Vidyo provides higher resolution video as well as some advanced features. Vidyo and MiCollab integration also requires the Vidyo Portal API License PN5130264.

Note 7: Refer to the *MiCollab Client Administration Guide* for Classic Streams configuration.

Note 8: UCC Entry users who have Legacy MiCollab Desktop Client R7.3 can view their Dynamic Status but cannot manage their Dynamic Status. UCC Entry users who have MiCollab for PC Client R8.0 and later can view and manage their Dynamic Status.

5.2 Manage MiVoice Business Subscription Ed.02 Licensing Bundles

Note:
This topic does not apply to MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400 communication platforms. For these communication platforms, you provision MiCollab users with licenses from the call manager administrator interface by assigning roles to the users.

This topic covers the following tasks:

- Assigning MiVoice Business Subscription Ed.02 Licensing Bundles on page 67

- Removing MiVoice Business Subscription Ed.02 Licensing Bundles on page 69

Note:
Templates are only applied during the creation of new users. If you apply a MiVoice Business Subscription license bundle to an existing user, upgrade a user's license bundle, or swap user bundles, you must manually assign the phone and application services.

Assigning MiVoice Business Subscription Ed.02 Licensing Bundles

You can assign MiVB Subscription Ed. 02 licensing bundles:

- directly to an existing user entry from the **User License Bundle** field in the **User** tab
- by applying one of the default roles when you create a new user with Quick Add or Bulk User Provisioning.
- by adding custom templates that specify a MiVoice Business Subscription licensing bundle (Entry, Elite CX, Premium, or Telephony) and then using Quick Add or Bulk User Provisioning to apply the template during the creation of new users.

Note:
If all the available MiVoice Business Subscription license bundles for a specific bundle type (Entry, Elite CX, Premium, or Telephony) are in use, you will receive a licensing violation message if you attempt to assign another one of those license bundles (that is, you cannot assign a bundle to a user if the in-use bundle count is already equal to the licensed bundle count). The system displays the number of "available" user licenses and the number "currently used" in the server-manager interface under **Applications** on the **Licensing Information** page.

Note:
In MiCollab Release 7.0 and later, you manage a user's Multi-Device User Group from the MiVoice Business system administration tool.

Assign MiVB Telephony Bundle

To assign a user who currently has no bundle with the MiVB Telephony bundle:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the User License Bundle field to MiVB Telephony (Ed.2) and click **Save**.

3. In the **Phones** tab, add one phone with **Service Label** set to *Full*. Enable one phone with an *External Hot Desk License*.
4. In the **MiCollab Client** tab, set the Feature Profile to **MiVB Telephony (Ed.2)**.
5. In the **NuPoint Unified Messaging** tab, click **Add New Mailbox**. Set the Feature COS field to 14 and check one or both Standard and Advanced Unified Messaging boxes. Enable 3300 Record-A-Call if applicable.

If EMEM is configured, and for the EMEM feature to work, refer to *Program the MiVoice Business Embedded VoiceMail section in MiVoice Business -System Administration Tool Online Help*. More details on EMEM can be referred from the System Properties table under MiVoice Business Network Element Field Descriptions on page 43.

Assign MiVB Entry Bundle

To assign a user, who currently has no bundle, with the MiVb Entry bundle:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the User License Bundle field to MiVB Entry (Ed.2) and click **Save**.
3. In the **Teleworker** tab, click **Add Teleworker Service** and select the Deskphone or Softphone extension.
4. In the **Phones** tab, add up to three phones with Service Levels set to "Multi-device". In the **MiCollab Client** tab, assign another phone as a Desk phone extension and the other as a Softphone extension. Note that the Softphone extension must be assigned with a device type of UC Endpoint, App Server Port, or a SIP phone device in the **Phones** tab.
5. In the **NuPoint Unified Messaging** tab, click **Add New Mailbox.** Set the Feature COS field to 14 and check one or both Standard and Advanced Unified Messaging boxes. Enable 3300 Record-A-Call if applicable.

   If EMEM is configured, and for the EMEM feature to work, refer to *Program the MiVoice Business Embedded VoiceMail section in MiVoice Business -System Administration Tool Online Help*. More details on EMEM can be referred from the System Properties table under MiVoice Business Network Element Field Descriptions on page 43.
6. In the **MiCollab Client** tab, set the Feature Profile to **MiVB Entry (Ed.2)**.
7. Log in in MiVoice Business and configure the user in a Multi-device Group type *Entry*.

Assign MiVB Premier Bundle

To assign a user, who currently has no license, with the MiVB Premier bundle:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the User License Bundle field to MiVB Premium (Ed.2) and click **Save**.
3. In the **Phones** tab, add up to three phones with Service Levels set to "Multi-device". In the **MiCollab Client** tab, assign another phone as a Desk phone extension and the other as a Softphone extension. Note that the Softphone extension must be assigned with a device type of UC Endpoint, App Server Port, or a SIP phone device in the **Phones** tab.

4. In the **NuPoint Unified Messaging** tab, click **Add New Mailbox**. Set the Feature COS field to 14 and check one or both Standard and Advanced Unified Messaging boxes. Enable 3300 Record-A-Call if applicable.

   If EMEM is configured, and for the EMEM feature to work, refer to *Program the MiVoice Business Embedded VoiceMail section in MiVoice Business -System Administration Tool Online Help*. More details on EMEM can be referred from the System Properties table under MiVoice Business Network Element Field Descriptions on page 43.
5. From the **User License Bundle** dropdown field, set the license bundle to **MiVB Premium (Ed.2)**.
6. In the **Audio, Web and Conferencing** tab, click **Add Service** and select the Desk phone extension.
7. In the **Teleworker** tab, click **Add New Teleworker** and select the Deskphone or Softphone extension.
8. Reach through to the MiVoice Business and configure the user in a Multi-device Group of type "Premium".

Assign MiVB Elite CX Bundle

To assign a user, who currently has no license, with the MiVB Elite CX bundle:

1. In the Users and Services directory, select the user and click **Edit**.
2. In the **User** tab, set the User License Bundle field to MiVB Elite CX (Ed.2) and click **Save**.
3. In the **Phones** tab, add up to three phones with Service Levels set to "Multi-device". In the **MiCollab Client** tab, assign another phones as a Desk phone extension and the other as a Softphone extension. Note that the Soft phone extension must be assigned with a device type of UC Endpoint, App Server Port, or a SIP phone device in the **Phones** tab.
4. In the **NuPoint Unified Messaging** tab, click **Add New Mailbox**. Set the Feature COS field to 14 and check one or both of the Standard and Advanced Unified Messaging boxes. Enable 3300 Record-A-Call if applicable.
5. In the **MiCollab Client** tab, set the Feature Profile to **MiVB Elite CX (Ed.2)**.
6. In the **Audio, Web and Conferencing** tab, click **Add Service** and select the Desk phone extension.
7. In the **Teleworker** tab, click **Add New Teleworker** and select the Deskphone or Softphone extension.
8. Reach through to the MiVoice Business and configure the user in a Multi-device Group of type "Elite CX".

Removing MiVoice Business Subscription Ed.02 Licensing Bundles

To remove a MiVoice Business Subscription licensing bundle from a user, set the User License Bundle field in the User tab to blank. After you set the license bundle to blank, delete the phones from the user. When you delete a phone, the services associated with that phone are also deleted.

Upgrading a MiVB Subscription Licensed User to the Next Bundle Level

You can upgrade an existing UCC licensed user to a higher level license by changing the UCC licensing bundle in the User tab. For example, you could upgrade a user from MiVB Telephony to MiVB Entry bundle.

The different types of upgrades that can be performed on MiVB Subscription Licenses are:

- Upgrade from MiVB Entry (Ed.02) to MiVB Telephony (Ed.02) license bundle
- Upgrade from MiVB Telephony (Ed.02) to MiVB Entry (Ed.02) license bundle
- Upgrade from MiVB Telephony (Ed.02) to MiVB Elite CX (Ed.02)/MiVB Premiere (Ed.02) license bundle

- Upgrade from MiVB Entry (Ed.02) to MiVB Elite CX (Ed.02)/MiVB Premiere (Ed.02) license bundle
- Upgrade from MiVB Elite CX (Ed.02)/MiVB Premiere (Ed.02) to MiVB Telephony (Ed.02)

Upgrade from MiVB Entry (Ed.02) to MiVB Telephony (Ed.02) license bundle

1. In the Users and Services tab, select the user and click **Edit**.
2. In the **User** tab, set the **User License Bundle** to MiVB Telephony (Ed. 2) bundle and click **Save**.
3. In the **MiCollab Client** tab, enter the Deskphone extension and set the **Feature Profile** to *Default Feature Profile*.
4. Reach through to the MiVoice Business and change the user's group programming from Multi-device Group - *External Twin* to *Standard*.

Upgrade from MiVB Telephony (Ed.02) to MiVB Entry (Ed.02) license bundle

1. In the Users and Services tab, select the user and click **Edit**.
2. In the User tab, set the User License Bundle to MiVB Entry (Ed. 2) bundle and click **Save**.
3. In the **MiCollab Client** tab, assign the Deskphone and Softphone extension and set the **Feature Profile** to MiVB Entry (Ed. 2).
4. In the **Audio, Web and Conferencing** tab, click **Add Service** and select the Desk phone extension

Upgrade from MiVB Telephony (Ed.02) to MiVB Elite CX (Ed.02)/MiVB Premiere (Ed.02) license bundle

1. In the **Users and Services** tab, select the user and click **Edit**.
2. In the **User** tab, set the **User License Bundle** to *MiVB Entry (Ed. 2)* bundle and click **Save**.
3. In the **MiCollab Client** tab, enter the Deskphone and Softphone extensions and set the **Feature Profile** to *MiVB Elite CX (Ed. 2)*/ *MiVB Premier (Ed. 2)*.
4. In the **Audio, Web and Conferencing** tab, click **Add Service** and select the Deskphone extension.

Upgrade from MiVB Entry (Ed.02) to MiVB Elite CX (Ed.02)/MiVB Premiere (Ed.02) license bundle

1. In the **Users and Services** page, select the user and click **Edit.**
2. In the **User** tab, set the **User License Bundle** to *MiVB Elite CX (Ed. 2)*/ *MiVB Premier (Ed. 2)* bundle and click **Save**.
3. In the **MiCollab Client** tab, enter the Deskphone and Softphone extensions and set the **Feature Profile** to *MiVB Elite CX (Ed. 2)*/ *MiVB Premier (Ed. 2)*.
4. In the **Audio, Web and Conferencing** tab, click **Add Service** and select the Deskphone extension.

Upgrade from MiVB Elite CX (Ed.02)/MiVB Premiere (Ed.02) to MiVB Telephony (Ed.02)

1. In the **Users and Services** page, select the user and click **Edit**.
2. In the **User** tab, set the **User License Bundle** to *MiVB Telephony (Ed. 2)* bundle and click **Save**.

3. In the **MiCollab Client** tab, enter the Deskphone extension and set the **Feature Profile** to *Default Feature Profile.*
4. In the **Audio, Web and Conferencing** tab, delete AWV services from the user.
5. Reach through to the MiVoice Business and change the user's group programming from Multi-device Group - "External Twin" to "Standard".

About Roles and Templates 6

This chapter contains the following sections:

- Default Roles and Templates
- Guidelines for Using Templates
- Manage User Templates
- Enter Template Information for UCC Licensing
- Manage Roles
- Apply Roles
- Template Migration

6.1 Default Roles and Templates

The system includes default Roles and Templates for

- applying UCC Licensing
- synchronizing Active Directory entries with the MiCollab database.

You can also create your own custom templates by clicking **Add** in the **User Templates** tab. Modify the fields in the blank template to create a custom template.

UCC User and Services Default Roles and Templates

You can use the default UCC Roles and Templates to apply UCC licenses to your users.

UCC license bundles, by default, map to the default UCC Roles and Templates listed in the following table. Default UCC Roles and Templates are only created for UCC licenses that are installed on the system. To assign a UCC license bundle to a user, you assign the associated default role to the user. The default role references a default template that applies the licensing to the user.

UCC Licenses	Default Roles	Default Templates
UCC Entry User for Enterprise	UCC (Vx.0) Entry	UCC (Vx.0) Entry
	UCC (Vx.0) Entry (Nupoint)	UCC (Vx.0) Entry (Nupoint)
	UCC (Vx.0) Entry (Advanced Messaging)	UCC (Vx.0) Entry (Advanced Messaging)
UCC Standard for Enterprise	UCC (Vx.0) Standard	UCC (Vx.0) Standard

Note:
MiCollab Advanced Messaging applies to MiVoice MX-ONE only.

The Default UCC templates assign the following functionality.

Default UCC Users and Services Template (Enterprise)	Template Contents	Functionality provided
UCC (Vx.0) Entry	1 User	UCC license bundle set to "UCC Entry User for Enterprise (Vx.0)"
	2 Phones	Primary Phone: Desk Phone Secondary Phone: EHDU Phone
	Include Group	Multi-device - Standard user group license (up to 8 devices for MiVoice Business ; up to two devices for MiVoice 5000 or MiVoice MX-ONE) Prime phone is pilot number of group Include Secondary phone as group member
	Include MiCollab Client Service	Feature Profile: UCC (Vx.0) Entry Desk phone extension: None Soft phone extension: None Deployment Profile: Do Not Deploy MiTeam Meetings

Default UCC Users and Services Template (Enterprise)	Template Contents	Functionality provided
	1 NuPoint Mailbox OR 1 MiCollab Advanced Messaging (AVST) mailbox	NuPoint mailbox license with Call Director and Standard & Advanced UM licensing OR MiCollab Advanced Messaging (AVST) mailbox
UCC (Vx.0) Standard	1 User	UCC license bundle set to "UCC Standard User for Enterprise (Vx.0"
	3 Phones	Primary Phone: Desk Phone Secondary Phone: EHDU Phone Other Phone: Soft Phone
	Include Group	Multi-device - Standard user group license (up to 8 devices for MiVoice Business ; up to two devices for MiVoice 5000 or MiVoice MX-ONE) Prime phone is pilot number of group Include Secondary phone as group member Include Other phone as group member
	Include MiCollab Client Service	Feature Profile: UCC (Vx.0) Standard Desk phone extension: Primary Soft phone extension: Other Deployment Profile: Do Not Deploy MiTeam Meetings

Default UCC Users and Services Template (Enterprise)	Template Contents	Functionality provided
	1 NuPoint Mailbox OR 1 MiCollab Advanced Messaging (AVST) mailbox	NuPoint mailbox license with Call Director and Standard & Advanced UM licensing OR MiCollab Advanced Messaging (AVST) mailbox
	2 Teleworker	Teleworker Service available for two phones, that is the primary phone and the other phone
	Include Audio, Web and Video Conferencing	Access for primary phone

Note:

MiCollab Advanced Messaging (AVST) licensing applies to MiVoice MX-ONE only.

Default Roles and Templates for Active Directory Entries

Role	Template	Purpose
Contact ð	MiCollab Client Contact ð	Configures Active Directory entries that are synchronized via MiCollab IDS as non-corporate contacts in the MiCollab Client database. The templates contains the user information and applies the MiCollab Client Default Feature Profile without any desk phone extension or soft phone extension.

Role	Template	Purpose
Teamwork Mode User	MiCollab Client Teamwork Mode User	Configures Active Directory entries that are synchronized via MiCollab IDS as Teamwork Mode users in the MiCollab Client database. The templates contains the user information and applies the MiCollab Client Default Feature Profile without any desk phone extension or soft phone extension. It also applies a default password of "default" and a default pass code of "1111" to the Teamwork Mode user.

Default Roles and Templates for SIP Softphone Users

Role	Template	Purpose
HotDesk SIP Softphone User	HotDesk SIP Softphone User	The template contains the user information and applies SIP softphone capability for hot desking users along with Teleworker service.

6.2 Guidelines for Using Templates

The follow guidelines apply when you are using templates:

- A template can include up to three phones: Primary Phone, Secondary Phone, and Other Phone. If you attempt to add a fourth phone you will receive the following error *This template is not valid on MiCollab: "Composite template contains more than three phone templates." and the template will become invalid. You cannot recover the template by simply deleting the fourth phone. You must delete the template and recreate it.
- There must be a primary phone configured in the user template. By default, the first phone that you add to a user template is designated as the prime phone.
- A template can contain up to two standard numeric (non-derived) directory numbers. The Primary Phone must have a standard directory number.
- The Secondary Phone and Other Phone can derive their directory numbers from the prime directory number. It's recommended that you assign a prime desktop phone in the template and derive the directory numbers of any additional phone devices from the prime phone directory number. Derived directory numbers are typically used to add user devices, such as cell phones into Personal Ring Groups or Multi-Device User Groups.
- Application service sub-sections (for example NuPoint Mailbox Number) that contain references to directory numbers must refer to a standard (non-derived) number. The only exception to this rule is the MiCollab Client application which supports both a deskphone and a softphone. One of these devices in the MiCollab Client sub-section can reference a derived directory number. The other must reference a standard numeric directory number.
- For phone key templates, the system does not validate the keys during template creation. The keys are only validated after you create a user from the role/template that includes the key template. If the key entries are invalid, the user cannot be saved. Ensure that you test phone key templates in the MiVoice

Business system administration tool against test users to ensure that the key templates are valid before you use them from MiCollab USP.

- If you modify a MiCollab template for a MiVoice Business or MiVoice MX-One system, the existing users are not changed if you reassign the MiCollab role to the user. The modifications are not automatically applied.
- If you modify a template for a MiVoice 5000 system, the changes to the template are applied to existing users on the next scheduled MiVoice 50000 synchronization with the MiCollab system.
- For MiCollab with MiVoice MX-One deployments, roles are associated with the MX-One Service Node Manager. When you create a user from the Provisioning Manager, you can only select roles that are associated with the user's Service Node Manager.
- For MiVoice Office 400 deployments, the following conditions apply:
  - Quick Add of a user is supported with any combination of services but at most one phone.
  - Quick Add of a user where the template includes MBG will cause an MBG SIP service to be created.
  - The **Add User** button in the Phone and Teleworker tab is disabled or hidden.
  - Add or delete of an existing user's AWV service is supported.
  - Modification of user, phone or any of the services is supported.
  - MiCollab Client feature profile can be changed.
  - Password changes are sent to the MBG for the teleworker service.
  - Client deployment of the softphone takes place when the profile is set during quick add or when user, phone or service details are updated.

6.3 Manage User Templates

User templates allow you to define a common set of phone and application services that you can then apply to new users. Each template consists of sub-sections for the user profile, phones, and services. For example, you could add a user template for a "Sales" role. This template would include a specific set of phone features and applications, such as External Hot Desk User, and Mitel Collaboration Advanced, to help salespeople sell product more effectively.

If your site requires custom templates we recommend that you create them by copying and editing the UCC Default Templates. These templates enable the functionality provided by the associated UCC licensing bundle.

Note:
The Flow Through Provisioning feature shares MiVoice Business templates with the MiCollab system. The MiVoice Business templates support key template programming for users created from MiCollab USP. However, when a key template is created on the MiVoice Business system, the template is not validated for incomplete key programming (such as a missing ring type in a DSS/BLF key). The system only generates errors when you attempt to apply the invalid key template to a user via a role. Therefore, whenever you create a new key template on the MiVoice Business, ensure that you test it by applying it to a MiVoice Business user. If you receive errors related to key programming when you attempt to apply a shared template, you must correct the key template on the MiVoice Business.

Note:
MiCollab users can be configured with multiple phones and each phone extension consumes a device (Multi-Device User Group device) on the MiVoice Business system. On enterprise MiCollab systems, it is possible to exceed the device limits of the MiVoice Business system(s). To minimize the possibility of over provisioning, do not assign users with unnecessary phones. Also, during initial bulk provisioning of an enterprise MiCollab system, create roles and templates that assign the actual phone requirements for the users.

Note:
If a user is configured as a Basic MiCollab Desktop Client user, Mitel recommends configuring one desk phone or one desk phone and EHDU device.

Note:
You cannot delete services from the UCC Default Templates.

Note:
You cannot re-apply a role to reset a users settings back to the template values.

Note:
After an upgrade from MiCollab Release 6.0 to MiCollab Release 7.0, the AMC will update the system with the UCC V4.0 Default Templates. However, it can take up to 12 hours before the system re-syncs with the AMC and downloads the new templates. To obtain the templates sooner, access the **Servicelink > Status** screen in the server manager and perform a **Sync** with the AMC.

Note:
On upgrade to MiCollab Release 7.2.2 or later, any existing templates that have the SIP Teleworker service and the user password set to "Same as Primary Phone Extension" are modified to have "Randomly Generate" as the password option.

To View the User Templates

1. Under **Applications**, click **Users and Services**.

2. Click **User Templates**.

To Add New User Templates

1. Click **Add**.
2. Enter a label for the new template.
3. Enter a description.
4. Enter the template information.

> **Note**:
> To support Messaging Waiting on MiVoice 5000 or MiVoice MX-ONE phones, the Messaging Waiting fields in the NuPoint Unified Messaging section of the template must be set to "DTMF-to-PBX".

5. Click **Save**.

To Edit the User Templates

Editing a user template has the following effects:

- **MiVoice Business** and **MiVoice MX-ONE**: Editing a template has no effect on users that were previously created using that template. Changes to a template are not applied automatically to existing users who are assigned with the associated role. You must reassign the role to an existing user to apply the template changes.
- **MiVoice 5000**: Changes to the template are applied to existing users who are assigned with the associated role on the next MiVoice 5000 synchronization with the MiCollab system.

To edit a template:

1. Check the box next to the template name and click **Edit**. The Edit Role and User Service Template window opens.
2. Enter the template information. If you change the UCC bundle type in a non-default UCC User and Service template, the system overwrites the template with a clone of the selected default UCC bundle. If you change the UCC license bundle type to "None", the template field information is not altered, but any users you create from this template will use "a la carte" licenses.
3. Click **Save**.

Copy

You can copy an existing template and then modify it to create a similar but different template:

1. Check the box next to the template that you want to copy and click **Edit**. The template opens.
2. Click **Copy**. The system creates a copy of the template.
3. Enter a label and description for the new template.

4. Modify the template fields as required.
5. Click **Save**.

Delete

Editing a user template has the following effects:

- **MiVoice Business**: Deleting a template has no effect on users who were created using that template.
- **MiVoice MX-ONE**: Deleting a template has no effect on users who were created using that template. However, removing the role from a user from the MX-ONE management interface deletes the user from the MiCollab USP database.
- **MiVoice 5000**: Changes to the template are applied to existing users who are assigned with the associated role on the next MiVoice 5000 synchronization with the MiCollab system.

You cannot delete a template if it currently references a role. You cannot delete the Default User and Service templates.

1. Click **User Roles** and delete any roles that are assigned to the template.
2. Click **User Templates**.
3. Check the box next to the template name and click **Delete**.
4. Click **Yes** to confirm the delete.
5. Click **Close**.

6.4 Enter Template Information for UCC Licensing

Note:
Fields that are not supported for the MiVoice 5000 , MiVoice MX-ONE or MiVoice Office 400 network elements are disabled (for example: Include Secondary Phone, Other Phone, and Group Type fields).

User Template

Field	Description	Values
Label	Enter reference name for this template (for Administrator use). This field is mandatory.	Between 1 and 64 characters. This field supports UTF-8 characters.
Description	Enter a description for this template	

User Information

Field	Description	Values
UCC Bundle	Select the UCC License bundle to apply to the users created with this template. Select <none> if you intend to use "a la carte" licensing.	Select one of the following: ********** ********** • <none> ********** ********** • UCC Entry User for Enterprise • UCC Standard User for Enterprise ********** ********** Default is <none>.
Department	Select the department where this template will place users from the drop-down menu. Optional.	Default is <none>.
Location	Select the location where this template will place users from the drop-down menu. Optional.	Default is <none>.

Field	Description	Values
Prompt Language	Select the language for the user's voice services (Telephone User Interfaces). The changes take affect immediately after you click **Save**. Active TUI sessions remain in the previous language until the next login session. **Note**: This setting changes all TUIs belonging to the user to the new language, with the exception of the Mitel Collaboration Advanced (MiCollab Audio, Web and Video Conferencing) application. This setting is not applied to the MiCollab Audio, Web and Video Conferencing TUI. The MiCollab Audio, Web and Video Conferencing TUI uses the System Default Language.	System Default. By default, the prompt language uses the System Default Language that is set from the server manager. To set the System Default Language, under **Configuration**, click **MiCollab Language**. Then, select the desired language from the **Language** drop-down box.
Password	Select one of the following options (mandatory): • **Same as Primary Phone Extension** to set the user's password to the user's extension number. • **Randomly Generate** to have the system generate a random password for the user. Note that the random password is masked for security. • **Use this value** to set the default password to the value specified.	4- 20 characters Manual passwords must contain at least four alphanumeric characters. It does not support the following special characters: "**| ;& !**" characters. If the Service Information E-mail feature is configured for the system, whenever you create or change a user's password, an e-mail is sent to the user with the password.

Field	Description	Values
TUI Passcode	Select one of the following options to set the user's TUI passcode (including Hot Desk User Login PIN): • **Same as Primary Phone Extension** to set the user's passcode to the user's extension number. • **Randomly Generate** to have the system generate a random passcode for the user. Note that the random passcode is masked for security. • **Use this value** to set the default passcode to the value specified.	4 to 8 telephony digits (*, #, 0-9) Manual passcodes must contain at least four numeric digits.
IDS-Manageable	Specifies that all the IDS managed fields (for example, First Name, Last Name, Department, Location, Email, and Login) for this user are managed from an Integrated Directory Service (IDS) server.	This option is enabled by default. If an IDS server is integrated with MiCollab , updates to specific user fields in the directory service record are applied to the corresponding MiCollab record fields. Updates are applied during the next synchronization event. If you clear the check box, updates made on the directory server are not applied to the MiCollab user entry. If a directory server is not integrated with the MiCollab system, this option is still enabled by default but it has no effect on the MiCollab system database.

Service Information

Click the check boxes next to the services that you want to include and complete the fields using the information from the following table:

Primary Phone

Field	Description	Values

Include Primary Phone	When the "Include Primary Phone" service check box is not selected, the following conditions apply:
	• You must specify a password and passcode in the "Use this value" field of the User Information section
	• The following options are not available:
	  • Secondary phone
	  • Other phone
	  • Group
	  • Speech Auto Attendant
		Default is unchecked.

Service Label.	Enter a name of up to 64 characters that identifies the service (for example, Desk Phone). The same label can be used for more than one service associated with the same user.	Up to 64 characters.
Network Element	Select an ICP from the Network Element list	Select the name of a MiVoice Business , MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400 element from the list. OR Select <blank> if the Network Element is a MiVoice Office 250 . **Note**: This selection is not available if an ICP host has already been added as a Network Element.)

Field	Description	Values
Secondary Element	For resiliency, select the phone's Secondary Element from the list. If the phone's primary Network Element goes out of service, the phone is supported by the specified Secondary Element.	The selected element must be different than the Network Element above.
Use DID Service Number as Outgoing DID Number	Check this box to display the DID number for outgoing calls made from the user's phone. The MiVoice Business CPN Substitution feature allows you to program a substitute number for outgoing calls made on a DID trunk. The substitute number is presented to the network for outgoing calls on the DID trunk.	Unchecked
CESID	Enter the Caller Emergency Service Identification (CESID) to be sent to the Public Safety Answering Point (PSAP) in the event of an emergency call. Up to 12 digits can be programmed. **Note**: Although a CESID can be programmed for any mobile DN, the system will only use it for External Hot Desk Users (EHDUs) that are logged on to private trunks. For regular hot desk users and EHDUs logged on to MiNET devices, the system will use the CESID associated with the set's registration DN.	Between 1 and 12 digits in length. Can contain digits 0 to 9. Default is blank.
Hot Desking User	Check to create a Hot Desking user; clear to create a standard user and device. **Note**: • Hot Desking User type requires COS entries.	Not selected.

Field	Description	Values
	• When you assign a newly created user as a Hot Desking User, the ACD Agent field is disabled. If required, select the ACD Agent field to create an ACD Agent with hot desking capability.	

Field	Description	Values
	• After a user has been assigned with the ACD Agent option, you cannot change this option using **Edit**. You must delete the phone and then add it again to change the ACD Agent option.	
ACD Agent	Check to designate a hot desking user as a Hot Desk ACD Agent. **Note**: • To enable this option, you must first select the Hot Desking User box.	Not selected.

Field	Description	Values
	• After a user has been assigned with the ACD Agent option, you cannot change this option using **Edit**. You must delete the phone and then add it again to change the ACD Agent option.	
Enable SIP Softphone for MiCollab Client	Check box to enable SIP Softphone functionality for a hot desking user. When you enable this functionality, **Enable SIP Softphone for MiCollab Client** MiCollab Client Service assigns the phone type as SOFTPHONE and Device Type as 76. **Note**: You can apply Teleworker service to a Hot Desking user with SIP Softphone enabled.	Not selected.
External Hot Desk License	Check box to enable External Hot Desk User (EHDU) functionality. The Device Type field must be set to Hot Desk User. External Hot Desk Users must be licensed. Licenses are programmed in the License and Option Selection form of the MiVoice Business . **Note**: You cannot apply the Teleworker service to an EDHU.	

Field	Description	Values
Hot Desk User External Dialing Prefix	Enter "9" or other prefix digit(s) required to dial out to the external hot desk device.	1 to 26 telephony digits, 0 to 9, * or #.
Preferred Set	For a hot desking user, select the user's preferred hot desking device type from the drop down list. This field only appears if the Hot Desk User option is enabled below. If No Device is selected as the Preferred Device, the device is assigned 96 keys by default.	No Device

Device Type	Select a device from the Device Type list.	The following rule applies: • You cannot edit device type for Generic SIP Device types that have Teleworker services assigned. • This field is not available if "Hot Desking User" is checked. • Enter a device type of "UC Endpoint" for MiCollab Client clients. • The following MiVoice Business Device Types are not supported: Analog, Analog-FXS, 5001 IP, 5201 IP, 5401 IP, NetVision IP, Spectralink NetLink, and Superset Devices. • This field does not apply to the MiVoice Office 250 .

Include Teleworker Service	Click to add Teleworker service to this user template.	The following conditions apply: • Default is unchecked. • This field does not apply to the MiVoice Office 250 . • Teleworker service can be added to multiple devices for a user. • When you include Teleworker service for a user's SIP phone, the system automatically configures a corresponding SIP service on the MiVoice Border Gateway. Note the following: • • The system sets the **Set-side username** on the MiVoice Border Gateway to <username-DN> (for example smithj-7328). This username format applies to MiVoice Business communication platforms only. • The password field in the User Information section of the template must be set to a strong password or "Randomly Generate".
SIP Device Capabilities	When Generic SIP Device type is selected, this field defaults to 1. When UC Endpoint is selected (for a MiCollab Client Deskphone or Softphone) this field defaults to 71.	Change the Default SIP Device Capabilities number as required.
SIP Password	Enter a SIP device password for the user. When you create or change a user's SIP password, the system automatically sends a Service Info Email with the password to the user. **Note**: The display on 5505 SIP and 5302 IP sets is limited to eight digits. For these sets, assign a numeric password of eight digits or less.	Up to 26 ASCII characters including numeric, alphanumeric, and special characters. Default is blank. This field is only enabled for SIP devices. SIP device passwords are optional. If this field is left blank, a password is not required to register a SIP device with the MiVoice Business .

Confirm SIP Password	Re-enter the passcode to confirm.	

Service Level	Displays the level of service for this directory number (DN): **Full** - A DN with this service level is assigned to a standard user and device with full telephony service. **IP Device Only** - A DN with this service level is assigned to an unlicensed device that has only basic telephony functionality (emergency or attendant calls). The device becomes functional when a hot desk user or hot desk ACD agent logs into it. **Trusted** - A DN with this service level is assigned to a trusted Mitel application that has full telephony service once it registers with the system. Although the DN can be programmed on the same forms as a Full Service DN, it does not use an IP User License. **Multi-Device** - A DN with this service level is assigned to a user that has only basic telephony functionality (emergency or attendant calls) until programmed as a member of a Multi-device User Group. Multi-Device User Groups (MDUGs) allow a single user to have multiple phones grouped under a common directory number without each phone requiring a full MiVoice Business IP License. There are two types of Multi-Device User Groups: • *Standard:* allows up to eight phones to be grouped under a common directory number. Only the prime number requires an IP User License. The group itself, requires a MDUG license. In a MDUG, phone functionality is essentially limited to one device in the group at any given time. When one of the user's phones is engaged in call, the other phones are consider busy (in other words, "One Busy All Busy" is always enabled) and have restricted functionality.	Full Service

	• *External Twin:* allows only two phones, typically a desk phone and a cell phone, to be twinned. This type of group does not require a MDUG license. It only requires an IP User License and an External Hot Desk User license. The prime number uses the IP User license. The second member must be an External Hot Desk number and consumes the EHDU license. **Note**: For SIP softphone, the Service Level should always be set to Multi-device.	
Zone ID	Enter a number to identify the Network Zone. The MiVoice Business platform uses Network Zones • for compression and bandwidth management • to associate the zones to time zones for the display of local time on IP sets • to configure the zone's Location Based Number (LBN) prefix for Location Base Call Routing (optional), and • to define the zone's CESID (optional).	Number from 1 to 999. Default is blank. If this field is left blank, the MiVoice Business defaults this setting to Zone 1.

Call Coverage Service Number	Assign the Call Coverage Service Number Call for the MiVoice Business Hot Desk PIN Security feature. The MiVoice BusinessHot Desk PIN Security feature ensures that all hot desk users create strong (resistant to guessing) PINs by forcing them to create PINs that adhere to a set of strengthening rules. Hot Desk PIN Security is programmed in the Call Coverage Services form of the MiVoice Business System Administration Tool. This form allows you to assign a Call Coverage Service number that uniquely identifies the type of Call Coverage Service. The number that you enter in this field must exist in the Call Coverage Service form on the MiVoice Business system. If Flow Through Provisioning is enabled, the phone's Call Coverage number is automatically updated on the MiVoice Business system. **Note**: This field only applies to MiVoice Business Release 6.0 or later systems.	This field only applies to Mitel IP phones. If you create a new phone, this field defaults to 1. If you upgrade an existing MiCollab system to MiCollab Release 4.0 SP2 or later, this field also defaults to 1. To have the system automatically assign a specific Call Coverage Number use the **System Managed** option (see below).

Deployment Profile	Select a profile for MiCollab for Mobile Client softphone or EHDU deployment: • **default**: Default profile • **Do Not Deploy**: The client will not be deployed. • **Status**: "Un-deployed" indicates that the client is not deployed. "Deployed" indicates that the configuration has been sent to the client but has not yet been downloaded. "Downloaded" indicates that the configuration has been downloaded and installed for the client. **Note**: This field only appears if MiCollab Client is integrated mode.	This field applies only if the Preferred Set is UC Endpoint, or if Enable SIP Softphone or EHDU is selected, and the MiCollab Client Deployment application is installed. For "UC Endpoint" devices: • Default profile is selected by default. • If you upgrade the MiCollab Client for Mobile application, the default profile is applied to all eligible phones. • If you are upgrading and you do not wish to use the MiCollab Client for Mobile application, change this setting from default to **Do Not Deploy**. For EHDUs: • For External Hot Desk Users, the default profile is set in the MiCollab Settings page. For SIP Softphones; • Default profile is selected by default • If you do not wish to use the MiCollab Client for Mobile application, change this setting from default to **Do Not Deploy**. **Note**: If there is no phone for which a deployment profile is selected, users need to provide their password every time they log in to PC and Mobile Clients.

Deployment Profile continued		**Note**: If a phone with a deployment profile is added later, the user must provide their password for every login to PC and Mobile Clients. However, if the administrator or the user changes the password after the user logs in, the updated password is automatically used for the next login to PC and Mobile Clients. **Note**: If a user is deployed from the MiCollab Client Service page, the Client will prompt for the password. This scenario occurs because the password is not set from MiCollab Server in the deployment configuration for the user. MiCollab Server will not have the password in clear text during the deployment.

Send Deployment Email	If this option is checked, a deployment email is sent to the user when you deploy a MiCollab for Mobile Client softphone from the Users and Services directory page; if unchecked, it is not sent. The deployment email provides users with a QR code. After scanning the QR code with their mobile phone, the user is authenticated, and the MiCollab for Mobile Client application is downloaded from the App Store to the user's phone. If you are only deploying a softphone to a user's web client (WebRTC client), then it is not necessary to send a deployment email.	This option is only available if the device type is set to "UC Endpoint". Default is checked (send deployment email).
Class of Service - Day	Enter a COS number for Day mode.	Number from 1 to 110. Defaults are blank. If you are integrating MiCollab with a MiVoice Business system enter COS 13 for users without the Record-a-Call feature; enter COS 14 for users with the Record-a-Call feature.
Class of Service - Night 1	Enter a COS number for Night 1 mode.	
Class of Service - Night 2	Enter a COS number for Night 2 mode.	
Class of Restriction - Day	Enter a COR number for Day mode.	
Class of Restriction - Night 1	Enter a COR number for Night 1 mode of service.	
Class of Restriction - Night 2	Enter a COR number for Night 2 mode of service.	

Secondary Phone (Optional)

Field	Description	Values
Include Secondary Phone	Click to set up a secondary phone for this user template. This option is only available if the Include Prime Phone box is checked.	Default is unchecked. Can be set to the same values available for Primary Phone.
Derive DN	Check this box if you want to derive the phone number from the primary phone directory number. It's recommended that you assign users with a prime phone and then derive the directory number of any additional phones from the prime phone directory number.	The system derives the directory number of this phone by inserting an*between the 1st and 2nd digits of the primary directory number. For example, if the Primary Phone DN is 2000, then the derived DN would be 2*000.
All other fields	See Primary Phone descriptions. **Note**: Network Element for the Secondary Phone automatically defaults to the Network Element of the Primary Phone.	See Primary Phone defaults.

Other Phone (Optional)

Field	Description	Values
Include Other Phone	Click to set up another phone for this user template. This option is only available if the Secondary Prime Phone box is checked.	Default is unchecked. Can be set to the same values available for Primary Phone.

Field	Description	Values
Derive DN	Check this box if you want to derive the Other Phone directory number from the primary phone directory number. It's recommended that you assign users with a prime phone and then derive the directory number of any additional phones from the prime phone directory number.	The system derives the directory number of this phone by inserting an * between the 2nd and 3rd digits of the primary directory number. For example, if the Primary Phone DN is 2000, then the derived DN would be 20*00.
All other fields	See Primary Phone descriptions. **Note**: Network Element for the Secondary Phone automatically defaults to the Network Element of the Primary Phone.	See Primary Phone defaults.

Group (Optional)

Field	Description	Values
Include Group	Select check box to create a group with this user template.	Default is unchecked

Field	Description	Values
Group Type	*Personal Ring Group* (PRG): Allows two or more phones for a single user to be grouped under a common directory number. The devices ring simultaneously (Ring All) when called. The typical scenario is a person's desktop phone and cell phone are twinned together, where the desk phone is considered the prime extension. Both devices require a full MiVoice Business IP User Licence. *Multi-Device - Standard*: Allows up to eight devices (phones) to be grouped under a common directory number. The devices in this group are licensed collectively to a user with a single Multi-device Users license. *Multi-Device - External Twin*: Allows only two devices, typically a desk phone and a cell phone, to be twinned. This type of group requires an IP User License and an External Hot Desk User license. The prime number uses the IP User license; the second number uses the External Hot Desk User license.	Default is Multi-Device - External Twin
Prime	Identifies the pilot phone for the group. The devices are group together under the primary phone directory number. This field is read-only.	Primary Phone.
Members	Check the boxes to include the Secondary Phone, Other Phone, or both, as members in the group.	By default, both Secondary and Other Phone are selected as group members.

Speech Auto Attendant (Optional)

Field	Description	Values
Include Speech Auto-Attendant	Select check box to create a registered Speech Auto Attendant user for this template.	Default is unchecked. This check box is disabled if Speech Auto Attendant is not installed. This check box is not applicable to MiVoice 5000 and MiVoice MX-ONE elements.
Contact Phone	Select the number that you want to use as your Speech Auto Attendant (SAA) contact number. Select "None" to unassign your current SAA number.	List of phones currently owned by the user. **Note**: User must have at least one phone service before entries in these SAA fields are enabled.
Private User	Select this option to exclude your phone from SAA recognition. (This means you cannot be reached by having a caller speak your name to the auto attendant.) **Note**: User is still recognized as a registered SAA user.	You can only select this option after a phone has been selected from the Contact Phone list.

MiCollab Client (Optional)

Field	Description	Values
Feature Profile	Assign a Feature Profile. Feature profiles define the licensed MiCollab Client features that are assigned to a user.	Default is Feature Profile 1.
User profile	User profile defines the dynamic status and other feature settings that are assigned to a user.	Values of the User Profile are set by the administrator.
Desk phone extension	Assigns MiCollab Client desk phone service to the specified phone.	**None**: Do not assign service. **Primary**:Assign to Primary phone's DN. **Secondary**: Assign to Secondary phone's DN.
Soft phone extension	Assigns MiCollab Client softphone service to the specified phone.	**None**: Do not assign service. **Other**: Assign to Other phone's DN.

Field	Description	Values
Deployment profile	This field allows you to select the deployment profile that should be applied when you deploy a MiCollab MAC or PC Client without a softphone to a user. After you click **Save**, a deployment e-mail is sent automatically to the user. The extension field in the e-mail is set to "None". The user clicks the link in the e-mail to complete the deployment.	Default is "Do Not Deploy". Typically, you would select the Default profile. **Note**: If there is no phone for which a deployment profile is selected, users need to provide their password every time they log in to PC and Mobile Clients. **Note**: If a phone with a deployment profile is added later, the user must provide their password for every login to PC and Mobile Clients. However, if the administrator or the user changes the password after the user logs in, the updated password is automatically used for the next login to PC and Mobile Clients.

Field	Description	Values
MiTeam Meetings	Allows you to disable or re-enable MiTeam Meetings for the user. This box applies to all UCC license bundles (except Basic bundle) and users on-boarded to CloudLink. This check-box becomes visible on the UI, when the settings under the **CloudLink Integration** tab **> MiTeam Meetings Entitlement** is checked. • When you clear this box, the cross-launch functionality from MiCollab Client to MiTeam Meetings application is disabled. • When you check this box, the users can click on **Meetings** option in the Client to open the MiTeam Meetings application.	By default, this box is unchecked.
MiTeam Classic	Allows you to disable or re-enable MiTeam Classic for the user. This box only applies to UCC Standard users with an active MiTeam Classic license. • When you clear this box, the MiTeam tab is removed from the user's client. • When you check this box, the MiTeam tab is added to the user's client.	By default, this box is unchecked.

EMEM Voicemail Service (Optional)

Field	Description	Values
Include EMEM Voicemail Service	Click to add EMEM voice mail service to this user template. **Note**: It is applicable only for docker deployments.	This value is checked by default.

NuPoint Unified Messaging Voicemail (Optional)

Field	Description	Values
Include NuPoint Unified Messaging Voicemail	Click to add a voice mail box to this user template. This field is disabled if the template provides an MiCollab Advanced Messaging (AVST) mailbox.	Default is unchecked.
Associate With Phone	Select the phone service with which to associate the voice mailbox.	**None**: Do not assign mailbox. **Primary**:Extension field is set to Primary phone's DN. Secondary: Extension field is set to Secondary phone's DN. (Only available when Secondary Phone service is selected.)
Use Extension Number for Mailbox	Click to use the extension number of the selected phone as the mailbox number.	Default is unchecked. If this check box is left unchecked, a Mailbox Number field is included in the manual entry section of the Quick Add form.
Attendant Extension	This is the number that is called if user dials 0 to return to the attendant. If an attendant extension is defined, it is assigned to ALL mailboxes being created. Optional.	Enter a valid extension number for the attendant. Default is blank. 0-11 telephony digits (*, #, 0-9).

Field	Description	Values
Feature COS	Select a value from the FCOS values available.	Default is 14.
Limits COS	Select a value from the LCOS values available.	Default is 1.
Message Waiting #1	Select a value from the options available.	Default is None.
Message Waiting #2		**Note**: To enable the MWI feature for MiVoice Business phones, you must have MiTAI Integration enabled for the associated phones. **Note**: To enable the MWI feature for MiVoice Business and MiVoice MX-ONE phones, you must use the "DTMF to PBX" setting.
Use 3300 Record-A-Call	Select to enable Record-A-Call feature.	Default is unchecked.

Field	Description	Values
Standard Unified Messaging	Select the check box to enable Standard Unified Messaging for the user's mailbox. Standard UM provides voice mail and FAX access to Lotus Notes, Novell GroupWise and Microsoft Outlook e-mail clients, or from the Web View in the user's e-mail client or Web browser. Users can also access voice, FAX, and Record-A-Call messages from the telephone user interface (TUI). When a voice mail message is left in a Standard Unified Messaging mailbox, the system sends messages to the *UM SMTP Email Addresses* that are defined for the user's mailbox. You can define these email addresses in the user's mailbox through the *NuPoint Web Console*, or the user can define them through their *MiCollab End User Portal*. Refer to the *Unified Messaging book* in the *NuPoint Web Console* online help for details.	Default is unchecked. **Note**: The following configuration conditions apply: • The Feature COS assigned to the mailbox must have the Standard UM feature enabled. • A Standard UM mailbox license must be available for each mailbox that you configure with Standard UM.

Field	Description	Values
Advanced Unified Messaging	Select the check box to enable Advanced Unified Messaging for the user's mailbox. **Note**: For MiCollab Release 5.0 and later systems, you must enable the Advanced UM option using the check box in the NuPoint Unified Messaging tab of the USP application. You cannot enable the Advanced UM option through the NP-UM web console. Advanced Unified Messaging offers a high level of messaging integration and synchronization between a user's e-mail client and NuPoint UM voice mailbox. Full MWI synchronization is provided for voice messages that are accessed through the e-mail client. Message status synchronization is provided for e-mails that are listened to from the NuPoint voice mailbox (they are marked as "read" in the e-mail inbox). Advanced UM users can access their voice, fax, RAC, and email messages (from their Microsoft Outlook inbox or Lotus Notes 7 inbox, and from the NuPoint Voice mailbox) over the phone. Access to email via the Telephone User Interface (TUI) is enabled by integration with the email client, the email server, and text-to-speech (TTS) technology. Refer to the *Unified Messaging book* in the *NuPoint Web Console* online help for additional details.	Default is unchecked. **Note**: The following configuration conditions apply: • The NP-UM Feature COS assigned to the mailbox must have the Advanced UM feature enabled. • An Advanced UM license is required for each mailbox that requires Advanced Unified Messaging. • If a UCC license bundle is assigned to the mailbox user, this option is enabled by default and read-only. • If you clear the check box, Advanced UM is disabled for the user and the license is removed. Also, the Advanced UM e-mail addresses are cleared from the Mailbox page in the user's MiCollab End User Portal .

Audio, Web and Conferencing (Optional)

Field	Description	Values
Include Audio, Web and Video Conferencing	Click to create a registered MiCollab Audio, Web and Video Conferencing user for this template. **Note**: Email address entry is mandatory when this template is applied.	Default is unchecked.
Registered Phone	Select the phone service (Primary, Secondary, or Other phone) with which to associate MiCollab Audio, Web and Video Conferencing .	Default is Primary. **Note**: If "Include Phone Service" is not enabled for a Secondary Phone or Other Phone, these options are not available.
Use Extension Number for Registered Phone	Click to use the extension number of the selected phone as the registered phone. OR Clear this box to allow entry of a number during the "Quick Add" process.	Default is unchecked.

Vidyo Field Descriptions (Optional)

Field	Description	Default
Include Vidyo Service	Check the box to enable the service. Clear the box to disable.	Disabled

Field	Description	Default
Room Type	Normal: Assign this setting to regular users . It allows a user to host personal Vidyo me etings from a desktop device or mobile devic e. VidyoMobile and VidyoDesktop users ca n also host meetings or join with other Vidyo users and room systems.	Default is Normal
	Vidyo Room: Assign this setting to meeting rooms. Meeting rooms must be equipped with a Vidyo supported device. **Note**: Vidyo supports their own room systems and devices. The MiVoice Video Phone can connect to a Vidyo conference via the Vidyo Gateway product (which supports connecting SIP enabled video devices to Vidyo's proprietary video codec environment). The MiVoice Video Phone user must dial into the Vidyo conference using the "Dial by URI" feature.	
	Executive: Assign this setting to priority u sers. It allows them to connect from any Vid yoMobile or VidyoDesktop enabled device without a concurrent use license.	
	Panoramic: Assign this setting to meeting ro oms that are equipped with multiple screens (up to nine high-resloution screens are supp orted).	

6.5 Manage Roles

After you create custom templates, add roles and associate them with the templates. Then, when a new person joins your corporation, you can apply the role and associated user template information to the user's profile using Quick Add.

Note:
You cannot edit or delete the MiCollab default roles.

View

1. Under **Applications**, click **Users and Services**.
2. Click **User Roles**.

Add

1. Click **Add**. The Create Role window opens.
2. Enter a name for the new role.
3. Select the user template that you want to assign to this role.
4. Enter a description of the new role in the Note field.
5. Click **Save**.

Edit

To edit a role name:

1. Check the box of role that you want to edit.
2. Click **Edit**.
3. Select the user template that you want to assign to this role.
4. If required, modify the description for this role in the Note field.
5. Click **Save**.

Delete

You cannot delete a role if it is currently applied to one or more users. To delete unused roles:

1. Do one of the following:
   - To delete a single role, select the box to the right of the role name and then click **Delete**.
   - To delete multiple roles, check the box beside each role and then click **Delete**.
2. Click **Yes** to confirm deletion of a single role or click **Yes to All** to delete all selected roles.
3. Click **Close**.

Note:
You cannot delete the MiCollab default roles.

6.6 Apply Roles

You can apply a role and its associated template information to

- a single user using the **QuickAdd** button
- multiple users from the bulk user provisioning tool.

6.7 Template Migration

When you upgrade from a previous release, the templates in the database restore are updated with any new fields. Generally, any new fields introduced in the release are either blank or set to an appropriate default.

Note:
All phones created in MiCollab Release 4.0 and earlier are full service phones. Therefore, any templates that are migrated to Release 5.0 or later will have a service level of Full. If you want to assign users with PRGs or MDUGs, you must modify the service level of the phone on the MiVoice Business .

Flow Through Provisioning - Description

7

This chapter contains the following sections:

- Flow Through Provisioning - Conditions and Limitations
- Flow Through Provisioning - Management Capabilities
- Flow Through Provisioning - Summary of Behaviors
- Flow Through Provisioning - Configuration
- Flow Through - Maintenance
- Flow Through Provisioning - Events and Alarms

7.1 Flow Through Provisioning - Conditions and Limitations

Refer to the *MiCollab Installation and Maintenance Guide* for instructions on how to configure Flow Through Provisioning.

General

- Flow Through Provisioning is only supported between MiCollab systems and MiVoice Business platforms.
- Flow Through Provisioning is not supported for co-located mode.
- MiCollab Release 7.0 or later is required.
- MiVoice Business Release 7.2 or later is required.
- If MiCollab Client is in co-located mode and you start sharing, then MiCollab Client must remain in co-located mode. You cannot put MiCollab Client in integrated mode after sharing has been started.
- Flow Through Provisioning is only supported from one MiCollab system. It is not supported for multiple MiCollab systems in the same SDS sharing network. You can only include one MiCollab system to share within a SDS sharing network.
- If MiCollab is managing a group of MiVoice Business systems, they must be configured within an SDS sharing cluster. All the MiVoice Business servers in the cluster must be at Release 7.2 or later.
- Flow Through Provisioning must be enabled (started) either from the Mitel Integrated Configuration wizard or manually from a MiVoice Business platform in the administration group of the cluster.
- The USP application allows you to manage the local MiCollab application services and the remote MiVoice Business phone services.
- The recommended best practice is to always manage (add, edit, and delete) users from the MiCollab Users and Services application. You can manage users from the MiVoice Business Users and Services Configuration form and the updates will be shared with MiCollab. However, if you add, edit or delete a user from the Telephone Directory form the update is not shared with MiCollab.
- If you create a user with System Admin or Root access in the MiVoice Business User Authorization form, the user is not shared with the MiCollab Users and Services database.
- The MiCollab USP database lists all the users in the MiVoice Business network. The USP application identifies the host network elements for extensions in the **Phone** tab and application services tabs. For example: **3001 (on Local_30)** where extension 3001 is hosted on network element Local_30.

- A maximum of three phones are supported in a shared MiCollab template. You cannot use a template that is programmed with more than three phones.
- If resiliency is configured for a MiVoice Business solution, data updates are sent from MiCollab to the primary controller. If the primary controller is out of service, the MiCollab USP application does not provide data updates to the secondary controller. Instead, an error message is presented in MiCollab indicating that the primary controller cannot be reached.
- Synchronization is bidirectional. Changes made to users, phones, templates, multi-device user groups, and personal ring groups in any remote MiVoice Business element in the sharing network are reflected in the MiCollab server's USP entry.
- The synchronization of MiVoice Business elements with MiCollab takes substantially longer than the synchronization of just MiVoice Business element form data.
- If Flow Through Provisioning is enabled, IDS Integration must be enabled from MiCollab to Active Directory, not from MiVoice Business to Active Directory.
- MiVoice Business allows you to associate multiple users with the same directory number; however, MiCollab does not support this functionality. If you associate multiple users with the same directory number from the MiVoice Business User and Services Configuration form, the association is not shown in the MiCollab Users and Services application. The following SDS Distribution Error is also generated: “Cannot associate more than one user to the same phone service”.

Topology

- You control the sharing topology of the solution from the following System Data Synchronization (SDS) forms in the MiVoice Business System Administration Tool:

  - Network Elements
  - Cluster Elements
  - Admin Groups
  - SDS Forms Comparison
  - SDS Form Sharing.

The system verifies the topology as part of the Start Sharing process with a MiCollab server. If the topology is invalid, the system displays an error message indicating that start sharing failed or cannot be started, you will need to correct the issue and try again. The MiVoice Business software will not allow the topology to become invalid after sharing has been started with MiCollab.

- Sharing is only supported to one cluster. It is not possible to start sharing with MiCollab from an SDS network which contains more than one MiVoice Business cluster. However, you do not have to have a cluster defined. MiCollab can perform flow through provisioning to a single MiVoice Business; however, if there are multiple MiVoice Business elements in the network which are hosting phone services, you must create a cluster before flow through provisioning can be used to manage all the MiVoice Business systems.
- All MiVoice Business controllers must be active and reachable from MiCollab when sharing is started. It is not possible to create phone services on a MiVoice Business controller which is offline. Flow through provisioning does not fall back to the resilient controller.
- You can configure how data is shared among the MiVoice Business elements using the ‘SDS Form Sharing’ form in the MiVoice Business System Administration Tool However, the flow through provisioning feature requires specific MiVoice Business forms to be shared with MiCollab, so you cannot remove sharing from these forms, nor can you share them at a scope which MiCollab cannot participate in. These restrictions are enforced by MiVoice Business. MiVoice Business will not allow ‘Start Sharing’ with MiCollab if an invalid sharing scope is currently selected. And, after sharing has started with MiCollab, MiVoice Business will not allow you to select an invalid sharing scope.

- The simplest supported configuration is one MiCollab server and one MiVoice Business server in a single (default) administration group with no cluster defined. If there is no cluster defined, MiCollab only shares its data with the MiVoice Business server that started sharing with MiCollab. Flow Through Provisioning is not offered to other MiVoice Business servers in this configuration even if they are included in the local administration group.
- To support Flow Through Provisioning to multiple MiVoice Business servers, a cluster must be defined. Only a single cluster is supported. MiVoice Business will not allow ‘Start Sharing’ with MiCollab if there are multiple clusters. After sharing has started with MiCollab, MiVoice Business will disallow the creation of a second cluster.
- You can use Admin groups to limit the sharing of data between selected network elements. If there are multiple MiCollab servers in an SDS network they must be placed into different Admin groups. MiVoice Business will not allow ‘Start Sharing’ to a new MiCollab server if there is already a MiCollab server in the admin group. In addition, Roles and Templates must be shared at admin group scope.After sharing has started with MiCollab, MiVoice Business will disallow a 2nd MiCollab to be added to an existing admin group which contains a MiCollab server and will disallow changing the sharing scope of Roles and Templates to ‘All Network Elements.
- To avoid role and template conflicts, it is recommended that you segregate the MiVoice Business servers into separate administration groups and change the sharing scope of roles and user templates to "Admin Group" before you start sharing with thefirstMiCollab server.
- Ensure that all MiVoice Business elements in the sharing network are configured with an IP address or FQDN. MiCollab will not support a network element unless it is provisioned with an IP address or FQDN. If a MiVoice Business element is provisioned in the network without an IP address or FQDN then sharing with MiCollab cannot be established. The **Start Sharing** operation will fail with a message to check the MiCollab logs.
- A MiVoice Business server should not be moved from an Admin Group that contains a MiCollab server to an Admin Group containing a different MiCollab server, otherwise; roles and templates learned in the first administration group may conflict with roles and templates in the second cluster.

Departments

- Departments and Locations are shared by default at the network scope, although you can narrow down the scope to just the Admin Group in the ‘Shared Forms Configuration’ form in MiVoice Business System Administration Tool.
- If you delete a department from MiCollab, the department is also removed from the user entries. If Flow Through Provisioning is enabled to MiVoice Business elements, the department is also removed from the MiVoice Business Department form and user entries. However, the behavior on the MiVoice Business is slightly different. Before you can delete a department from the MiVoice Business Department form, you must first remove all references to that department name from the MiVoice Business user entries. After you delete a department from the MiVoice Business, the department is also removed from MiCollab if Flow Through Provisioning is enabled.

Roles and Templates

- A shared template definition is used to create phone services. Flow Through Provisioning is only able to offer the ability to create phone services on MiVoice Business servers which are sharing role and template data.
- Role and template data is shared among the MiCollab server and the MiVoice Business servers in the same Admin Group. Role and template data is not shared with other MiCollab servers (only one MiCollab server is allowed in an Admin Group). Roles and templates are merged during the synchronization process and may need to be reconciled.
- Templates can be added by either copying an existing template (in the Edit Template page) or by adding a new template. You can edit templates either in USP or MiVoice Business System Administration Tool

and the changes are shared. You need to refresh the form to see changes that were made on a remote network element.

- If MiVoice Businesswas upgraded from Release 6.0, there may be legacy templates in the database. These templates will not be imported into MiCollab and will not appear in MiCollab USP. If you attempt to create a new template with the same name as a legacy template, an error is presented.
- USP can manage all the service components within a user and service template, but only a subset of the fields which are offered in the MiVoice Business System Administration forms are available in USP. Use Reach Through to manage the complete phone service template on the MiVoice Business (for example, to edit feature key templates).

Users and Services

- Create users from MiCollab USP using pre-defined roles and templates. Do not create users from the MiVoice Business servers.
- The USP directory only displays phones that are assigned to users. However, the MiVoice Business supports phones that do not have users associated with them. To manage these phones from USP, add a new user to the phone or associate a user with the phone in the MiVoice Business User and Services Configuration form. After you assign a user to the phone, the user and phone will appear in the USP directory and you can add services to the user.
- You cannot assign DNIC or analog phone services to users from USP. However, DNIC or analog phones that have been created on the MiVoice Business system administration tool are displayed in the USP directory and can be modified or deleted.
- The USP directory does not list the following MiVoice Business directory numbers:

  - Phones that are not associated with users
  - Directory numbers that are associated with line appearances on feature keys
  - Local-only phones
  - Directory numbers that are used in certain types of hunt groups.
- It is only possible to manage multi-line MiNET and SIP devices. Single line, DNIC and analog devices cannot be created from the Users and Services application and are not listed in the directory. The same is true for other types of service such as traditional ACD agents, IP consoles, non-prime broadcast groups, and so forth.
- The Users and Services application does not manage phones which are not associated with a user.
- You can assign the "Phantom" Device Type to any MiCollab entries that you do not want shared or synchronized with the MiVoice Business via Flow Through Provisioning. For example, you could assign a "Phantom" device to

  - a mailbox-only entry to allow the mailbox number to be located in the USP directory using the Search feature.
  - an entry that is programmed in the MiVoice Business database as a system speed call, non-prime broadcast group, or console.

Fully Qualified Domain Name (FQDN) for Cloud Deployments

The following Domain Name Server (DNS) configurations are possible in Cloud solution deployments:

- MiVoice Business server may or may not be resolvable in DNS.
- MiCollab server may or may not be resolvable in DNS.
- Any of the servers which make up the solution may resolve to a different IP address inside the LAN versus out in the WAN/cloud (split DNS).
- Any of the servers may not resolve internally, but may resolve externally (partial DNS).

- Mitel Standard Linux operating system can be configured to use a corporate (external) DNS server.

The following conditions apply to programming FQDN(s):

- When MiCollab is initially deployed, the IP address that you enter for the local (LAN) interface is added to the network element in the Network Element list. The FQDN field is initially blank.
- Enter the FQDN for the MiCollab server at any time by editing the local network element in the Network Element page. The FQDN can be the same as the host name and domain that is entered in MiCollab server console or it may be a different FQDN which is only resolvable externally.
- After Mitel Integrated Configuration Wizard adds MiVoice Business servers to the MiCollab server, you must provide the IP address. You can also provide an FQDN. This is also the case when you add MiVoice Business servers to the network.

Note:
The host name and domain entered during server commissioning may not be resolvable anywhere except inside the MSL system. For this reason, the MiCollab server will not attempt to reverse-DNS in order to 'automatically' detect FQDNs.

7.2 Flow Through Provisioning - Management Capabilities

Flow Through Provisioning provides the following management capabilities from USP across a cluster of MiVoice Business systems:

- Manage users:
  - view all users in the MiCollab and MiVoice Business server databases in the USP directory
  - add a single user by role and template on the MiCollab
  - bulk add users
  - update or delete any users who have services hosted on the local MiCollab .
- Manage templates
- Manage application services for the MiCollab users
- Manage phone services for users within the same SDS Admin Group:
  - assign phones that are hosted by MiVoice Business servers in the same SDS Admin Group to users.
  - create and delete phone services
  - perform basic phone service management on every MiVoice Business server in the administration group from a single MiCollab server.
- Maintain network database synchronization:
  - changes made to the MiCollab users and services are synchronized to the MiVoice Business servers
  - changes made to MiVoice Business phone services are synchronized to the MiCollab and other MiVoice Business databases.

- Manage department and locations
- Manage network elements
- Manage resilient configurations

    - supports the programming of resilient devices (the secondary can be any MiVoice Business server in the same cluster).

7.3 Flow Through Provisioning - Summary of Behaviors

- If you add

    - a user to the MiCollab server without a phone, the user is added without a phone to the databases all other MiVoice Business network elements that are sharing.
    - a single user to the MiCollab server with one or more phones, the single user is added with the phone(s) to all other network elements databases which are sharing.
    - a user to a MiVoice Business server, the user is added to all MiCollab servers and all other MiVoice Business server databases.
    - a phone to a user in MiCollab , the phone is added in all MiVoice Business servers and other MiCollab server databases.
    - a phone to a user in a MiVoice Business server, the phone is added to the MiCollab server database.
    - a template to the MiCollab database, the template is added to the database of all the MiVoice Business servers in the same administration group.
    - a template to the a MiVoice Business server database, the template is added to all the other MiVoice Business server databases and to the MiCollab database that is in the same administration group.
- If you make changes to

    - users in MiVoice Business servers, the users are updated on the MiCollab server.
    - phones in MiVoice Business servers, the phones are updated in the secondary controllers and the MiCollab server in the same cluster as the MiVoice Business server.
- Services and templated services have a label which is unique within the user template or user and service template. Use this label to identify the phone list in MiCollab with the phone list in MiVoice Business .
- MiCollab automatically creates teamwork mode MiCollab Client services for users created by remote network elements MiVoice Business servers that are in the same administration group.

7.4 Flow Through Provisioning - Configuration

You start data sharing from the MiVoice Business system administration interface by adding MiCollab as a network element in the **Voice Network** form and then pressing **Start Sharing**. Data sharing can be started from any MiVoice Business. It cannot be started from within MiCollab alone.

Refer to the *MiCollab Installation and Maintenance Guide* for configuration instructions.

7.5 Flow Through - Maintenance

This topic describes the following maintenance tasks:

- Adding a MiVoice Business Element (Start Sharing)
- Updating Network Elements
- Changing an IP Address or Hostname
- Removing MiCollab from a Sharing Cluster
- Stop and then Start Sharing from MiCollab
- Removing a MiVoice Business System from the SDS Sharing Network
- Creating or Deleting a Cluster from the Network
- Checking Software Logs

Adding a MiVoice Business Element (Start Sharing)

To add a MiVoice Business or MiVoice Business Express element to an existing sharing (Flow Through Provisioning) network:

1. Ensure that the MiVoice Business element databases are in sync:
   - Perform a sync from one MiVoice Business to all the other MiVoice Business elements in the network
   - Resolve any synchronization errors that are encountered.
2. Log into the System Administration Tool of the sharing MiVoice Business platform.
   - In the top left corner, select **View Alphabetically**.
   - In the left forms menu, click **Network Elements**.
   - Click **Add** and add the MiVoice Business or MiVoice Business Express as a network element.
3. Start sharing with the newly added element..
   - In the MiVB Network Elements form, check the box of the element
   - Click **Start Sharing**.
   - Click **OK**. After the start sharing operation is complete, the Data Sharing field for the MiVoice Business element changes to YES.
4. Perform a full SDS synchronization with new element:
   - Check the box of the new MiVoice Business or MiVoice Business Express server.
   - Click **Sync**.
   - Click **Data Migration**.
   - Click **Apply**.
   - Click **OK**.

Note:
The synchronization of MiVB elements with MiCollab takes substantially longer than the synchronization of just MiVB element form data.

5. In the Network Element tab of the User and Services application, access the newly added network element and enter the desired Set Registration and Set Replacement Codes.

Note:
When you add a MiCollab Server as a network element in **MiVB System Administration Tool** and initiate Flow Through Provisioning, default login credentials are generated in the **Credentials** tab of the **Network Element** page in the MiCollab Server. Make sure that you replace these default credentials with the MiVB System login credentials. If the credentials are incorrect, PBX synchronization from MiCollab Client Service will not work, and the MiTAI authentication in MiCollab Client and NuPoint Unified Messaging does not work.

6. Reconcile any conflicting data entries.
7. Check the Distribution Error application and resolve any distribution errors.
8. Create backups of the MiCollab database and all MiVoice Business databases.

Updating Network Elements

Updates that you make to the basic data (**Element Identification**, **Credentials**, and **System Properties** fields) of a network element are shared to all the other network elements. Typically, the sharing scope is across the cluster. Changes that you make in the application data (**Voicemail** fields) of the network element page are not shared and do not result in a distribution.

If you change the IP address or name of a 3300 ICP network element that is using a NuPoint UM IP Integration License, you must activate the NuPoint UM inactive configuration. in order for the changes to take effect.

Changing an IP Address or Hostname

If you change the IP address of a node which participates in data sharing, the distribution of that and subsequent data changes are sent to the new IP address. Therefore, it is recommended that you change the IP address from the local node, except in cases where other nodes may be out of sync with the IP address (for example, after a restore).

The System Name and IP address of the local MiCollab Network element cannot be edited in the Users and Services application, but is displayed as read-only with the current values.

Updating the IP address of the MiCollab server is carried out via the MSL server console "Configure this server" option after which a reboot is performed to apply the changes. After the change is applied, the IP address of the MiCollab network element is changed.

The System Name of the MiCollab Network element is modified with the hostname of the MiCollab server. Updating the hostname is also carried out via the MSL server console "Configure this server" option. If the hostname is changed, the System Name of the MiCollab Network element will be changed to the first 9 characters of this hostname.

Once the MiCollab server IP or hostname has been updated, the IP address or System Name for the MiCollab Network Element should be updated automatically in the Network Element forms for all other sharing Network Elements.

If the IP address of a node which is enabled for data sharing is incorrect, all nodes with the wrong IP address will be able to distribute shared data updates to that node and thus distribution errors will accumulate. These errors may be deleted or will be retried automatically once the IP address has been corrected.

Removing MiCollab from a Sharing Cluster

Use this procedure to remove MiCollab from the sharing network if

- you have accidently added MiCollab to the wrong cluster, or
- you want to move MiCollab to a different cluster.

Note:
Do not delete the MiVoice Business network elements from the MiCollab USP Network Elements tab if you want to remove MiCollab from the sharing network. This action will cause the SDS network to stop sharing. Instead use the procedure described below:

To remove MiCollab from a sharing cluster:

1. Log into the MiCollab Linux shell, via SSH or local console using the root account.
2. Run the following Linux command: */usr/mas/bin/sds-utility --disconnect-sds*
3. You are presented with a list of actions that will be performed and a confirmation if these actions should be applied. Confirm to proceed disconnecting from SDS.
4. Confirm that the Linux command completes successfully.
5. Log into the System Administration of a MiVoice Business element that remains in the sharing network.
6. Choose to view the forms alphabetically.
7. Select **Maintenance and Diagnostics**and then click **Maintenance Commands**.
8. Enter REMOVENE <MiCollab network element name> and select **OK** to confirm.
9. Repeat the REMOVENE command on all remaining Network Elements in the sharing network.
10. Verify that all remaining nodes within the sharing network no longer display the MiCollab Network Element within the **Network Elements** list.
11. The **User Roles** and **User and Service Templates** forms will still contain a set of templates that was previously shared with MiCollab. If these templates and roles are not required, you can delete them.

Stop and then Start Sharing from MiCollab

If you need to modify data on the MiCollab system that you don't want distributed to the other MiVoice Business elements, you can stop sharing from MiCollab, apply the updates to MiCollab, and then start sharing again with the MiVoice Business network elements.

To stop sharing from MiCollab:

1. Log into the MiCollab linux shell, via SSH or local console using the root account.
2. Run the following command from the linux prompt:

   /usr/mas/bin/sds-utility --stop-sharing
3. Make any required updates to the MiCollab database. The data is not shared to the MiVoice Business.

To start sharing again:

1. Log into the System Administration of a MiVoice Business element that remains in the sharing network.
2. Choose to view the forms alphabetically and select the **Network Elements** form.
3. Locate the MiCollab network element, select it, click **Start Sharing** and confirm **OK.**
4. Verify the sharing and synchronization completes successfully and if instructed, log into the MiCollab server and observe the red banner directing a run of the **Reconcile Wizard** to align the data.

Removing a MiVoice Business System from the SDS Sharing Network

To remove a MiVoice Business element from the SDS sharing network:

1. Log into the MiCollab Linux shell, via SSH, or local console using the root account.
2. At the command prompt, run the following command:

removene <MiVoice Business network element name>

1. You will be presented with a list of actions that will be performed and a confirmation if these actions should be applied. Confirm to proceed with removing the network element and verify that the removal completes successfully.
2. Log into the System Administration of a MiVoice Business element that remains in the sharing network.
3. Choose to view the forms alphabetical.
4. Select **Maintenance and Diagnostics** and then click **Maintenance Commands** .
5. Enter REMOVENE <*MiVoice Business network element name*> and select **OK** to confirm.
6. Repeat the REMOVENE command on all remaining Network Elements in the sharing network.
7. Verify that all remaining nodes within the sharing network no longer display the MiVoice Network Element within the **Network Elements** form.

Note:
If you remove all MiVoice Business network elements from the MiCollab Network Elements list, SDS sharing is stopped. If the SDS includes other MiVoice Business platforms that were not managed by MiCollab, then sharing will also be stopped between these elements. To restart sharing among these other elements, log into the Network Elements page of one of the MiVoice Business systems, select the check boxes of the elements that should be sharing and click **Sync**.

Note:
Even after re-initiating the SDS sharing between the network elements, certain issues are reported where few MiCollab services for existing MiCollab users are impacted, like AWV extension information, NPM user mailboxes, and Teleworker information, even if these users exist over MiVoice Business.

If You Create or Delete a Cluster

If you create or delete a cluster of elements in a network that has Flow Through Provisioning enabled, you must perform a **Sync** operation from a MiVoice Business element in the network with MiCollab. Otherwise, Flow Through Provisioning will not function correctly and data distribution errors will be generated.

In the case where you delete a cluster from the network and then perform the **Sync**, Flow Through Provisioning will function through the MiVoice Business from which you performed the **Sync** operation.

Checking Software Logs

The main components involved with flow through provisioning write software logs here:

- /var/log/mom-server/*
- /var/log/sdscc/*
- /var/log/upm/*

If you encounter a problem check these logs. The latest log is always called ‘current’ and the older logs will be present with timestamps.

7.6 Flow Through Provisioning - Events and Alarms

The following table describes the key server manager events and alarms that can be raised by the Flow Through Provisioning feature. These events and alarms appear in the server manager Event Viewer.

Flow Through Provisioning: Key Events and Alarms

Event or Alarm Description	Severity	Details
Flow Through Provisioning Inactive	Minor	This alarm indicates that a database was restored or the that the MiCollab server was upgraded from an earlier release in which single point provisioning was enabled. This alarm condition is raised because single point provisioning is no longer enabled. To enable Flow Through Provisioning, you must perform an SDS **Start Sharing** operation from a MiVoice Business in the cluster administration group. Then, perform a Data Reconcile if required.
Starting Sharing from a MiVoice Business server	Indeterminate	This event indicates that a MiVoice Business server started sharing with the MiCollab server and that the start sharing operation was completed.
Sync Required Alarm	Minor	This alarm indicates that a MiVoice Business server started sharing with the MiCollab server and that the start sharing operation was completed, but a sync has not been completed. This is an alarm condition because USP has an incomplete view of the shared data and as a result is unable to perform Flow Through Provisioning operations and share updates from USP to the MiVoice Business servers. This alarm is cleared after you perform a sync from any MiVoice Business server to this MiCollab server.
Device Data Notification Started or Completed	Indeterminate	This event lists the elements or group with which the MiCollab server registered for device data. Phone services hosted on these servers will have full details in the USP application. Phone services hosted on other servers will just have a directory number. The presence of this event indicates that the listed MiVoice Business servers will send shared updates to the MiCollab server whenever their phone or group information is updated.
User Sync Started or Completed from a MiVoice Business server	Indeterminate	This event indicates that a MiVoice Business server performed a ‘Sync’ to synchronize data with the MiCollab server and that the synchronization is complete.

Event or Alarm Description	Severity	Details
Device Data Synchronization Started or Completed	Indeterminate	This event indicates that the MiCollab server performed a synchronization of device data with all network elements. All of the phone services hosted by all of the MiVoice Business servers in the administration group will have full service details listed in USP if this event is present.
Sync Reconcile Required	Minor	This alarm indicates that a MiVoice Business server performed a 'Sync' operation to synchronize data with the MiCollab server and conflicts were detected between the current configuration data and the data which was synchronized with the MiCollab server. This is an alarm condition because USP has an inconsistent view of the shared data and as a result is unable to perform Flow Through Provisioning operations and share updates from USP with MiVoice Business servers. This alarm contains a hyperlink which you can use to launch the 'Sync and Reconcile' wizard. This alarm is cleared after you run the sync and reconcile wizard.
SDS Distribution Errors	Minor	This alarm indicates that a shared update which was generated by the MiCollab server was rejected by some other nodes in the network, resulting in another node in the network having an inconsistent view of the shared data and some updates may fail because of this. This alarm contains a hyperlink which you can use to launch the SDS Distribution Error application. This alarm is cleared after you delete or retries the failed distributions. Before your delete a distribution error, ensure that the data entry is not valid or required.

Event or Alarm Description	Severity	Details
NuPoint UM Network Element Updated	Minor	This alarm indicates that a network element which is programmed in NuPoint has been updated or removed. This could be the result of an update being made in the 'Network Elements' form of a MiVoice Business System Administration Tool. In order to apply the update, you must perform a NuPoint Activation. This alarm contains a link to the Nupoint Activation page.
MiTAI Authentication Failed for <MiVB IP Address> - Incorrect Username/ Password	Critical	This alarm indicates that MiTAI authentication failed because the MiVoice Business System login credentials entered in **Users and Services** > **Network Element** page is incorrect. To clear this alarm, you must enter the correct login credentials, select the **Use NuPoint UM IP Integration Licenses** checkbox and click **Save**. You must then activate this change in the NuPoint UM application from the activation link at the top of the page.
MiTAI Authentication Failed for <MiVB IP Address> - Username/Password not provided	Critical	This alarm indicates that MiTAI authentication failed because the MiVoice Business System login credentials were not entered in the **Users and Services** > **Network Element** page. To clear this alarm, you must enter the correct login credentials, select the Use **NuPoint UM IP Integration Licenses** checkbox and click **Save**. You must then activate this change in the NuPoint UM application from the activation link at the top of the page.
Update Rejected	Minor	If the MiCollab server rejects an update from another network element, an event listing the details of what was rejected and why it was rejected is displayed. Use this information to correlate events that are displayed in the distribution error management tools of other network elements.
SDS Sharing could not be started	Minor	If an older MiVoice Business attempts to start sharing with MiCollab , MiCollab reverts the sharing attempt and displays an event and red banner stating that the sharing could not be started.

Reconcile Wizard - Description 8

This chapter contains the following sections:

- Reconcile Wizard - Conditions
- How Entries are Paired
- Reconcile Wizard - Welcome
- Reconcile Wizard - Analyze Reconcile Operations
- Reconcile Wizard - Non-Sharing Network Elements
- Reconcile Wizard - Sharing Network Elements
- Reconcile Wizard - MiCollab Phones to be Reviewed
- Reconcile Wizard - Execute Reconcile
- Reconcile Wizard - Manually Reconciling Operations
- Reconcile Wizard - Configure MiCollab Network Element Settings
- Reconcile Wizard - Troubleshooting

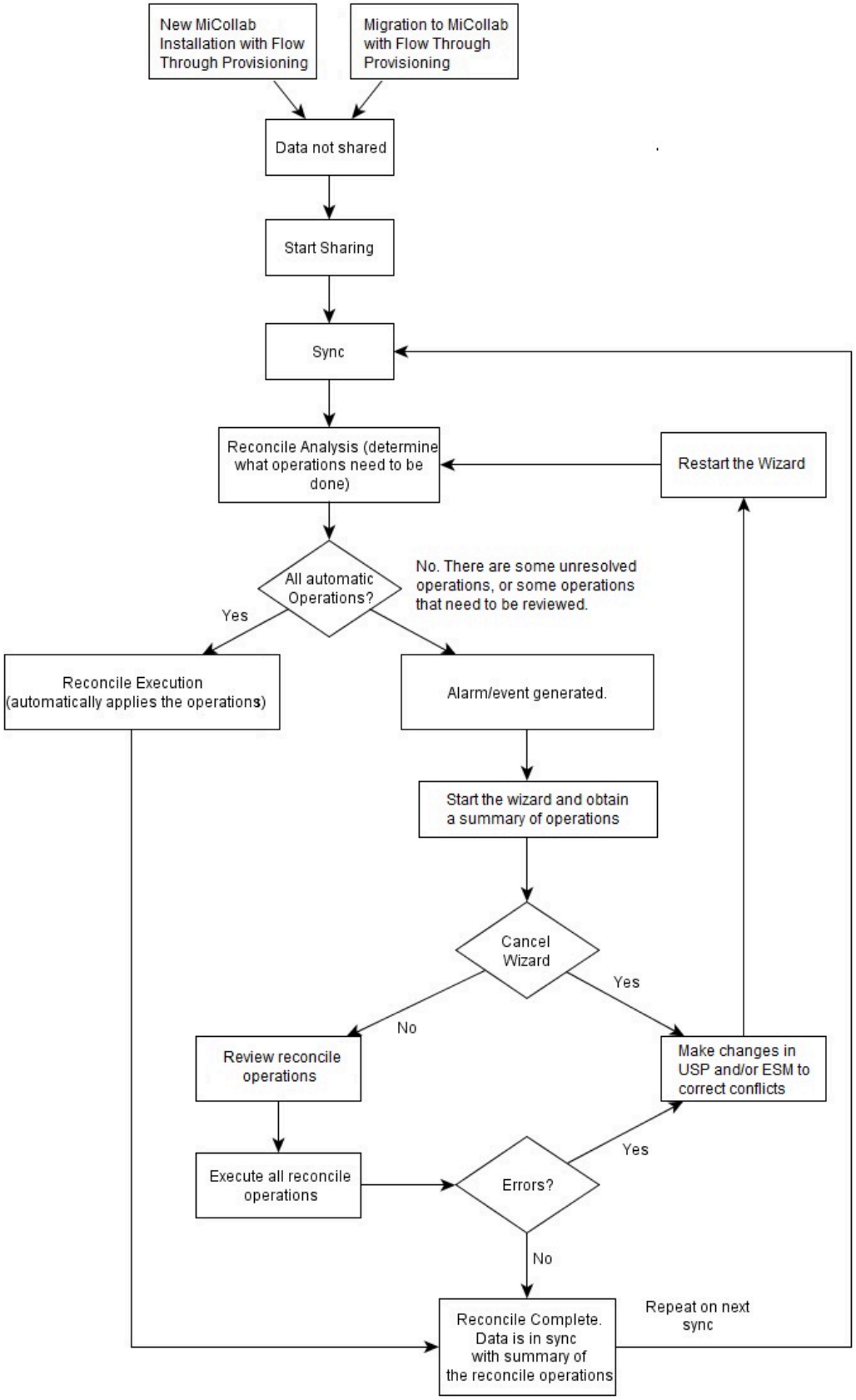
The Reconcile Wizard pairs data entries in the MiCollab database with data entries in the MiVoice Business databases in a network that is being configured to support Flow Through Provisioning. It also identifies any data conflicts between the databases so you can manually resolve them.

When you configure Flow Through Provisioning, you must add the MiCollab system as a network element to the MiVoice Business Network Element form, click the **Start Sharing** button to share and begin the synchronization process. At the start of the synchronization process, the system automatically runs a reconcile analysis of the databases, detects any matching entries, and then attempts to automatically merges them.

- If the wizard is able to match all the data entries and does not detect any conflicts, synchronization is complete and no further action is required.
- If the wizard detects data conflicts that it cannot resolve or conflicts that you should review, the system displays a warning banner in the server manager that instructs you to run the wizard. In this case, you must run the wizard to identify the unresolved conflicts and then manually correct them by modifying the entries either from the MiCollab USP application or the MiVoice Business system administration tool. You must repeat this process until you have corrected all unresolved data conflicts.

Note:
If the databases are not in sync, duplicate user entries with the same LoginID and e-mail address can occur in the MiVoice Business database. To resolve, run the Reconcile Wizard.

The following flowchart illustrates the Reconcile Wizard use cases:


New MiCollab Installation with Flow Through Provisioning
Migration to MiCollab with Flow Through Provisioning
Data not shared
Start Sharing
Sync
Reconcile Analysis (determine what operations need to be done)
Restart the Wizard
All automatic Operations?
No. There are some unresolved operations, or some operations that need to be reviewed.
Yes
Reconcile Execution (automatically applies the operations)
Alarm/event generated.
Start the wizard and obtain a summary of operations
Cancel Wizard
Yes
No
Review reconcile operations
Make changes in USP and/or ESM to correct conflicts
Execute all reconcile operations
Errors?
Yes
No
Reconcile Complete. Data is in sync with summary of the reconcile operations
Repeat on next sync

After Flow Through Provisioning is enabled and proper synchronization is achieved, you should not need to use the wizard again.

8.1 Reconcile Wizard - Conditions

- While a reconcile operation is in progress, do not attempt to make changes to users and services from any of the administration tools (for example, MiCollab USP, MiVoice Business system administration tool, and so forth) as this might introduce data inconsistences while the reconcile is running.
- If Integrated Directory Services is enabled for MiCollab , any updates from the directory server are blocked while a reconcile is in progress.
- The Reconcile Wizard merges MiVoice Business data entries that are paired with MiCollab data entries based on matching criteria.
- Only one instance of the Reconcile Wizard can be run at any time. However, multiple views of the operation summary can be displayed.
- An application event log is generated whenever the reconcile wizard determines that there are reconcile operations that require administrator intervention. In addition, ared banner appears on the server-manager web pages warning that the reconcile wizard must be run.
- While you are viewing the Reconcile Wizard operations in the Summary of Operations page and while the wizard is executing the reconcile operations, MiCollab rejects any SDS updates that it receives from the sharing network.
- If the Event logs indicate that you need to run the Reconcile Wizard, do not make any updates from the MiCollab USP until after you have run the wizard and the databases are in sync. While the databases are out of sync, MiCollab USP updates are not shared to the network elements.
- During a reconcile, if a MiCollab user entry is assigned Teleworker service, but the phone type for a MiVoice Business user does not support Teleworker service then the Teleworker service is removed from the corresponding MiCollab user entry.
- It is possible to program non-existent phones (for example MiNET devices) in the USP application against voice mail boxes, speed calls, hunt group numbers, and non-prime broadcast groups. This allows you to search for the directory number in the USP directory and find the user assigned with the feature. If you have programmed non-existent phones in the Users and Services application, the Reconcile Wizard will assign them with a "Phantom" device type during the reconcile. MiCollab entries that are assigned with the "Phantom" device type are not shared or synchronized with the MiVoice Business via Flow Through Provisioning.

8.2 How Entries are Paired

The Reconcile Wizard pairs up entries in the MiCollab database with entries in the MiVoice Business databases that have matching data for the following:

- User Information (Directory Number, Login ID, and Email Address)
- Network Elements
- Locations
- Department Names
- Template Names, and
- Role Names.

It pairs MiCollab with MiVoice Business users

- firstly, by phone directory numbers (and PRG/MGUG group membership if available) and
- secondly, upon the user's login ID and e-mail address.

If a MiCollab user is paired with one or more MiVoice Business users, the reconcile operation merges them into a single entry.

The following data is not paired:

- Single-line devices
- Line Appearance Keys
- Local-only devices
- Phones without users (example, application ports)

The following table summarizes how the wizard automatically pairs data entries:

Status of entries	Reconcile Operation
MiCollab and MiVoice Business users have same directory numbers.	The user entries are collapsed into a single user with one or more phones. The MiCollab user information is applied to the user. If there are multiple MiVoice Business users, they will be either collapsed or deleted. The end result being a single user with the MiCollab user information and the phones from the MiVoice Business entries.
MiVoice Business users that are not paired with a MiCollab user are not automatically assigned MiCollab Client service.	In previous MiCollab releases, when a user was created the user was automatically assigned MiCollab Client service. However, in MiCollab 7.0 and later, when MiVoice Business users are synchronized with the MiCollab database via System Data Synchronization, if those MiVoice Business users are not paired with a MiCollab user, then they are not automatically assigned with MiCollab Client service.
Matching MiCollab and MiVoice Business entries have different services for the user.	If a MiCollab user who is assigned application services (such as MiCollab Client or NuPoint) gets paired with a MiVoice Business user who also has services (such as a PRG or MDUG) then the reconciled user receives both the MiCollab services and the MiVoice Business services. **Note**: Exception MiCollab doesn't display MiVB embedded voice mail services

Status of entries	Reconcile Operation
Duplicate non-default Template Names	The wizard renames the MiVoice Business template as follows: <Template Name> becomes <Template Name>(x). Where (x) is a number starting with 1. For example, in a scenario where there are more than two servers in the network and they all have a non-default template with the same name, the resulting template names would be: “Example Template Name” (for the template that was on the first node in the sharing network) "Example Template Name (1)” “Example Template Name (2)”
Reconciling Duplicate Departments or Locations	The wizard merges the MiCollab and MiVoice Business departments such that only one department with that name will exist. When departments are merged, the department number and description are retained in the MiCollab database If the MiCollab and MiVoice Business both have a location with the same name, then the wizard merges these two locations into a single location.
Same role name referring to a different template	The wizard renames the MiVoice Business role as follows: <Role Name> becomes <Role Name> (x)”, where (x) is a number starting with ‘1’.
MiCollab and MiVoice Business user match on a directory number (DN) and the MiVoice Business user has additional DNs.	The wizard pairs the MiCollab and MiVoice Business users based on the matching DN. The merged user uses the MiCollab user information. The additional MiVoice Business user DNs are also included with the merged user.

Status of entries	Reconcile Operation
MiCollab user has multiple DNs, one or more of which match the DNs of a MiVoice Business user.	The wizard merges the MiCollab and MiVoice Business users. The merged user uses the MiCollab user information. If there are multiple MiVoice Business users, they will be either collapsed or deleted. The end result being a single user with the MiCollab user information and the phones from the MiVoice Business entries.
MiCollab user has DNs that match to MiVoice Business DNs that are not assigned to users.	MiVoice Business DNs that are not assigned to users that are matched to a MiCollab user are merged with the MiCollab user.
Teldir entries are updated when MiVoice Business users are merged with MiCollab users.	The wizard updates the MiVoice Business telephone directory entries when a MiVoice Business user is merged with a MiCollab user.
Non-sharing network elements that are either • programmed on the MiCollab system but not programmed in the MiVoice Business sharing network, or • programmed in the network but their data is not being shared with any other elements.	Non-sharing network elements will not support Flow Through Provisioning after the reconcile. You must add the missing elements to the sharing network from the System Administration tool of one of the member MiVoice Business systems, and then start the Reconcile Wizard again.
Network elements that need to be reconciled with this network element.	
External and Other-PBX Phones	The wizard does not attempt to pair up the DNs for these phones with DNs on the MiVoice Business. Instead, these phones are treated as MiCollab services that are not shared across the network.

8.3 Reconcile Wizard - Welcome

The Reconcile Wizard pairs data entries in the MiCollab database with matching data entries in the MiVoice Business databases for a network that is being configured to support Flow Through Provisioning. It also identifies any data conflicts between the databases so you can manually resolve them.

Note:
If the databases are not synchronized, duplicate user entries with the same LoginID and e-mail address can occur in the MiVoice Business database.

The current synchronization status is indicated at the top of the Welcome page.

Field	Description	
Current Status	Reconcile not required	Databases are synchronized.
	Reconcile required	Databases out of sync. You must run the Reconcile wi zard to synchronize the databases and configure Flow Through Provisioning. The MiCollab USP database will not begin sharing data with the MiVoice Business datab ases until you have completed this wizard.
	Data Sync in Progress	
	In use by another admin	
	IDS sync in progress	
Previous Reconcile Reports	Downloads previous reconcile operation summary reports. The most recent Reconcile Su mmary report of the failed, unresolved, and successful operations.	
Backups	Make backups of MiCollab and MiVoice Business system databases before running this w izard. Click the links to access the system backup functions.	

Running the Reconcile Wizard

1. In the server manager, under **Configuration**, click **Reconcile Wizard**.
2. Ensure that you are the only administrator using the wizard. Only one administrator should access the Reconcile Wizard at a time.

CAUTION:
While a reconcile operation is in progress, changes to users and services should not be made from any of the administration tools (for example, MiCollab USP, MiVoice Business system administration tool, and so forth).

3. Make backups of the MiCollab and MiVoice Business system databases before running this wizard. Click the links to access the system backup functions.
4. Check the **Backups Recommended** box. You must check this box to enable the **Next** button.
5. Click **Next**.

Note:
If you navigate away from the reconcile wizard or click **Abort** prior to the execution phase, then the analysis must be repeated when you open the wizard again. You must complete the Reconcile Wizard in order for the USP database on the MiCollab to start sharing and become synchronized with the MiVoice Business databases.

8.4 Reconcile Wizard - Analyze Reconcile Operations

The wizard analyzes the databases and displays the number of required reconcile operations. There are three types:

- **Automatic Operations**: matching entries that the reconcile operation automatically resolves.
- **Operations For Review**: operations that you should review before the wizard performs the reconcile.
- **Unresolved Operations**: data conflicts that the wizard is unable to resolve. You can proceed with the reconcile wizard even if unresolved operations are detected. However, these operations will not be performed and you must manually resolve these conflicts either from the MiCollab USP application or the MiVoice Business system administration tool before the reconcile process can be completed.

Click **Start Analysis**. After analysis is 100% complete, click **Next** to proceed. You must run the analysis in order to proceed.

Field	Description
Elapsed Time	Hours:Minutes:Seconds
Operations Count	Number of operations identified (automatic operations, operations for review, an d unresolved operations). Operation details are provided in a summary at the end of the wizard.
Progress Bar	Provides visual indication of the analysis process.

8.5 Reconcile Wizard - Non-Sharing Network Elements

This page displays any non-sharing network elements that will not use Flow Through Provisioning after the reconcile is complete. These are elements that are either

- programmed on the MiCollab system but not programmed in the MiVoice Business sharing network, or
- programmed in the network but their data is not being shared with any other elements.

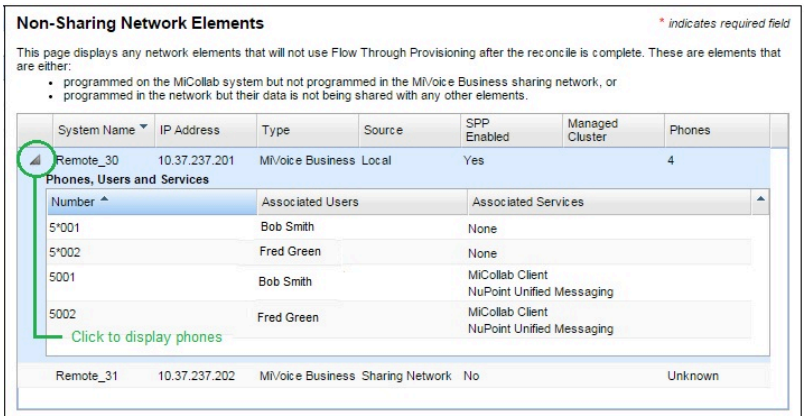
Note:
This page only appears if there are non-sharing network elements.

Review the contents of the table. If an arrow is present the arrow in the first column next to a network element, you can click it to display a list of all the phones, users, and services that are programmed on that element.

- If there are network elements listed in the table that should support Flow Through Provisioning after the reconcile, click **Abort**. Add the elements to the sharing network and restart the wizard.

  OR
- If the listed elements do not require Flow Through Provisioning, check the **I wish to proceed** box and then click **Next**.

Parameter	Description
System Name	System name of the network element
IP Address	IP address of the network element
Type	Identifies the type of network element: MiCollab or MiVoice Business
Source	Where the element is programmed: • Local: programmed on MiCollab system • Sharing Network: programmed on a MiVoice Business in the sharing network
SPP Enabled	Yes: Prior to the upgrade to MiCollab Release 7.0, this element had Single Point of Provisioning enabled. Therefore, it is most likely that this element should be added to the sharing network and configured for Flow Through Provisioning.
	No: Prior to the upgrade to MiCollab Release 7.0, this element did not have Single Point of Provisioning enabled.
Managed Cluster	Name of the managed cluster

Parameter	Description
Phones	Number of phones on the element. If the network element is programmed in the MiCollab Network Elements tab, the number of phones will be listed. If not, Unknown is displayed. If phones are listed, click the ▶ key to see the details. 
Confirmation	If there are elements listed that previously supported Single Point Provisioning, you are required to confirm that these elements do not need to share data with any other network elements after the reconcile operation is complete. You must check the I wish to proceed box to enable the Next button.

8.6 Reconcile Wizard - Sharing Network Elements

This page displays a list of all the network elements that need to be reconciled with the Local/Sharing Network (MiCollab) element. After the reconcile is complete, these network elements will share data in the SDS network.

- If all the network elements that should be in the SDS sharing network are listed, then click **Next**.
- If not, click **Abort** , add the missing elements to the sharing network from the System Administration tool of one of the member MiVoice Business systems, and then start the Reconcile Wizard again.

Parameter	Description
System Name	System name of the network element
IP Address	IP Address of the network element
Type	Identifies the type of network element: MiCollab or MiVo ice Business

Parameter	Description
Source	Where the element is programmed: • **Local**: programmed on MiCollab system only • **Sharing Network**: programmed on a MiVoice Business in the sharing network • **Local/Sharing**: programmed on a MiVoice Business in the sharing network.
Managed Cluster	Name of the managed cluster

8.7 Reconcile Wizard - MiCollab Phones to be Reviewed

This page lists the phones that you should review before proceeding with the Reconcile operation. The list includes phones that are

- programmed in MiCollab, but not programmed in MiVoice Business
- programmed in the MiVoice Business, but are not programmed in MiCollab
- programmed with matching directory numbers on MiCollab and the MiVoice Business, but the phone on the MiVoice Business is assigned with a Device Type that is not supported on MiCollab.

Review the list of phones:

- If there are phones in the list that should be in the sharing network or on a non-sharing MiVoice Business element, click **Abort**. Log into the System Administration Tools of the MiVoice Business elements and add the phones.
- If there are phones that are not required in the network, click **Abort**. Log into MiCollab USP and delete the phones.
- If there are phone entries that have been purposely programmed only in the MiVoice Business database (for example, IP Consoles, system speed calls, or non-broadcast groups) leave these entries unchanged.
- If there are phones that have been purposely programmed only in MiCollab, (for example as a mailbox, so it can be located using search in the USP directory) leave these entries unchanged. This type of entry should be programmed with a "Phantom" Device Type in the Phones tab of the user.

Note:
This page is not displayed if there are no phones identified for review.

Parameter	Description
Number	Extension number of the phone to be reviewed
Network Element	Name of network element that should be hosting phones
Associated Users	User assigned to phone

Parameter	Description
Associated Services	Services (applications) assign to the phone

8.8 Reconcile Wizard - Execute Reconcile

This page displays a summary of the automatic operations, operations for review, and unresolved operations that were detected. If unresolved operations are detected, you can manually resolve them prior to proceeding with the reconcile operation.

After you click **Reconcile**, the wizard executes the reconcile operations and displays a summary of the failed, unresolved, and successfully completed operations.

Warning: Ensure that you review the Analysis Summary carefully.

To reconcile the databases:

1. Review the Analysis Summary. Optionally, click **Save Report**and save a copy of the Analysis Summary to your PC.

   - If there are "Operations for Review" listed, review them to ensure that these operations will have the desired result.
   - If there are "Unresolvable Operations" listed, manually reconcile the unresolved operations and click **Rerun Analysis**. On subsequent runs of the analysis, unresolved operations that you manually corrected are not listed. Repeat this step until all unresolved conflicts are removed from the summary.
   - The wizard performs the "Automatic Operations" automatically after you start the reconcile.
2. Click **Reconcile** and then click **Ok**. The wizard generates a Reconcile Summary of the failed, unresolved, and successful operations.

> **Note**:
> If you navigate away from the reconcile wizard during the execution phase, the reconciliation process is not stopped. It continues to run in the background until it is finished.

3. Review the Reconcile Summary. Optionally, click **Save Report** and save a copy of the Reconcile Summary to your PC.
4. If there are failed operations listed, manually reconcile the failed operations and run the wizard again. On subsequent runs of the analysis, any failed operations that you manually corrected are not listed. Repeat this step until all failed operations are removed from the summary.
5. Click**Finish**.

Note:
If you run the wizard on a new site installation (Greenfield MiCollab and a Greenfield MiVoice Business) where the MiCollab Client application is configured in co-located mode a red warning banner is displayed in the server manager. See Configure MiCollab Client Network Element Settings for additional configuration steps.

Note:
The Analysis Summary and Reconcile Summary reports are saved to the MiCollab Server Manager Log Files.

6. Check the Distribution Error application and resolve any distribution errors.

8.9 Reconcile Wizard - Manually Reconciling Operations

The following table summarizes the corrective actions that you must take to resolve conflicts that the wizard could not resolve automatically

Failed or Unresolved Operations	Description	Corrective Action
Conflicting DNs	More than one MiCollab User has a DN that matches one of the DNs for a single MiVoice Business User	In this scenario, there are two or more MiCollab users that each have one or more DNs that match up with the DNs on a common MiVoice user. For example, on the MiCollab there is User ‘X’ with DN ‘1000’ and User ‘Y’ with DN ‘2000’. On the MiVoice Business there is User ‘Z’ with DNs ‘1000’ and ‘2000’. You need to determine which users should own each DN. If MiCollab User “X” should own DN ‘1000’ and User “Y” should own DN ‘2000’, reach through to the MiVoice Business system administration tool and disassociated one of the DNs from User “Z”. On a subsequent reconcile, the result would be that User “Z” is merged with one of the MiCollab users and DN ‘1000’ remains associated with User “X” and DN ‘2000’ remains associated with User “Y”. If you want all three of these users merged into one user, then DN ‘1000’ and DN ‘2000’ on the MiCollab have to both be associated with either User “X” or User “Y”. Then, when the reconciliation is repeated, there will be one user that owns both phones (in both the MiCollab and in the sharing network).

Failed or Unresolved Operations	Description	Corrective Action
Accented characters in Department or Location	MiCollab Department or Location names cannot contain accented characters	Remove accented characters: 1. Access the USP application. 2. On the **Department** and **Location** tabs, remove any accented characters from the names. 3. Run the Reconcile Wizard again to resolve.
MiCollab users or templates refer to departments or locations that contain accented characters	If a user or template in MiCollab refers to a department or location that contains accented characters, then the wizard cannot automatically resolve those users and templates.	Remove accented characters: 1. Access the USP application. 2. On the **Department** and **Location** tabs, remove any accented characters from the fields. 3. Run the Reconcile Wizard again. Those departments and locations will be reconciled along with any users or templates that referred to those departments or locations.
MiCollab users or templates refer to a role that contains accented characters	If a user or template in MiCollab refers to a role that contains accented characters, then the wizard cannot automatically resolve those users and templates.	Remove accented characters: 1. Access the USP application. 2. On the **User Roles** tab, edit the roles and remove any accented characters from the fields. 3. Run the Reconcile Wizard again. Those departments and locations will be reconciled along with any users or templates that referred to those departments or locations.

Failed or Unresolved Operations	Description	Corrective Action
Unresolvable User Operation Users from this MiCollab that cannot be resolved because they have a login ID conflict with a user in the sharing network:	Example: * John Rae -> John R Teleworker, John Rae MiCollab has two entries: • John Rae with 2 phones (7236, 7336) and login ID 'jrae'. But MiVB has three entries: • John Rae with no phones and login ID 'jrae'. • John Rae with 7236 with no login ID. • John R Teleworker with 7336 and no login ID.	Pair users on login ID (providing that the first name and last name are identical and that the DN pairing is also identical).
User entry cannot be aligned due to configuration issue	A MiCollab user and a MiVoice Business user are matched based on DN, but the hosting network element for each user is different. For example: MiCollab user Johnny has DN 1000 that is hosted on MiVoice Business A. The matching MiVoice Business user John has DN 1000 BUT the phone is hosted on MiVoice Business B.	Change the hosting element of one of the user entries to match the other.
User entry cannot be aligned due to configuration issue	A MiCollab user is paired with multiple MiVoice Business users, but one of the MiVoice Business users has a phone with a secondary network element, which is a MiVoice Business that is NOT sharing.	Change the secondary element to that of one in the sharing network.

Failed or Unresolved Operations	Description	Corrective Action
MiVoice Business users are unresolvable.	The MiVoice Business users are sharing a phone.	MiCollab does not support the sharing of phones. On the MiVoice Business , assign the users with different phones.

8.10 Reconcile Wizard - Configure MiCollab Network Element Settings

After you run the wizard on a new site installation (Greenfield MiCollab and Greenfield MiVoice Business systems) where MiCollab Client is configured in integrated mode you will receive the following warning in the MiCollab server manager.

WARNING: Because MiCollab Client is configured in integrated mode, you must update the System Login Name, Password, and Set Registration Code settings in the **Network Element** tab of the USP application to match the settings of the MiVoice Business network elements. See help.

If you receive this warning, complete the steps listed below:

1. In the server manager, under **Applications**, click **Users and Services**.
2. Click the **Network Element** tab.
3. For each network element in the list:
   - Select the network element and click **Edit**.
   - If the settings must be updated, the System Login field will display "CHANGEME". Change the System Login, Password, and Set Registration Code fields to match the MiVoice Business system login ID, password and set registration code.
4. Click **Save**.

8.11 Reconcile Wizard - Troubleshooting

Symptom	Probable Cause	Corrective Action
The reconcile wizard fails with a message similar to "sds sync did not sync proper info."	The Reconcile Wizard is not properly licensed with the Application Management Center (AMC). The Application Record ID is not registered with the AMC.	Log into the MiCollab server manager, access the Status page and Sync the MiCollab ARID with the AMC.

Reach Through - Description 9

This chapter contains the following sections:

- Reach Through - Conditions
- Reach Through - Configuration
- Using Reach Through

MiCollab Reach Through provides you with the ability to access MiVoice Business System Administration System Administration Tool (MiVB System Tool) forms from links or drop-down menus within specific USP pages. Because you have logged into the MiCollab server manager, you are allowed direct access and do not have to log in separately to the MiVoice Business. This functionality reduces the amount of time it takes to perform programming tasks, such as modifying a user's MiVoice Business phone and group settings, that require configuration on the MiVoice Business.

Note:
The MiVoice Business also supports Reach Through. It allows administrators to link directly to MiCollab USP forms from specific MiVoice Business system administration tool programming forms.

USP Pages that Support Reach Through

You can reach through from MiCollab USP pages to the following MiVoice Business System Administration Tool forms:

MiCollab User and Services Application page	MiVoice Business (MiVB) System Administration Tool form
Network Element	MiVB System Administration Tool main menu page
Users and Services main page	User and Services Configuration
Reconcile Wizard Welcome page	Maintenance and Diagnostics > Backup/Restore > Backup

MiCollab User and Services Application page	MiVoice Business (MiVB) System Administration Tool form
User Templates > (Select Template) > Edit User Template	Users and Devices > Templates > User and Services Templates > (Edit Template)
Users > (Select User) >Edit User	Users and Devices >User and Services Configuration > (Selected User) > Summary
Users > (Select User) > Edit User > Phones > Open Service Details (for extension)	Users and Devices > Users and Services Configuration > (Selected User) > (Selected Phone) > Profile
Users > (Select User) > Edit User > Phones > Open Group in MiVB (for Group)	Users and Devices > Group Programming > Personal Ring Groups > (Selected Group)
	Users and Devices > Group Programming > Multi-Device User Groups > (Selected Group)

Typical Reach Through Tasks

From MiCollab to MiVoice Business

You can Reach Through from the MiCollab USP application into the MiVoice Business System Administration Tool to

- edit a phone's device's Service and Authentication Details (such as MAC, PLID, and so forth.)
- edit a Template's Phone Applications and Keys
- configure MiVoice Business system settings such as features, ARS, or trunking.
- resolve user entry conflicts that exist with the MiCollab database
- adjust MiVoice Business template settings
- configure a user's personal ring groups
- configure a user's multi-device user group
- perform database backups on a MiVoice Business network element.

From MiVoice Business to MiCollab

You can Reach Through from the MiVoice Business System Administration Tool into the MiCollab USP application to

- edit a user's or template's services: NuPoint, MiCollab Client, Teleworker, or AWV
- change a User's passcode.

How Reach Through is Supported

To support Reach Through, the USP application pages have been modified. The following images highlight the most significant modifications (see the table below the images for details).

Figure 1: Network Element Page

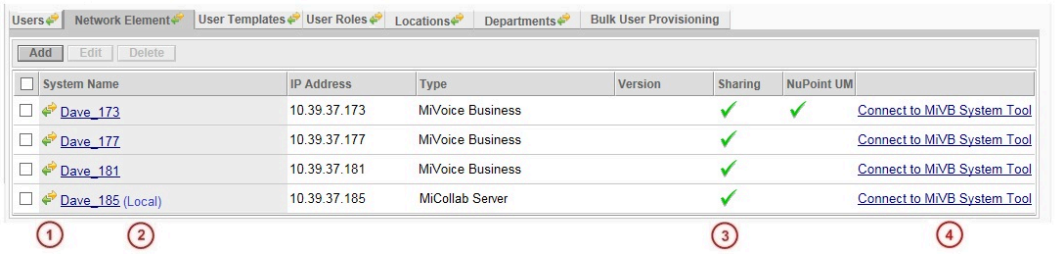


Figure 2: Edit User Page

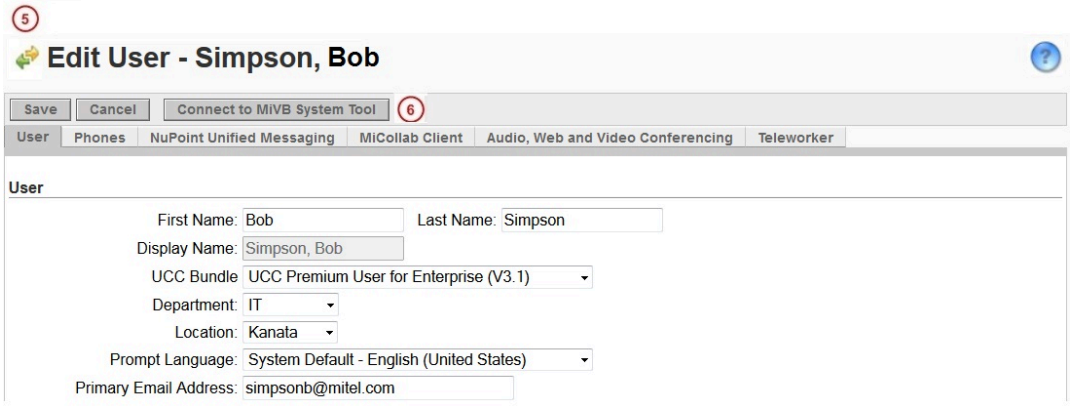


Figure 3: Phone Details

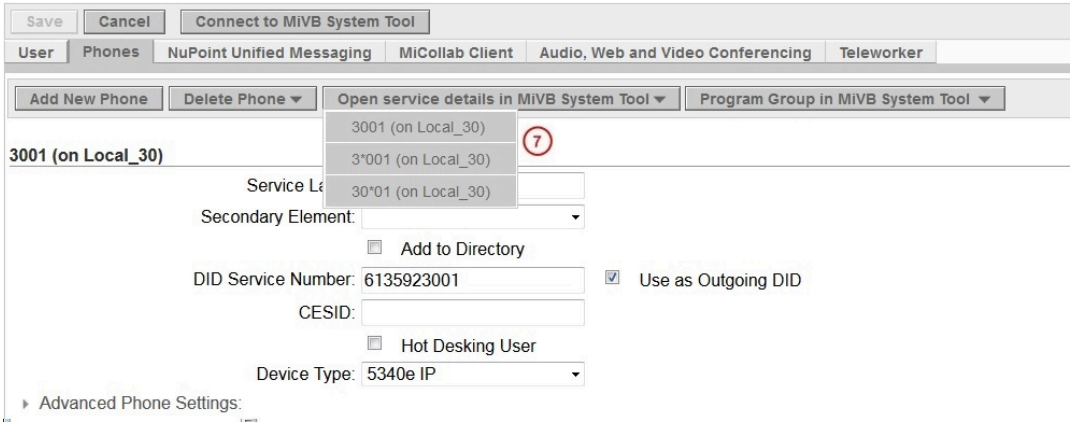


Figure 4: Group Details

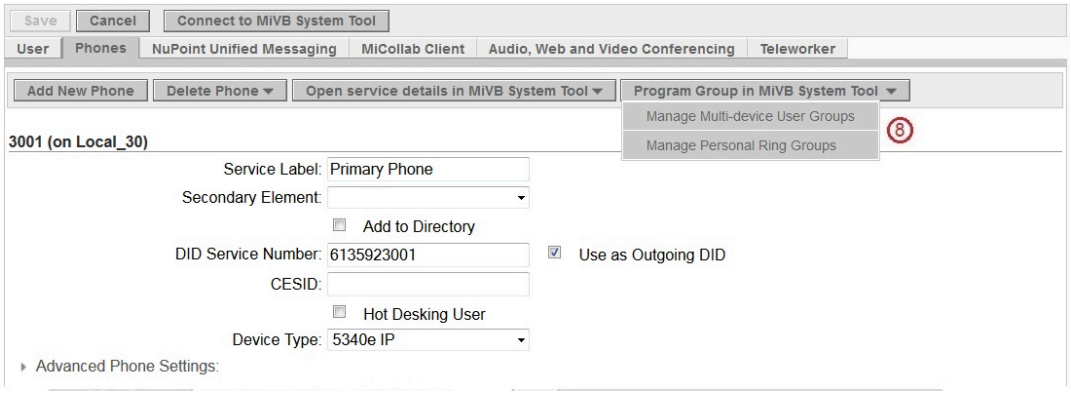


Table 1: Reach Through Support

Item	USP Page	Description
1	Network Element	 icon indicates that Flow Through Provisioning is enabled with the network element.
2	Network Element	(Local) identifies the MiCollab system that you are logged into.
3	Network Element	 indicates that database sharing is enabled with this element.
4	Network Element	Click Connect to MiVB System Tool to reach through to the MiVoice Business system administration tool (ESM) forms menu.
5	Edit User	 icon indicates that this user entry is being shared to other network elements.
6	Edit User	Click Connect to MiVB System Tool to reach through to the Users and Services form of the MiVoice Business system administration tool.
7	Phone Details	Select a phone extension to open the phone's service details in the User and Services Configuration form of the MiVoice Business system administration tool.
8	Group Details	Select a group extension to open the group's service details and members in the Multi-Device User Groups form of the MiVoice Business system administration tool.

9.1 Reach Through - Conditions

- Flow Through Provisioning must be enabled to the MiVoice Business network elements and the MiCollab database must be synchronized with the MiVoice Business network element databases (that is, the Reconcile Wizard Welcome page must identify that the databases are in sync).
- Reach through is enabled from MiCollab USP to the MiVoice Business (MiVB) system administration tool using the MiVoice Business "system" administrator account. The MiVoice Business must have an administrator account configured in the **User Authorization Profiles** form with Login ID "system" and System Admin authorization set to "True".
- Reach Through is only supported using Mozilla Firefox browsers and you must have installed the browser with the Mitel Root Certificate. If you attempt to use any other type of browser to reach through from MiCollab to MiVoice Business, reach through will be blocked.
- Reach through from MiCollab USP to the MiVoice Business System Administration Tool and from the MiVoice Business System Administration Tool to MiCollab USP is in the context of the "admin" account for audit purposes.
- You must enable the SNMP Agents on every element in the SDS Admin Group.
- It is not necessary to log in when performing Reach Through from the MiCollab USP application to the MiVoice Business System Administration Tool or vice versa. A trust relationship is established based on the fact that you have already logged in to one of these administration tools.
- If the MiVoice Business system is running on an Multi-Instance platform, you must add the IP addresses of the MiVoice Business System Administration Tool and the IP address of the Multi-Instance manager to the MiCollab trusted network.

For example, if the IP address of the system administration tool is 10.46.26.100, you would need to add the following IP addresses to the MiCollab trusted network:

10.46.26.100

10.46.26.101

A simpler option is to add the subnet to the trusted network (10.46.26.1).

9.2 Reach Through - Configuration

Configure MiVoice Business Administrator Account for Reach Through

Reach through is enabled from MiCollab USP to the MiVoice Business (MiVB) system administration tool using the MiVoice Business "system" administrator account. Ensure that there is a MiVoice Business administrator account configured in the **User Authorization Profiles** form with Login ID "system" and with System Admin authorization set to "True".

Note:
The Reach through feature is disabled by default for new installations. To enable the Reach Through feature, refer to MiVB Sharing.The administrator should ensure that "system" administrator account is used while enabling the Reach through feature. The default system admin policy assigned to 'system' (which is called root) allows the administrator access to every form in the system.

Enable SNMP Agents

Enable the SNMP agents on every MiVoice Business network element in the SDS Admin Group. This procedure clears the alarm that is generated when you start sharing between the MiVoice Business servers.

1. Launch the browser.
2. Navigate to the IP address of the MiVoice Business server.
3. Log into the System Adminstration Tool.
4. Navigate to Voice Network ⇒ Admin Groups
5. Click **Change**.
6. Select the admin group name.
7. Click **Save**.
8. Navigate to System Properties ⇒ System Administration ⇒ SNMP Configuration
9. Click **Change**.
10. Check 'Yes' for 'Enable SNMP Agent'.
11. Set a contact.
12. Set a location
13. Set the Read Only Community to 'public'.
14. Set the Read/Write Community to 'public'.
15. Click **Save**.

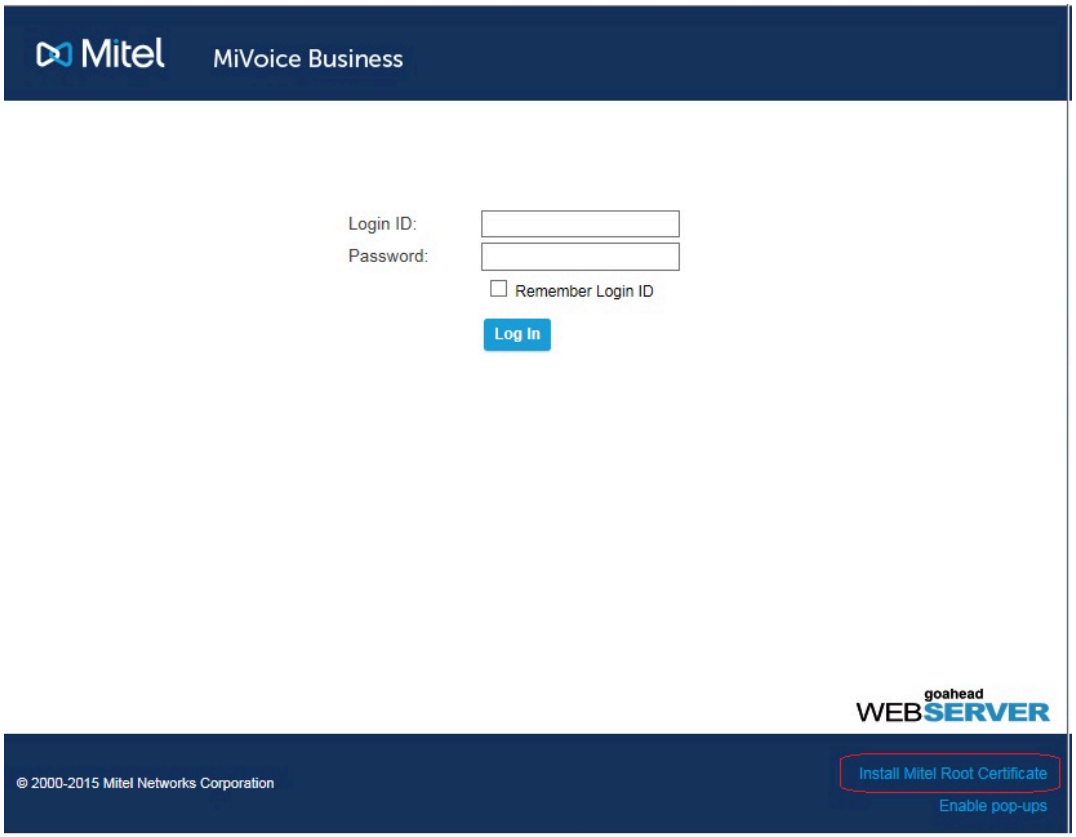
Note:
If you perform this procedure after sharing has been started, it may take a few minutes before the group alarm status clears.

Import MiVoice Business Mitel Root Certificate to Browser

MiVoice Business web server uses a Mitel signed certificate to encrypt web connections. A common certificate is used for all MiVoice Business platforms. To support reach through navigation from MiCollab server manager to the MiVoice Business system administration tool you must download this common Mitel

Root Certificate from one of the MiVoice Business servers and import it into your Firefox browser as a 'Trusted Root Certification Authority'.

1. Access the log in page of the MiVoice Business System Administration tool.



2. Click Install the Mitel Root Certificate.
3. Save the Mitel Root Certificate to a location on your PC hard drive.
4. Follow the instructions for your Firefox browser to import the file.

For Internet Explorer browsers only, you must also add the MiVoice Business servers to the 'Local intranet' security zone:

1. Under **Tools**, click **Internet Options**.
2. Click **Security**, click **Local intranet**, and then click **Sites.**
3. Click **Advanced** and add the IP addresses of the MiVoice Business systems as websites.
4. Click **Close**.

Upload or Import Trusted Root Certificate

If the trusted Mitel root certificate is not installed on your PC, you will receive security certificate warnings when you access MiVoice Business tools, such as the System Administration Tool.

To prevent these warnings from appearing, you install the Mitel Root Certificate in your browser.

Upload MiVoice Business Mitel Root Certificate to MiCollab Server

1. Access the log in page of the MiVoice Business System Administration tool.
2. In the bottom right corner of the login screen, click Install Mitel Root Certificate.
3. Follow the instructions for your browser.

OR

Import MiCollab Web Server Certificate to Your Browser

1. Log into the MiCollab server manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Download the current web server certificate**.
5. Click **Perform**.
6. Click **Download**.
7. Select **Open with WinZip** and click **OK**.
8. Extract the certificate file to a folder on your local PC.
9. Import the certificate file from your PC into your browser as a "Trusted Root Certification Authority".

To import the certificate into Firefox

1. Launch Firefox.
2. Navigate to the IP address of the MiVoice Business server.
3. Click **I Understand the Risks** followed by **Add Exception...**
4. Clear the **Permanently store this exception** check box, and then click **Confirm Security Exception.**
5. After you confirm the exception, the MiVoice Business System Admin Login page is displayed. You can now install the Mitel Root Certificate..
6. Click the Firefox button at the top of the Firefox window and select **Options** ⇒ **Options** (or select it from the **Tools** menu if the Menu Bar is showing).
7. Click **Advanced** ⇒ **Certificates** (or Encryption in older versions of FireFox ⇒ **View Certificates**.
8. Make sure the focus is on the Authorities tab and then click Import.
9. Navigate to the mitelcert.cer file you saved and click **Open**.
10. In the resulting dialog box, select **Trust this CA to identify websites** and T**rust this CA to identify software developers**.
11. Click **OK**.

After the certificate is installed, exit FireFox, and then restart it. You can now log in to MiVoice Business and not receive the security certificate warnings.

Note:
If you are unable to log in, clear your browser cache, and then try again.

Set up Security Exceptions for Application Reach Through

The popup blocker must be disabled and security exceptions created as these interfere with application reach through.

Firefox

1. Launch Firefox.
2. Click the Firefox button at the top of the Firefox window and select **Options > Options** (or select it from the **Tools** menu if the Menu Bar is showing).
3. Choose **Content**.
4. Clear the **Block pop-up windows** check box or click **Exceptions** and add the IP addresses of the MiVoice Business servers to the list of websites to allow.
5. Click **OK** to close the Options dialog.

Extend the MiVoice Business System Administration Security Session Timeout

By default, System Administration Tool sessions time out after 15 minutes of user session inactivity. You can adjust the time out period as follows:

1. Launch the browser.
2. Navigate to the IP address of the **PRIMARY** MiVoice Business server.

1. Log in (Login ID 'system', Password 'default').
2. Click **System Administration Tool**.
3. Navigate to **System Properties** ⇒ **System Administration** ⇒ **System Security Management**.
4. Click **Change**.
5. Set the User Session Inactivity Period to 720.
6. Click **Save**.

Trust the Self-signed Certificate

To avoid receiving trusted certificate warnings when using the server manager interface, perform this procedure:

1. Launch the browser.
2. Navigate to the Local IP address of the MiCollab server manager (that is https://<ip of MiCollab>/server-manager)
3. You are prompted to stop because the server uses a self-signed certificate.

4. Override the default choices and continue to the server.
5. Login (Username = admin, Password = default).
6. Navigate to **Security** ⇒ **Web Server Certificate**.
7. Select **Download the current web server certificate**.
8. Click **Download**.

   The web server certificate is saved as a zip file.
9. Open the zip file and extract the certificate contained within it.
10. Import the certificate into your browser.

Firefox

1. Launch Firefox.
2. Click the Firefox button at the top of the Firefox window and select **Options** ⇒ **Options** (or select it from the Tools menu if the Menu Bar is showing).
3. Click **Advanced** ⇒ **Certificates** ⇒ **View Certificates**.
4. Make sure the focus is on the **Authorities** tab and then click **Import**.
5. Navigate to the extracted certificate (.crt) file you extracted from the zip above and click **Open**.
6. In the resulting dialog box, select **Trust this CA to identify websites** and **Trust this CA to identify software developers**.
7. Click **Ok**.

Add IP Addresses to MiCollab Trusted Network (MiVB Multi-Instance platforms only)

If your system is a MiVoice Business Multi-Instance platform, you must add the IP addresses of the MiVoice Business System Administration Tool and the IP address of the Multi-Instance manager to the MiCollab trusted network.

For example, if the IP address of the system administration tool is 10.46.26.100, you would need to add the following IP addresses to the MiCollab trusted network:

10.46.26.100

10.46.26.101.

A simpler option is to just add the subnet to the trusted network (that is, 10.46.26.1).

To add the IP addresses to the MiCollab trusted network, see Configure Networks.

Remove Embedded Voicemail from the default template

MiCollab default templates create directory numbers with a mixture of n and n+1 length (1000, 1*000, 10*00) and so forth. This format is incompatible with embedded voice mail. MiCollab Release 7.0 and later uses the default template as the basis for MSCR calls to create new phones, regardless of which role is selected. Therefore, you must remove the embedded voice mail feature from the default template in the MiVoice Business.

1. Launch a new browser.
2. Navigate to the IP address of the MiVoice Business server.
3. Log in (Login ID 'system', Password 'default').
4. Click System Administration Tool.
5. Navigate to **Users and Devices** ⇒ **Templates** ⇒ **User and Service Templates**.
6. Right-click on the Voicemail template and choose **Delete Voicemail** then click **OK** in the confirmation dialog.

9.3 Using Reach Through

To reach through to a MiVoice Business system, click the **Connect to MiVB System Tool**, **Open Service Details in MiVB System Tool**, or **Open Group Details in MiVB System Tool** button in one of the supported pages.

Note:
Reach Through is only supported using Internet Explorer or Firefox browsers and you must have installed the browser with the Mitel Root Certificate. If you attempt to use any other type of browser to reach through from MiCollab to MiVoice Business , reach through will be blocked.

- If the MiVoice Business server is reachable, the MiVoice Business system administration tool opens in a new browser window. You do not need to sign in again to the MiVoice Business system since you have already signed into MiCollab .
- If you click another reach through link or button in USP, the MiVB system tool form opens in a new tab.
- In the case of a hosted context (for example, reaching through to a user with phone services, or to a template which contains phone services) the reach through targets the MiVoice Business which is the primary host (home element) of the user's phone services.
- In the case of a non-hosted context (for example, reaching through to a template with no phone services or to the backup form) reach through will arbitrarily select one of the MiVoice Business servers in the local administration group.

About SDS Distribution Errors 10

This chapter contains the following sections:

- Resolving Distribution Errors
- Exporting Error Data
- Viewing Data Distribution Alarms

Flow Through Provisioning synchronizes user and services data updates between the MiCollab database and MiVoice Business system databases in a sharing network. If you make an update in the MiCollab USP database and the update is not successfully shared to all the other elements in the sharing network, a distribution error is sent to the MiCollab SDS Distribution Errors application. If the number of distribution errors exceeds an SDS alarm threshold, a data distribution alarm is generated in the Event Viewer application.

The SDS Distribution Error application allows you to view and manage distribution errors and pending updates:

- **Distribution Errors** are updates that could not be applied to the destination elements.
- **Pending Updates** are updates that have not yet been applied to the destination elements.

From this application, you can:

- reload the list of distribution errors
- export the errors to a file
- delete updates
- retry failed updates
- filter errors in the list.

Launching the SDS Distribution Error Application

Note:
The SDS Distribution Error application is only available if Flow Through Provisioning has been enabled between MiCollab and MiVoice Business platforms.

1. Under **Administration**, click **SDS Distribution Errors**.
2. Resolve any distribution errors.

Field Descriptions

Parameter	Description
	Click to select a record

Parameter	Description
	Click to display the details for the record.
Action ID	A unique number sequence that identifies the transaction of a specific shared form distribution attempt.
To	Indicates the destination network element for the membership data. **Note**: This field displays the name of the destination network element as it appears in the Network Elements form of the MiVoice Business system.
Date/Time	Displays the date and time that a distribution transaction was attempted.
Last Retried	Displays the date and time of the most recent failed update retry.
Action	Specifies the configuration action type (for example: add, modify, or delete).
MiVB Form Name	Identifies the name of the MiVoice Business form from which the data distribution originated.
Error Type	The types of distribution error messages include: • Transport errors - failures of data update event delivery • Application errors - failures of data update transaction at destination • Concurrency error - conflicting data update information at the destination because • a change was made to a record but the original record on the remote system(s) was not in sync with the original record on the local (master) system, or • a change was made at the same time by two or more administrators on the same record. • Transport and Concurrency Error • Application and Concurrency Error
Reason	Displays an error message.

Parameter	Description
Status	Displays the status of the update: • Idle - awaiting Retry operation • Retry Pending - administrator has retried the update and a system response is pending. • Pending - automatic update has been sent and a response is pending. **Note**: The status field is updated approximately every 30 seconds.
Count	The Count in the lower left corner of the Distribution Error screen displays the total number of error listed.

10.1 Resolving Distribution Errors

Data distribution errors and pending updates are collected and displayed in the MiCollab Distribution Error application. If there are errors, a warning message is displayed at the top of the server manager interface. The message is a reminder to resolve the errors. It goes away when there are no more errors or when the check box to skip the message is selected. You must resolve data distribution errors that were initiated from MiCollab USP from the Distribution Error application. To resolve distribution errors:

- Review the updates
- retry the updates
- correct the data conflict and then delete the update, or simply delete the update if you determine that the update is not required

Review Updates

1. Under **Administration**, click **SDS Distribution Errors**. The pending updates and errors are listed.
2. Click **Reload** to refresh the table. If new distribution errors occur while you are viewing the table, the table is not updated automatically. You must click **Reload** to see the latest view.
3. To customize the way data records are displayed, you can right-click on the column header and

   - *Sort Ascending*: sort the column data in ascending order.
   - *Sort Decending*: sort the column data in descending order.
   - *Group by Form Name*: allows you to group records by form name
   - *Ungroup*: click to ungroup a previously grouped set of records.

4. Click the icon  to display the details for a specific record.

Retry Updates

To manually retry updates:

1. Select a record that has a Status of "Idle". Only "Idle" records can be retried.
2. Click **Retry**, select **Retry Selected**, and then click **OK** to update the remote node with the record from the local node. "Retry Pending" appears in the Status field of the record. If the update is successful the update record disappears from the list. If you retry an update and the update fails, the record is temporarily highlighted.

> **Note**:
> To retry all idle records, click **Retry** and then select **Retry All,** and then click **OK**. If you have applied a filter to the list, then **Retry All** only applies to the displayed "Idle" records.

3. Click **Reload** to update the main window with the latest data.

> **Note**:
> The system automatically retries "transport" errors. Updates that are fixed by the system will disappear from the Distribution Errors window after a **Reload**.

The system automatically retries data updates that are not successfully transported to the destination element (due to a network or element failure). The following conditions apply to system initiated automatic retries:

- Automatic retries are started every 30 seconds.
- Updates are retried from oldest to newest based on the initial time stamps of the record.
- Automatic retries yield to manual retries and new updates.

The following data updates are not automatically retried

- updates that fail because an application on the destination element was unable to write the data to its database
- updates that fail because the same data was updated concurrently.

Delete Updates

1. Correct the data conflict on the network element or confirm that the update is not required.

Note:
Deleting an error record could result in data inconsistencies that cause subsequent retry operations to fail because of a dependency between the records. Only delete an error record if you understand the error and have determined that the update is not required.

2. Select a record that has a Status of "Idle". Only "Idle" records can be deleted.
3. Click**Delete**, select**Deleted Selected**, and then click**OK**to remove the record. If the delete operation fails to remove the record, the record is temporarily highlighted.

Note:
To remove all idle records or all selected idle records, select the **Delete All** or **Delete Selected** options and then click **OK**. If you have applied a filter to the list, then **Delete All** only applies to the displayed "Idle" records.

4. Click **Reload** to update the main window with the latest data.

10.2 Exporting Error Data

You can export the records that are listed in the Distribution Errors application table.

1. Under **Administration**, click **SDS Distribution Errors**.
2. Click **Reload** to refresh the table. You must click **Reload** to see the latest view.
3. Click **Export**.

Note:
Only the records displayed in the table will be exported.

4. Select the file type:

   - CSV (Excel)
   - XLS (Excel 97)
   - XLSX (Excel 2007/OOXML)

5. Click **Export**.
6. If prompted, **Open** or **Save** the exported data file. By default, the system saves the file with the name "SDSDistributionErrors" (for example, SDSDistributionErrors.csv).

10.3 Viewing Data Distribution Alarms

Data Distribution alarms are displayed in the Event Viewer application. The system generates a minor alarm after the number of SDS Distribution Errors exceeds 100, and a major alarm after the number exceeds 1000. There is no Critical alarm for such errors. Fewer than 100 errors results in a warning alarm at the top of the server manager interface. Alarms are cleared by resolving the distribution errors. After the number of errors falls below the threshold level the system clears the alarm. You can also clear the alarm from the Event Viewer application.

Distribution errors are typically caused by the following error conditions:

- the device associated with the data distribution error is not programmed properly on the remote controller
- a required feature or feature option is not enabled on the remote controller.
- the network connection to the remote controller is down (results in a large number of errors).

The maximum number of updates that can accumulate is 60,000. After the 60,000 limit is reached, the system will prevent you from making any further changes to the records in the shared forms. In addition, any changes to telephone user data through the telephone user interface (TUI) will not be shared between the primary and secondary controllers. Before the system will allow you to start making changes again, you must reduce the number of errors in the Distribution Error application (see Resolving Distribution Errors).CHECK WITH SDS DESIGN GROUP

About the Bulk User Provisioning Tool 11

This chapter contains the following sections:

- Bulk Import from File
- Auto Fill Selection
- Add User Entries
- Correcting Errors

The Bulk User Provisioning tool allows you to perform the following tasks:

- add user entries to the database
- bulk import user data from a .csv or LDIF file
- program a range of fields using Auto Fill Selection prior to saving imported entries to the database
- manage detained and failed IDS updates.
- importing contacts using BUP

Note:
For MiCollab with MiVoice MX-ONE or MiVoice Office 400 integrations, you only use the Bulk User Provisioning Tool to import a .CSV file of users into MiCollab from the communications platform during initial provisioning and to synchronize MiCollab Client contacts with a directory server. Contacts that fail to be imported during a directory server synchronization are listed in the Manage Detained Queue. You do not use the Bulk User Provisioning Tool for MiCollab with MiVoice 5000.integrations.

You can perform user data operations such as adds or edits in the Bulk Provisioning tool grid and then save the operations to the Users and Services database. The Bulk User Provisioning Tool has three modes:

- **Bulk User Add:** This mode allows you to add records into the grid of the tool. You can then save the newly added records to the User and Services database.
- **Bulk User Edit:** This mode allows you to edit the users' passwords in bulk. You can select user names from the .CSV file and change the password by clicking the **Reset Password** button.
- **Manage Detained Queue**: This mode allows you to manage detained and failed Integrated Directory Service (IDS) operations. Detained IDS operations are operations that have been performed on the directory server that have not been applied to the USP database yet. Failed IDS operations are directory server updates that the MiCollab system could not apply to the USP database due to errors.

Note:

The administrator can create the contacts as basic users from Bulk User Provisioning tab.

The total number of records in the Bulk Provisioning tool is displayed in the lower-left corner of the grid.

Bulk User Provisioning Tool - Element Descriptions

Element	Description	Notes
Mode	Selects the Bulk Provisioning tool mode of operation.	The bulk user tool has three modes of operation: • Bulk User Add • Bulk User Edit • Manage Detained Queue
Add	Adds a new blank user record in to the grid.	You can add new records in all four operational modes.
Delete	Deletes selected user records from the grid.	Check the box next to a record to select it.
Save	Performs the operations that are specified in the grid for each record.	Add, Update, and Delete operations are applied to the Users and Services database upon Save.
Reset Password	Resets the passwords of selected users.	Select the user names from the imported .CSV file and click the **Reset Password** button. When prompted, click **OK** to confirm your selection. Bulk User Provisioning for resetting the selected users' password takes effect. Each user receives a welcome email which will contain a new temporary password. Users must log in to the **End User** portal using the temporary password and specify a new password. **Note**: The **Reset Password** option will not work for MiCollab installations that have the welcome email disabled. In this case you must re-enable the welcome email.

Element	Description	Notes
Tools	Download Example CSV File	Download an example CSV file that you can use to create an import file of data entries.
	Import from File	Import entries from a CSV or LDIF file into the Bulk User Provisioning tool
	Empty Detained Queue	Remove all entries from the Detained Queue quickly.
	Reload Detained Queue	Refresh the data entries in the grid from the Detained Queue.
	Reload Grid from Cache	Refresh the data entries in the grid from the server cache
	Click  to expand the row and display the current user and service details for this record. If there are any errors associated with the record, a detailed summary of the error is provided.	Prior to performing an **Add** or **Delete** operation, use this function to identify the detailed changes that will be made to the database.
	Check the box to select a record.	To select all records, check the box in the table header.
 	Click  and  to sort column data.	You can sort column data in ascending or descending order. You can also configure custom sorting criteria.
OP	This column indicates the operation for each entry, for example: **A** (Add), **U** (Update), and **D** (Delete). The operations are applied when you click **Save**.	Hover your cursor over the letter to display the operation. Add, update, and delete operations are applied to the User and Services database on **Save**.
Timestamp (Managed Detained Mode only)	Shows the date and time of when the entry entered the detained queue.	

Element	Description	Notes
First Name	Enter user's first name.	Enter a first name up to 256 alphanumeric characters in length (for example, "Bob"). This field is optional and can be left blank.
Last Name	Enter user's last name. For example: "Smith".	Enter a last name up to 256 alphanumeric characters in length (for example, "Smith"). This field is mandatory.
Domain	The Domain Name is read-only and is either read from a directory server or set to the local domain	You can only manage non-local domains from the directory service or by performing an LDIF file import. The domain field is set in the LDIF file and should not be changed. In all other cases, the domain field is set to the local domain.
Login ID	Enter a login ID for the user.	For example, "smithb".
Email Address	Enter a unique primary email address for the user. For example: "smithb@mitel.com"	Use the format " name@place.suffix", where • name is 2 to 40 characters in length • place is 2 to 40 characters in length • suffix is from 2 to 6 characters in length • address does not contain special characters.
Role	Select the desired role for this user.	When you save the user, the template associated with the role is applied to the entry.
Prime Phone	Enter the directory number of the user's prime phone.	
Secondary Phone	Enter the directory number of the user's secondary phone.	
External Number	Enter the number of the user's external phone.	

Element	Description	Notes
Direct Inward Dial Number	Enter the dialing prefix and external number of the designated DID trunk.	Direct Inward Dialing (DID) routes incoming calls on a designated trunk to the user's phone.
SIP Password	Enter the SIP password which is passed to MBG to authenticate the SIP user.	
	Indicates an error in a data field	Hover your cursor over the error icon for information.
	Indicates that the data entry failed to import into the database.	Click the icon for a detailed report.

Note:
In MX-ONE integration, the secondary phone is an attribute of the primary phone. The secondary phone can be set or not set from MX-ONE provisioning manager.

Note:
To use the Teleworker services in MiVoice Office 400 or MiVoice MX-ONE, **SIP Username** field must be added manually in the example csv file.

Customizing the Column Data

You can customize the way data entries are displayed in the Bulk User Provisioning tool. By right-clicking in the column header and selecting the desired menu item, you can

- sort a column of text entries alphabetically in either ascending or descending order
- sort a column of numbers in either ascending or descending order
- configure a custom sort based on column headings
- group entries according to the data in a column heading

You can also

- move a column by clicking the header and dragging it to a new position
- adjust a column width by selecting the right border of the column header with your cursor and dragging it to the left or right.

Note:
After you reload the data or switch to a new tab, the sort order reverts to the default. The default sort order is as follows:

- Error icon (ascending order based on description)
- Last Name (ascending order)
- First Name (ascending order).

11.1 Bulk Import from File

Use the Bulk User Provisioning Tool to provision users and services. The tool allows you to perform the following tasks:

- import a database of user entries from a file
- edit the user entries in the online editor, and then
- upload the entries into the MiCollab Users and Services database.

Conditions

- You cannot use the bulk import feature to change existing user records in the database. Bulk import is for adding new users and services only.
- You can import user data from the following source files:
- • comma-separated value (CSV) file exported from a communications platform
  - LDAP Data Interchange Format (LDIF) file exported from a directory server.
- You cannot import MiCollab Client contacts via a CSV or LDIF file.
- Contacts imported via Active Directory are displayed as read-only in the Bulk User Provisioning tool.
- You must open the **Example CSV File** (BUPExample.csv) in Microsoft Excel and use it to import your user data. It is not possible to bulk add a user by manually data-fill (typing into the grid).
- The maximum import file size is 5000 entries.
- MiCollab users can be configured with multiple phones and each phone extension consumes a device (Multi-Device User Group device) on the MiVoice Business system. On a 2500 or 5000-user MiCollab system, it is possible to exceed the device limits of the MiVoice Business system(s). To minimize the possibility of over provisioning, do not assign users with unnecessary phones. Also, during initial bulk provisioning of a 2500 or 5000-user MiCollab system, create roles and templates that assign the actual phone requirements for the users. For example, if you have UCC Premium users who only require two phones, create and apply a "UCC Premium - 2 phone" role and template. If you use the default

UCC roles and templates, the maximum number of phones are applied, increasing the risk of over provisioning.

- The Bulk User Import Tool does not support importing MAC addresses from the CSV file.
- Disable Skype plug-ins before you import records using the Bulk User Provisioning tool. Skype plug-ins can cause the BUP import process to be very slow or in extreme cases stop functioning.
- 2-byte UTF-8 character format is supported in the following User and Services application fields: First Name, Last Name, and Role. To import entries with UTF-8 characters, you must import them from a CSV or LDIF file that supports UTF-8 encoding. Use an editor (for example, Notepad++) that supports UTF-8 encoding to create the import file.

Note:

Do not use an Excel file. Excel does not display UTF-8 characters properly in CSV files, even if the encoding is set to UTF-8. Also, if you are importing from an LDIF file, ensure that only ISO-8859-1 characters are present in the file. For LDIF import files, the Users and Services Bulk User Provisioning tool only supports the ISO-8859-1 character set.

- The Bulk Import from File functionality is not supported for MiCollab integrations with the MiVoice 5000. However, MiCollab Client contacts that fail to be imported during a directory server synchronization can be managed from the Manage Detained Queue.
- For MiCollab with MiVoice Office 400 or MiVoice MX-ONE integrations, you only use the Bulk User Provisioning Tool to import users into MiCollab. You can export a CSV file of user entries from the communications platform and then import the user entries into the MiCollab system using the Bulk User Provisioning (BUP) tool in USP. Note that an import CSV file for the BUP tool can contain a maximum of 5000 users.

Note:

The Flow Through Provisioning feature shares MiVoice Business templates with the MiCollab system. The MiVoice Business templates support key template programming for users created from MiCollab USP. However, when a key template is created on the MiVoice Business system, the template is not validated for incomplete key programming (such as a missing ring type in a DSS/BLF key). The system only generates errors when you attempt to apply the invalid key template to a user via a role. Therefore, whenever you create a new key template on the MiVoice Business, ensure that you test it by applying it to a MiVoice Business user. If you receive errors related to key programming when you attempt to apply a shared template, you must correct the key template on the MiVoice Business.

Import File Format

The file must include the mandatory headers listed in the following table:

Column Header	Mandatory or Optional	Format	Notes
First Name	optional	Up to 256 characters. UTF8 characters are supported; however, ordinal indicator characters are not displayed correctly in the First Name and Last Name fields across MiCollab applications.	The first name or last name must be provided.
Last Name	mandatory		
Login ID	mandatory	2 to 21 characters. Limited to ASCII (non-accented) characters (@, comma, or space are not allowed).	A login ID is generated from the user's first and last name if this value is missing. This field does not apply to corporate contacts.
Email Address	optional (unless required by template for specified role)	Must be a valid e-mail address. Limited to ASCII (non-accented) characters.	Email address is mandatory if MiCollab Audio, Web and Video Conferencing is included in the template.
Role	mandatory	UTF8 characters are supported.	The roles that you specify in the Import file must be programmed in the Roles tab of the User and Services application (with the exception of the default Contact role). Otherwise, warnings will be present after you import the entries into the Bulk User Provisioning tool. The Role that you assign to a user must correspond to the user's MiVoice Business network element.
Primary Phone	optional (unless required by template for specified role)	1 to 7 digits, # or *. No spaces	Directory number must be unique (cannot already exist in system directory). For non-corporate contacts, external numbers are permitted.

Column Header	Mandatory or Optional	Format	Notes
Secondary Phone	optional (unless required by template for specified role)	1 to 7 digits, # or *. No spaces.	Directory number must be unique (cannot already exist in system directory). For non-corporate contacts, external numbers are permitted.
External Number	optional (unless required by template for specified role)	E.164 format is supported.	This column is mandatory if the selected template requires an external hot desk user (EHDU) number. For MiCollab with MiVoice MX-ONE integrations, this field only applies to MiCollab Client contact entries.
DID Number	optional	E.164 format is supported	Direct Inward Dialing (DID) routes incoming calls on a designated trunk to the user's phone. Enter the dialing prefix and external number of the designated DID trunk. This field only applies to MiCollab with MiVoice Business integrations. Not applicable to corporate contacts
SIP Password	optional (unless required by template for specified role)	Up to 26 characters (ISO-8599-1). This field can be blank.	SIP password which will be passed to MBG to authenticate the SIP user. This column is mandatory if the selected template requires a SIP Password.
ID	optional	E.164 format is supported	

Note:
For MiVoice MX-ONE, DTS Phone field is treated as Secondary Extension.

Import from .CSV File

1. Export the user data from the MiVoice Business , MiVoice MX-ONE, MiVoice Office 400 or MiVoice Office 250 communications platform to a CSV file. For MiVoice Business systems, you can export the user data from the User and Device Configuration form (refer to the *MiVoice Business System Administration Tool* online help for instructions).
2. In the MiCollab server manager, under **Applications** click **Users and Services**.
3. Click the **Bulk User Provisioning** tab.
4. Click **Tools**, click **Download Example CSV File**, scroll down to the bottom of the screen, and then click **Open**. The file (BUPExample.csv) opens in Excel. The BUPExample.csv file is shown below:

1. Copy the communication platform user data from the exported file into the import file spreadsheet columns, starting at row 2.

   MiVoice Business Specific Information:

   The following table shows how the BUP file headings map to the MiVoice Business User and Service Configuration form headings. Refer to the notes provided below for additional guidelines.

BUP File Column Heading	User and Services Configuration File Column Heading
First Name	First Name
Last Name	Last Name
Login ID	Login ID
Email Address	Email
Role	Not applicable - you need to create roles on MiCollab and specify one of the roles in the BUP file.
Primary Phone	Number
DID Number	DID Service Number
SIP Password	

BUP File Column Heading	User and Services Configuration File Column Heading
Department	Department
Location	Location

MiVoice Business Specific Notes:

- If you are importing a Bulk User Provisioning file to migrate to Flow Through Provisioning, the phone service details (for example: Device Type) are irrelevant. The sync and reconcile operation that runs at the end of the start sharing process assigns the users' phone services from the MiVoice Business database to the MiCollab user entries.
- In MiVoice Business, Login IDs are case sensitive (so, smithF and smithf are two unique Login IDs). However in MiCollab, Login IDs are not case sensitive (so, smithF and smithf are the same Login ID). To avoid conflicts during the synchronization, ensure that all Login IDs consist of a unique set of characters.

1. Click the **Office Button**  , click **Save As**, click **Other Formats** and then save the file type as CSV (comma delimited) (*.csv).
2. If you are prompted to "keep the workbook in this format", click **Yes**. Close the file.
3. Click **Tools** and then click **Import from File**. The Import from File window opens.
4. Select **Import Bulk Add CSV File**.
5. Click **Browse** and navigate to the .csv file.
6. Select the file and click **Open**.

Note:
Ensure that you disable Skype plug-ins before you import records using the Bulk User Provisioning tool. Skype plug-ins can cause the BUP import process to be very slow or in extreme cases stop functioning.

1. Click **Import**. The data from the .csv file is imported.
2. If the import is successful, the entries are listed in the Bulk User Provisioning Tool. Invalid entries are indicated with error icons. Correct any invalid entries.
3. Ensure that an appropriate role is assigned to each user.
4. If required, add user entries to the grid, or remove user entries from the grid.
5. Check the boxes next to the entries that you want to save to database. Click the box in the table header to select all entries.

6. Click **Save**. The Operation Progress window opens and displays the save to database progress. If necessary, you can stop the save process at any time by clicking **Cancel**. The Bulk Add Progress window closes and you return to the Bulk User Add screen. The screen displays error icons for any entries that were not saved to the database.
7. After the import is complete, the Operation Progress window closes.
8. Click the **Users** tab and check to ensure that all the entries are listed correctly.

Import from LDIF File

Note:
You cannot import a MiVoice MX-ONE LDIF into MiCollab. Although the MiVoice MX-ONE manager (AM7450) supports LDIF export, the format of the LDIF file is not compatible with MiCollab.

To import data from a .LDIF file:

1. Export the user data from the directory server to a LDIF file and save the file in a directory on your client PC.
2. In the MiCollab server manager, under **Applications** click **User and Services**.
3. Click the **Bulk User Provisioning** tab.
4. Click **Tools** and then click **Import from File**. The Import from File window opens.
5. Select **Import LDAP Data Interchange Format (LDIF) File**.
6. Click **Browse** and navigate to the LDIF file.
7. Select the file and click **Open**.
8. Click **Import**. The data from the LDIF file is imported.
9. If the import is successful, the entries are listed in the Bulk User Provisioning Tool. Invalid entries are indicated with error icons. Correct any invalid entries.
10. Ensure that an appropriate role is assigned to each user. Note that you can use Auto-Fill to quickly complete the roles for a selection of users.
11. Check the boxes next to the entries that you want to save to database. Click the box in the table header to select all entries.
12. Click **Save**. The Operation Progress window opens and displays the save to database progress. If necessary, you can stop the save process at any time by clicking **Cancel**. The Bulk Add Progress window closes and you return to the Bulk User Add screen. The screen lists any entries that were not saved to the database.
13. After the import is complete, the Operation Progress window closes.
14. Click the **Users** tab and check to ensure that all the entries are listed correctly.

11.2 Auto Fill Selection

The Auto Fill Selection function allows you to quickly complete the following fields across a selection of user entries in the Bulk User Provisioning tool:

- Role
- E-mail Address
- Login ID
- Directory Numbers.

On a new system, if you have a database that contains only user names, you can use roles and templates in combination with Auto Fill Selection to complete user and services provisioning. After you create the roles and templates, use Auto Fill Selection to assign user entries in the Bulk User Provisioning tab with roles, directory numbers, and e-mail addresses.

Auto Fill Roles

1. Import a file of user entries into the Bulk User Provisioning tool. See Bulk Import from File for instructions.
2. In the left-most column, check the boxes of the user entries that you want to auto fill.
3. Place your cursor in the **Role** column header, right-click and select **Auto Fill Selection**. The Auto Fill Role dialog box opens.
4. Select the role that you want to apply to the selected entries.

Note:
Any existing role would be overwritten with the new role.

5. Click **Auto Fill**. The Role fields for the selected entries are updated with the new role.
6. Click **Save**. The Operation Progress window is displayed. When the operation is complete, the directory is updated with the user entries. The user entries contain the template data of the assigned role.

Auto Fill Directory Login ID

The auto fill Login ID function allows you to program a selection of user entries with login IDs.

Note:
Do not program users from the MCD System Administration Tool; otherwise, conflicts could occur. Instead, program users only from MAS and use single point provisioning to update the MCD system.

1. Import a file of user entries into the Bulk User Provisioning tool. See Bulk Import from File for instructions.
2. In the left-most column, check the boxes of the user entries that you want to auto fill. Only selected entries are auto-filled. If a selected entry is already programmed with a directory number, the number will be overwritten.

3. Place your cursor in the Login ID column, right-click and select **Auto Fill Selection**. The Auto Fill dialog box opens.
4. Specify the Login ID format.
5. Click **Auto Fill**. The Directory Number fields for the selected entries are updated from the specified Starting Directory Number.
6. Click **Save**. The Operation Progress window is displayed. When the operation is complete, the user directory is updated with the login IDs.

Auto Fill Directory Numbers

The auto fill directory number function allows you to program a selection of user entries with a consecutive range of directory numbers.

Note:
Do not program users from the MCD System Administration Tool; otherwise, conflicts could occur. Instead, program users only from MAS and use single point provisioning to update the MCD system.

1. Import a file of user entries into the Bulk User Provisioning tool. See Bulk Import from File for instructions.
2. In the left-most column, check the boxes of the user entries that you want to auto fill. Only selected entries are auto-filled. If a selected entry is already programmed with a directory number, the number will be overwritten.
3. Place your cursor in a column that contains directory numbers (for example, PrimePhone or SecondaryPhone) right-click and select **Auto Fill Selection**. The Auto Fill dialog box opens.
4. Enter the starting Directory Number.
5. Click **Auto Fill**. The Directory Number fields for the selected entries are updated from the specified Starting Directory Number.
6. If there are other columns that require directory numbers, select each column and run Auto Fill Selection to add them.
7. Click **Save**. The Operation Progress window is displayed. When the operation is complete, the user directory is updated with the directory numbers.

Auto Fill Email Addresses

Use auto fill to enter corporate e-mail addresses into entries with blank e-mail address fields.

1. Import a file of user entries into the Bulk User Provisioning tool. See Bulk Import from File for instructions.
2. In the left-most column, check the boxes of the user entries that you want to auto fill. Only selected entries are auto-filled. If a selected entry is already programmed with an e-mail address, it will be overwritten.
3. Place your cursor in the **Email Address** column, right-click and select **Auto Fill Selection**. The Auto-Fill Email Address dialog box opens.
4. Select the name ordering.

5. Select the separator type.
6. Enter the domain name. A domain name is required.
7. Click **Auto Fill**. The e-mail fields are completed for all selected entries.
8. Click **Save**. The Operation Progress window is displayed. When the operation is complete, the user directory is updated with the e-mail addresses.

11.3 Add User Entries

To add user entries to the directory from the Bulk User Provisioning tool:

Note: You cannot add MiCollab Client contacts from the Bulk User Provisioning tool. Contactsin the Bulk User Provisioning tool are read-only. Modifications to contact entries should be made in the directory service.

1. Under **Applications** click **User and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the Mode field, select **Bulk User Add**.
4. Click **Add**. A row for a new user entry is added. The First Name column cell is enabled for data entry and the remaining column cells are blank. The column headings list the basic data fields for an entry without any application services.

> **Note**:
> The Domain Name is read-only and is either read from a directory server or set to the local domain. You can only manage non-local domains from the directory service or by performing an LDIF file import. The domain field is set in the LDIF file and should not be changed. In all other cases, the domain field is set to the local domain.

5. Enter data in the First Name (optional), Last Name, Login ID, and Role fields. When you select a role, the cells required for that role are automatically enabled for editing. A cell entry for the record is either enabled or disabled based on the assigned role and its associated template.
6. Enter data in the remaining column cells for the user as required. Use the scroll bar at the bottom of the window to show the columns to the left. If the entry is missing any required data for the specified role or if the field contains invalid data, error icons are displayed.
7. Click to review a summary of the user and services changes that will be applied to the database. If there are any errors associated with the entry, a detailed summary of the error is provided. You must resolve the errors before you can save the entry to the directory. Click **Done**.
8. Check the box to select the entry.
9. Click **Save**. The Operation Progress window opens. When the operation is complete the entry is added to the directory with the specified data.
10. Entries that cannot be saved to the database are identified with a failed import icon. You must resolve the error before you can save the entry to the directory. Click the failed import icon for details.

Note:
The grid can contain a maximum of 5000 records.

11.4 Correcting Errors

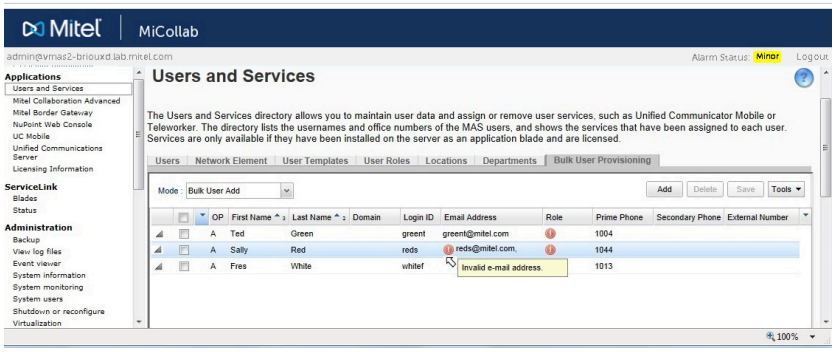
If errors occur during a bulk data import, they are listed in the Bulk Provisioning Tool screen and indicated by icons:

 indicates a field entry error. To display the error, hover your cursor over the icon. The error message provides the corrective action.

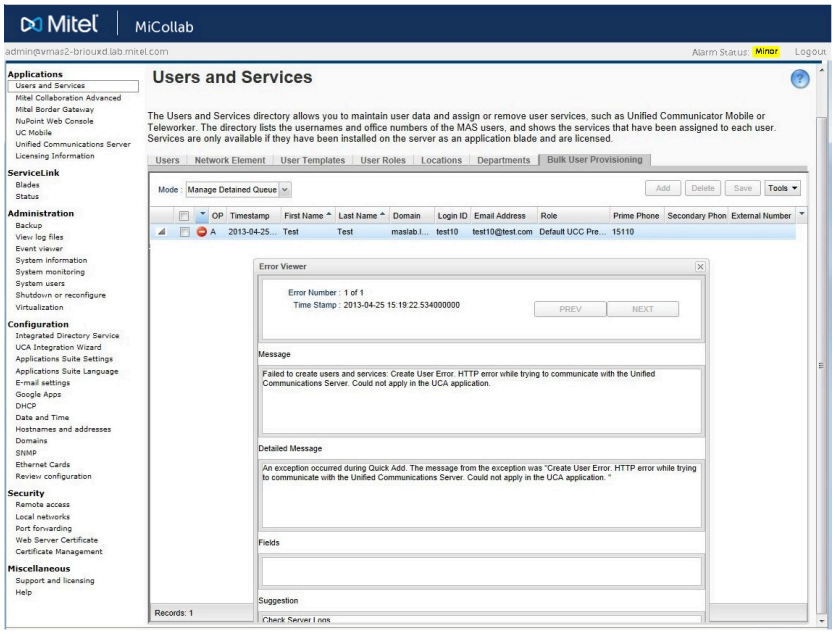
 indicates a data import failure. To display the error, click the icon for details. The error report provides the corrective action. If multiple errors exist against the update, click **Next**.

You can also click the  icon next to an entry to review a detailed summary of any errors. You must resolve the errors before you can save an entry to the directory.

Example of a Field Entry Error



Example of a Data Import Error



View User Directory 12

This chapter contains the following sections:

- Enter User Information
- Quick Add
- Delete Users
- Send Service E-mail

Overview

The Users and Services directory allows you to manage user data and assign or remove application services, such as MiCollab Audio, Web, and Video Conferencing or NuPoint UM. The directory lists user names and office numbers for MiCollab users and shows the services that are assigned to each user. Above the directory list, the "Unassigned services" and "Total number of users" are displayed.

View Directory Entries

1. Under **Applications**, click **Users and Services**.
2. Click the **User** tab.
3. Click **Show all**. Users are listed alphabetically by their last names. Services appears as column headings along the top of the directory.

Field/Column	Description
Last Name First Name	Displays the name of the user. The name fields can be blank, but you must assign a Login ID. Duplicate names are allowed. Although the Last Name and First Name can be the same, the combination of "Last Name, First Name" and "Office Phone #1" must be unique. Click a user's last name to display the information for that user.
Phone(s)	The user's extension number(s) on the communications platform. This field can be blank.
	Indicates that a service (for example, Teleworker) that is hosted on the local node is assigned to the user. A blank cell indicates that the service is not assigned. The MiCollab Client service is available to all users. However, the service is not active unless it's assigned to one or more of the user's phones.
	Identifies data elements that are being shared via Flow Though Provisioning.

Note:
To display e-mail addresses, perform a search on an e-mail address.

Note:
If AWV and NP-UM ports are listed in the MiCollab USP directory, do not delete them from USP. They should not be assigned any services.

Locate an Existing User in the Directory

1. In the Search field, enter one of the following for the user:
   - First Name
   - Last Name, or
   - Phone extension number

   Note:
   Entering a partial name or number broadens your search and typically returns more results.

2. In the View field, set the number of results that you want to display per page.
3. Click on **Search**.

Directory Tasks

From the Users directory, you can perform the following tasks:

- Quick Add
- Edit a user's information
- Reset a user's login password and TUI passcode
- Add a new service to a user
- Delete a service from a user
- Delete users
- Send a user a welcome email
- Send CloudLink Welcome Email

- Deploy Mobile Client for Softphone
- Deploy MiCollab Clients for EHDU
- Generate Reports
- Connect to MiVB System Tool

About Unassigned Services

Unassigned services or mailboxes are services that have been registered with an application but have not yet been assigned to a user. Click the **View** link to display a list of available services (for example, unassigned mailboxes). See Managing Unassigned Services for more information.

Note:
When you add or delete services through any of the applications, it can take up to 5 minutes before the numbers are updated. For example, if you add a mailbox through the NuPoint UM Web Console, it can take up to 5 minutes before the number of "Unassigned mailboxes" is increased.

12.1 Enter User Information

The user information that you program in this tab is available to all installed MiCollab applications. User information that you provision using the USP application is also provisioned in the associated MiVoice Business database if Flow Through Provisioning is enabled. Flow Through Provisioning is not supported for the MiVoice Office 250, MiVoice Office 400, MiVoice 5000, or MiVoice MX-ONE.

The following conditions apply:

- Do not add and delete MiCollab users from the MiVoice Business system administration tool even if Flow-Through Provisioning is enabled. Perform these tasks from MiCollab.
- Users must have at least one phone service assigned.
- You cannot add a phone to a user who does not already have one. Use Quick Add or import user entries with a phone using Bulk User Provisioning.
- You can enter accented characters in the MiCollab supported languages into the following User and Services application fields: First Name, Last Name, Login ID, Password, Template Name, and Role Name.
- If MiCollab is integrated with MiVoice 5000 or MiVoice MX-ONE, the fields in this tab are read-only with the exception of the **Password** and **TUI Password** fields. The **Add**, **Quick Add**, and **Delete** buttons will not be available. Add users from the communication platform management interfaces.

Field Descriptions

Personal Info

Field	Description	Values
First Name	Enter user's first name. The Search function in the MiCollab End User Portal can locate users based on the first or last name.	Enter a name up to 256 characters in length. This field can be left blank. This field supports UTF-8 characters. It's recommended that you make the name in this field match the " First name" of the " Last name, First name" entry in the Name field of the MiVoice Business Telephone Directory Assignment form.
Last Name	Enter the user's last name. You can leave this field blank. The Search function in the MiCollab End User Portal can locate users based on the first or last name.	Enter a name up to 256 characters in length. This field is mandatory. This field supports UTF-8 characters. It's recommended that you make the name in this field match the " Last name" of the " Last name, First name" entry in the Name field of the MiVoice Business Telephone Directory Assignment form.
Display Name	Displays the " Last name, First name" of the user.	If a First Name is not entered, only the Last Name is displayed. If the Last Name is not entered only the first name is displayed. If both the first name and last name are not entered, this field is blank.
Role	Select the desired role for this user. When you save this entry, the role label is just applied to the entry. The associated template information is not applied. Template information is only applied during a Quick Add operation.	Default is None.

Field	Description	Values
UCC Bundle (for UCC licensing bundles) OR User License Bundle (for MiVoice Licensing bundles)	For the UCC licensing bundles, select the UCC Licence Bundle to apply to this user. The license bundle determines the services and application licenses that are assigned to this user. A site can use a mix of UCC licenses and "a la carte" licensing. For MiVoice Business Subscription licensing, select the User License Bundle to apply to the user.	Select one of the following: • None (Default) • Default UCC Basic User for Enterprise • Default UCC Entry User for Enterprise • Default UCC Standard User for Enterprise • Default UCC Premium User for Enterprise ********** • MiVb Telephony (Ed.2) • MiVB Entry (Ed.2) • MiVB Premiere (Ed.2) • MiVB Elite CX (Ed.2)
Department	Select the department that the user belongs to from the drop-down menu. (Optional)	To populate this list see Add or Edit Department Information
Location	Select the location of the user from the drop-down menu. (Optional)	To populate this list see Add or Edit Location Information

Field	Description	Values
Prompt Language	Select the language for the user's voice services (Telephone User Interfaces). The changes take affect immediately after you click **Save**. Active TUI sessions remain in the previous language until the next login session. **Note**: This setting changes all the user's TUIs to the new language with the exception of the MiCollab Audio, Web and Video Conferencing application. This setting is not applied to the AWV TUI. The AWV TUI uses the System Default Language.	By default, the prompt language uses the System Default Language that is set from the server manager. To set the System Default Language, under **Configuration**, click **MiCollab Language**. Then, select the desired language from the **Language** drop-down box. **Note**: If MiCollab is sharing user data with MiVoice Business elements, user updates that you make on a MiVoice Business platform are also updated on the MiCollab system. If you assign a user on an MiVoice Business element with a language that is not supported on MiCollab , US English (system default) is applied to the MiCollab user entry.

Field	Description	Values
Primary E-mail Address	Enter a unique primary email address for the user. Users can also configure their primary email address from their MiCollab End User Portal. Entering a primary email address in this field automatically populates the Unified Messaging SMTP email address in the NuPoint UM Web Console application. With Release 9.3 onwards, the email id field is mandatory for creating a user. For existing users with no email id specified, the administrator will not be able to edit the user and would need to provide an email id to continue. **Note**: It is not possible to update the primary email from the MiCollab Client Service. In case a user has a different primary email in MiCollab Client Service than the USP, they can run the following steps to synchronize the email at both places to avoid any issues:	Use the format " name@place.suffix", where • name is 2 to 40 characters in length • the place is 2 to 40 characters in length • the suffix is from 2 to 6 characters in length This field is limited to ASCII characters.

Field	Description	Values
	• Change the email in the USP to the one set in MiCollab Client Service. It will change the email in USP.	

Field	Description	Values
	• Again change the email in USP to the original email. It will change the email in both USP and MiCollab Client Service.	
	Note: Changing a MiCollab Audio, Web and Video Conferencing user's email address deletes the original MiCollab Audio, Web and Video Conferencing account (including collaboration history) and starts a new account.	
	Note: If you do not enter an address here, then the automatic population of NuPoint UM SMTP email address in the NP Web Console application is not performed and, if an SMTP email address is required, you will have to enter it manually in both MiCollab and NuPoint UM .	
	Note: A primary email address is mandatory to Quick Add users or Add users from the IDS Detained queue.	

Field	Description	Values
Distinguished Name	If this user entry is managed from an Integrated Directory Service (IDS) server, this field displays the Distinguished Name that will be used by MiCollab for a logon attempt using LDAP to the directory server. If the user cannot log onto MiCollab, this value should be checked against the location of the user within the directory server, and make sure that the locations are same. If a user is moved within the directory server and an IDS sync is performed, and the user data is updated, this value will be updated. If this user entry is not managed from an Integrated Directory Service (IDS) server, this field displays the MiCollab server (MSL) domain name.	Read-only field

Field	Description	Values
IDS-Manageable	Specifies that the data for this user can be managed from an Integrated Directory Service (IDS) server. If an IDS server is integrated with MiCollab , updates to specific user fields in the directory service record are applied to the corresponding MiCollab record fields. Updates are applied during the next synchronization event. When this box is checked, all the IDS managed fields (for example, First Name, Last Name, Department, Location, Email, and Login) are disabled because the data is obtained from the directory services. Clear this check box if do not want the user's directory server data to be synchronized with the MiCollab user's data. You can then modify these fields from the USP application. Note that data is only synchronized from the directory service to MiCollab . Therefore, if you remove the IDS Manageable box, changes that you make to the entry in USP will not appear in the directory service database. The entry will be out of sync. If you subsequently check the IDS Manageable box, any changes that you made to the IDS managed fields will be overwritten by the directory service on the next synchronization. If you check this box on a record that was previously not managed by the directory service, the MiCollab system attempts to synchronize the user with the matching entry on the directory server. If the system cannot find a matching entry, a list of possible entries is displayed for you to select from. If none of the entries are a suitable match, resolve the mismatch by either deleting the entry from MiCollab or creating a corresponding entry on the directory service.	If a directory server is not connected with the MiCollab system, this option does not appear. If you check this option when LDAP Authentication is enabled, the user's login credentials are changed to the user's directory server domain name and password. The change does not occur until after the next full synchronization. The system automatically sends a Welcome E-mail to inform the user of the password change. If you disable this option when LDAP Authentication is enabled, the system prompts you to enter a new MiCollab password for the user in this form. After you set a new password, the system automatically sends a Welcome E-mail to inform the user of the new password. Default is Enabled

Authentication

Field	Description	Values
Login	Enter a Login ID for the user's MiCollab End User Portal. The Login ID must be unique. If you have entered the First Name and Last Name for the user, the Login ID is automatically set to the last name followed by the first initial of the first name. For example, the Login ID for John Smith would be "smithj". UPN is also supported in login ID. **Note**: The UPN login is supported only in the integrated mode. **Note**: Users that are in the detained queue will not be updated with UPN on the upgrade of server(s) to R9.4. If the user is configured with a SIP Phone and you change the user's Login ID: • The user's **Set-side username** on the MiVoice Border Gateway is updated with the new Login ID. However, if you change a user's **Set-side username** on the MiVoice Border Gateway, the change is not applied to the user's account on MiCollab. • The user is automatically sent a Service e-mail with their Login ID and password.	The Login ID can be between 2 and 113 alphanumeric characters in length. You cannot leave this field blank. The Login ID can be numeric but it should not conflict with any other user's DN. The user can use his own DN as a login ID. Login ID Validations: • invalid characters are Can you please provide me with access to this document? & * + / = ? { } | < > ( ) ; : , [ ] " ‘ • characters allowed are A – Z, a - z, 0 – 9, % . - _ ! # ^ ~ Letters with diacritical marks, such as umlauts, accents, and tildes, are invalid characters **Note**: This field supports ISO8859-1 characters with some exceptions. **Note**: TheUPN as a Login ID is supported in MiCollab Azure integration.

Field	Description	Values

Login
 	
continued
	• You or the user must re-register the SIP User ID with the MiVoice Business Gateway. The user's SIP Phone displays "No Reg" until it is registered.	The UPN specifications are as follows:
		• The userPrincipalName (UPN) attribute must be in the internet-style sign-in format where the user name is followed by the @ symbol and a domain name. For example, username@abc.com.
		• The maximum number of characters for the UPN attribute is **113**. A specific number of characters are permitted before and after the @ symbol; the specifications are as follows:
		  • maximum number of characters for the username, that is the characters before the @ symbol should not be more than 64
		  • maximum number of characters for the domain name following the @ symbol should not be more than 48
		  • the @ symbol is required in each userPrincipalName value
		  • the @ symbol cannot be the first character in each userPrincipalName value
		  • the username cannot end with a period (.), an ampersand (&), a space, or with the @ symbol
		  • the username should not have spaces
		  • routable domains must be used; for example, local or internal domains cannot be used
		• unicode is converted to underscore characters
		• userPrincipalName cannot contain any duplicate values in the directory

Field	Description	Values
Password	Enter a password for MiCollab End User Portal access. Required password content is determined by the configuration applied to MiCollab Settings. Click **Generate Password** to have the system create a random password for the user. Note that the random password is masked for security. If the Service Information E-mail feature is configured for the system, whenever you create or change a user's password, an E-mail is sent to the user with the password. If the user is configured with a SIP Phone and you change the user's Password: • The user's **Set-side username** password on the MiVoice Border Gateway is updated with the new password. This also applies if the user changes their password. However, if you change a user's **Set-side username** password on the MiVoice Border Gateway, the change is not applied to the user's account on MiCollab. • You or the user must re-register the SIP Password with the MiVoice Business Gateway. The user's SIP Phone will display "No Reg" until it is registered.	4 to 20 characters. This field is limited to ISO-8859-1 characters. **Note**: If the user has a SIP phone, you must enter a secure password that is not trivial. Ensure that it contains letters, numbers, and punctuation. (For example, Mitel*Server1!).
Confirm Password	Re-enter the password to confirm (not necessary if generated randomly).	

Field	Description	Values
TUI Passcode	Set a passcode for the user's Telephone User Interfaces. This passcode allows the user to access voice applications, such as a (NP-UM) voice mailbox and is also used as the Hot Desk User Login PIN. There are no passcode strength restrictions enforced when you, the administrator, set a passcode for a user. When a user creates a passcode, the passcode must • consist of digits only (0 to 9) • be from four to ten digits in length • cannot match the user's mailbox number or any other company extension number. • not be easy to guess (for example, 1234). • not contain the same digit repeated more than three consecutive times (for example: 1111 or 2222). Click **Generate Random Passcode** to have the system create a random passcode for the user. Note that the random passcode is masked for security.	4 to 8 telephony digits (*, #, 0-9) **Note**: Default set by Mitel Integrated Configuration Wizard is the user's DN. **Note**: DNs that contain * or # are not supported for Hot Desk User Login PIN. **Note**: The passcode that you enter in this field is distributed to the User PIN field in the User Configuration form on the MiVoice Business . Do not change the User PIN field on the MiVoice Business ; otherwise, the User PIN and passcode will be out of sync. Also, users should not change their User PIN from their sets using Feature Access codes for the same reason.

Field	Description	Values
TUI Passcode *continued*		**Note**: For 5505 SIP phone, the wireless PIN is the first four digits of the directory number. After the phone is provisioned, the wireless PIN can only be modified from MiVoice Business. If the directory number is less than four digits, zero is added at the end of the digit to make it a four-digit number.
Confirm Passcode	Re-enter the passcode to confirm (not necessary if generated randomly).	

12.2 Quick Add

Use Quick Add when you want to add a new user and override some of the template settings:

1. On the **Users** tab, click **Quick Add**. The **Quick Create User** page opens.

Note:
Quick Add is not supported if MiCollab is integrated with MiVoice 5000 or MiVoice MX-ONE.

2. Select the desired user role. The associated template information for this role is applied.

Note:
Shared roles that are not applicable to Quick Add (for example, a role with more than three phones, will not be available for selection from the drop-down list.

3. Edit the fields as required. The Quick Add form displays a subset of the fields that are available in the Template form.

   For UCC licensing bundle, refer to Enter Template Information for UCC Licensing on page 80.

   For MiVoice Business licensing bundle, refer to Enter Template Information for MiVoice Business Subscription Ed.2.

> **Note**:
> With MiVoice Business call manager, when you create a new user via the **Quick Add** feature, ensure that the phone number field must contain 1 to 7 digits and the length of the phone number should be less than 7, including the * symbol.

> **Note**:
>
> If a user has voicemail service and the voicemail number starts with 0 is entered and saved, the system will display the following error message:
>
> **Create User Error. Mailbox number cannot start with 0**
>
> To avoid the above error during user creation, ensure that the voicemail number field does not start with 0.

4. If you add Teleworker service to a user's SIP phone, the system automatically configures a corresponding SIP service on the MiVoice Border Gateway. You must set the User Password field in the template to "Randomly Generate" or "Use this Value. If you select "Use this Value", the password value must be set to a strong password. The following conditions apply:

   - The system sets the **Set-side username** on the MiVoice Border Gateway to <username-DN> (for example, smithj-7328). This username format applies to MiVoice Business communication platforms only.
   - The SIP Password is a mandatory field when you are creating a SIP Teleworker service. You cannot use the extension number as the password. You must configure a strong password; otherwise, the **Quick Add** operation will fail.
   - If you change a user's **Set-side username** or password on the MiVoice Border Gateway, the changes are not applied to the user's account on MiCollab.

Note:
The Flow Through Provisioning feature shares MiVoice Business templates with the MiCollab system. The MiVoice Business templates support key template programming for users created from MiCollab USP. However, when a key template is created on the MiVoice Business system, the template is not validated for incomplete key programming (such as a missing ring type in a DSS/BLF key). The system only generates errors when you attempt to apply the invalid key template to a user via a role. Therefore, whenever you create a new key template on the MiVoice Business, ensure that you test it by applying it to a MiVoice Business user. If you receive errors related to key programming when you attempt to apply a shared template, you must correct the key template on the MiVoice Business.

5. Click **Save**.

12.3 Delete Users

Note:
If Flow Through Provisioning is enabled, when you delete a user the user data is also deleted from the associated MiVoice Business system.

To delete a user:

1. Under **Applications** , click **Users and Services** .
2. Locate the user in the directory.
3. Click the check box next to the user's Last Name.

Note:
The administrator can select multiple users on a page for deletion. To perform multiple deletion, the administrator must be logged in to the Users and Services Provisioning application using one session only.

4. Click **Delete** .
5. Click **Yes** .

Note:
Delete is not supported if MiCollab is integrated with MiVoice 5000 or MiVoice MX-ONE .

12.4 Send Service E-mail

To send a Service Information E-mail to a user:

1. Configure a Service Info E-mail.
2. On the **User** tab, select the desired users from the directory list.
3. Click **Send Service Info E-mail**.
4. Click **Okay**.

Enter Phone Information 13

This chapter contains the following sections:

- Enter Speech Auto Attendant Information
- Configure Groups
- Enter NuPoint UM Information
- Enter MiCollab Client Information
- Enter MiCollab Audio, Web and Video Conferencing Information
- Enter MBG Information
- Enter Vidyo Information
- Enable Google Integration Features
- Add External Numbers

The data that you enter in this form is shared across the applications that are installed on the MiCollab server. If Flow Through Provisioning is enabled, configuring a phone (adding, editing, and deleting phones) in this form also configures the phone on the associated MiVoice Business.

Note:
Although you can add and delete phones from the MiVoice Business system administration tool, the recommended best practice is to perform these tasks from MiCollab.

Note:
For integrations with MiVoice Business, you cannot associate more than one user to the same phone service.

Note:
For integrations with MiVoice 5000 or MiVoice MX-ONE, you must provision phone services from the MiVoice 5000 or MiVoice MX-ONE management interfaces by applying a role to the user entry. Therefore, the **Add New Phone** and **Delete Phone** buttons are disabled in this tab. Although MiVoice 5000 and MiVoice MX-ONE supports users with multiple devices, only the users' primary directory numbers appear in MiCollab (that is, MiVoice 5000 or MiVoice MX-ONE users on MiCollab only have one phone). The MiCollab services are applied to the prime directory number of the user.

Adding a Phone

To add a user phone:

1. Edit the user record.
2. Click the **Phones** tab.
3. Click **Add New Phone**. If Flow Through Provisioning is enabled, the fields are populated from the MiVoice Business default template. If Flow Through Provisioning is not enabled, the fields are populated from the MiCollab Basic template.
4. Select the Phone Type.
5. Complete the required fields for the Phone Type that you selected (see tables below). The fields depend upon the selected Phone Type.

Note:
If you check the box next to a feature option, the fields associated with that option are displayed. For example, if you click Hot Desking User, the Call Coverage Service Number field, ACD Agent check box, and External Hot Desk License check box are presented.

6. Click **Save**. If Flow Through Provisioning is enabled, the changes are automatically migrated to the MiVoice Business. If it is not enabled, you must activate the new device using the registration procedure listed in the *Register Mitel IP Telephones* topic of the *MiVoice Business System Administration Tool Online Help*.

Note:
"Phone Type" and "Number" cannot be edited. To change this information, delete the phone and add a new one.

To determine the next available directory number on a MiVoice Business platform:

1. Reach through to the MiVoice Business **Users and Services Configuration** form.
2. Click **Add > Default User and Devices**.
3. Click the **Service Profile** tab. The system automatically populates the field with the next available number.
4. Copy the number and cancel the changes.
5. Return to MiCollab Users and Services application and enter the directory number for the user in the Number field.

Changing a User's Directory Number

You can change a user's directory number in Users and Services and the change is applied to the other phone fields in the user's applications.

The following conditions apply:

- If Flow Through Provisioning to the MiVoice Business is enabled, you cannot change the directory number of a user who is assigned with MiCollab services. The system will display an error message.
- If Flow Through Provisioning is not enabled, you can change the directory number of a user regardless of whether or the user has MiCollab services assigned. However, after you change a user's directory number, you must manually change the user's directory number on the MiVoice Business.
- If user provisioning is supported via Integrated Directory Services (IDS), directory number change is not supported.
- If you attempt to change a user's directory number to a number that is already in use, the system displays an error message.
- If the directory number operation fails, the current number is maintained.
- When you change a user's directory number, the change is not applied to

  - the voicemail actions in NuPoint Unified Messaging Call Director call flows, or
  - the Speech Auto Attendant directory.

You must manually update the Call Director call flow and/or Speech Auto Attendant directory with the new directory number.

To change a user's directory number:

1. In the Users and Services directory, select the user and click **Edit**.
2. Click **Phone** tab.
3. Change the user's directory number to an available directory number.
4. Click **Save**.

When you change a user's directory number:

- All the application fields that contain the current directory number are updated with the new number. (For example, if the Number field in the user's Phone tab is set to 2222 and you change it to 3333, all the user's application fields that are set to directory number 2222 are changed to 3333.)
- If the number field in an application is blank or has been configured with a number that is different from the one that you are changing, then the field is not updated.
- The user's NuPoint Messenger greetings and recordings, AWV conferences, MiCollab Client dynamic status, and so forth are maintained.
- If a user's mobile phone is deployed via the MiCollab Client Deployment service, the phone number is updated immediately.

Deleting a Phone

To delete an IP phone service from a user:

1. Edit the user record.
2. Click the **Phones** tab.
3. Click **Delete Phone.**
4. Select the phone to delete from the list. A confirmation message is displayed
5. Click **Yes** to delete the phone and its associated services. If you delete a phone that is set as the Registered Phone for MiCollab Audio, Web and Video Conferencing service, the Registered Phone is removed from the MiCollab Audio, Web and Video Conferencing service. However, the MiCollab Audio, Web and Video Conferencing service is NOT deleted.

DNIC and Analog Phone Support

MiCollab only supports Flow Through Provisioning for IP phones. Analog/Analog-FXS devices and users must be added in the MiVoice Business database. After Flow Through Provisioning is initiated, these will be available in MiCollab. However, you can add DNIC users into MiCollab and then program the user and phone separately into the MiVoice Business database using the Reach Through feature.

Note:
MiCollab does not allow to edit DN or device type for Analog-FXS devices. Also, HotDesking and Teleworker are not supported for Analog-FXS devices.

You can program entries into MiCollab for DNIC and analog phones and then use the phone number as

- a reference to the associated mailbox
- a reference to the associated SAA contact point.
- as a default reference to a registered phone (call me) for MiCollab Audio, Web and Video Conferencing collaboration user settings.

Field Descriptions

General

Field	Description	Values
Service Label.	Enter a name of up to 64 characters that identifies the service (for example, Desk Phone). The same label can be used for more than one service associated with the same user.	Up to 64 characters.
Phone Type	Select the type of system that supports the phone.	**Mitel PBX Phone** if the phone is on a MiVoice Business system, MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400 system. **Other PBX Phone** if the phone is supported by a MiVoice Office 250. Note that Single Point Provisioning is not supported on the MiVoice Office 250.

For Mitel Phone

Field	Description	Values
Network Element	System-generated field. You can only set the network element if this is the first phone that you are assigning to the user. All the user's phones must be hosted on the same network element.	Elements are configured in the Network Element tab. Although you can select any network element as the home element, Flow Provisioning Through is only supported to MiVoice Business elements that are sharing with this MiCollab system.
Secondary Element	For resiliency, select the phone's secondary element from the list. If the phone's primary network element goes out of service, the phone is supported by the specified secondary element.	The selected element must be different than the network element above.
Number	Enter the primary extension number of the phone. **Tip**: To determine the next available directory number on a MiVoice Business platform	Required. **Note**: MiCollab does not support extension numbers beginning with a zero. **Note**: If this user is a Hot Desk user or requires a SIP Authentication password, the DN must not contain * or #.

Field	Description	Values
Secondary Line Number	Enter the secondary line number of the phone.	The Secondary Line Number allows MiCollab Client user to have a second monitored deskphone. Teleworker Service is not assigned to this number. The secondary Line Number is supported in MX-ONE integration only. **Note**: MiCollab does not support extension numbers beginning with a zero.
DID Service Number	Direct Inward Dialing (DID) routes incoming calls on a designated trunk to the user's phone. Enter the external number of the designated trunk. Assign the DID number to the user's prime phone. Program the user's other phones in a Personal Ring Group or Multi-Device User Group with the prime phone as the pilot number for the group.	1 to 26 telephony digits, 0 to 9, * or #. **Note**: The length of the external number cannot exceed 26 digits. **Note**: This feature is only supported with MiVoice Business Release 7.0 and later.

Field	Description	Values
Use as Outgoing DID	Check this box to display the DID number for outgoing calls made from the user's phone. The MiVoice Business CPN Substitution feature allows you to program a substitute number for outgoing calls made on a DID trunk. The substitute number is presented to the network for outgoing calls on the DID trunk.	Disabled
CESID	Enter the Caller Emergency Service Identification (CESID) to be sent to the Public Safety Answering Point (PSAP) in the event of an emergency call. Up to 12 digits can be programmed. **Note**: Although a CESID can be programmed for any mobile DN, the system will only use it for External Hot Desk Users (EHDUs) that are logged on to private trunks. For regular hot desk users and EHDUs logged on to MiNET devices, the system will use the CESID associated with the set's registration DN.	Between 1 and 12 digits in length. Can contain digits 0 to 9. Default is blank.

Field	Description	Values
Hot Desking User	Check to create a Hot Desking user; clear to create a standard user and device. **Note**: • Hot Desking User type requires COS entries.	Not checked.

Field	Description	Values
	• When you assign a newly created user as a Hot Desking User, the ACD Agent field is disabled. If required, select the ACD Agent field to create an ACD Agent with hot desking capability.	

Field	Description	Values
	• After a user has been assigned with the ACD Agent option, you cannot change this option using **Edit**. You must delete the phone and then add it again to change the ACD Agent option.	
ACD Agent	Check to designate a user as a ACD Agent with hot desking capability. **Note**: • To enable this option, you must first select the Hot Desking User box on a newly created user.	Not checked.

Field	Description	Values
	• After a user has been assigned with the ACD Agent option, you cannot change this option using **Edit**. You must delete the phone and then add it again to change the ACD Agent option.	
Enable SIP Softphone for MiCollab Client	Check box to enable SIP Softphone functionality for a hot desking user. When you enable this functionality, MiCollab Client Service assigns the phone type as SOFTPHONE and Device Type as 76. **Note**: You can apply Teleworker service to a Hot Desking user with SIP Softphone enabled.	Not selected.
External Hot Desk License	Check box to enable External Hot Desk User (EHDU) functionality. The Device Type field must be set to Hot Desk User. External Hot Desk Users must be licensed. Licenses are programmed in the License and Option Selection form of the MiVoice Business. **Note**: You cannot apply the Teleworker service to an EDHU.	

Field	Description	Values
Hot Desk User External Dialing Prefix	Enter "9" or other prefix digit(s) required to dial out to the external hot desk device.	1 to 26 telephony digits, 0 to 9, * or #.
Hot Desk User External Number	Enter the telephone number of the external hot desk device.	1 to 26 telephony digits, 0 to 9, * or #. **Note**: The combined length of the external dialing prefix and external number cannot exceed 26 digits.
DTS	Enter the telephone number of the DTS phone.	1 to 26 telephony digits, 0 to 9, * or #. **Note**: For MiVoice MX-One, DTS phone fields are treated as Secondary Extension.

Field	Description	Values
Preferred Set	For a hot desking user, select the user's preferred hot desking device type from the drop down list. The default value is No Device. • To display this field, you must select the Hot Desking User box. • Users can select their preferred hot desking device type from the Desktop Tool. • If No Device is selected as the Preferred Device, the device is assigned 96 keys by default.	No Device

Field	Description	Values
Deployment Profile	Select a profile for MiCollab for Mobile Client softphone or EHDU deployment.	This field is only displayed if the device type is set to "UC Endpoint" or if External Hot Desk User is selected. For "UC Endpoint" devices, the default is the "default" profile. For External Hot Desk Users, the default profile is set in the MiCollab Settings page. **Status**:"Un-deployed" indicates that the client is not deployed. "Deployed" indicates that the configuration has been sent to the client but has not yet been downloaded. "Downloaded" indicates that the configuration has been downloaded and installed for the client. **Note**: You must configure MiCollab Client Deployment. See the online help associated with the **Applications > MiCollab Client Deployment** application for configuration instructions. **Note**: If there is no phone for which a deployment profile is selected, users need to provide their password every time they log in to PC and Mobile Clients.

Field	Description	Values
Deployment profile *continued*		**Note**: If a phone with a deployment profile is added later, the user must provide their password for every login to PC and Mobile Clients. However, if the administrator or the user changes the password after the user logs in, the updated password is automatically used for the next login to PC and Mobile Clients. **Note**: If a user is deployed from the MiCollab Client Service page, the Client will prompt for the password. This scenario occurs because the password is not set from MiCollab Server in the deployment configuration for the user. MiCollab Server will not have the password in cleartext during the deployment.

Field	Description	Values
Send Deployment Email	If this option is checked, a deployment email is sent to the user when you deploy a MiCollab for Mobile Client softphone from the Users and Services directory page; if unchecked, it is not sent. The deployment email provides users with a QR code. After scanning the QR code with their mobile phone, the user is authenticated, and the MiCollab for Mobile Client application is downloaded from the App Store to the user's phone. If you are only deploying a softphone to a user's web client (WebRTC client), then it is not necessary to send a deployment email.	This option is only available if the device type is set to "UC Endpoint". Default is checked (send deployment email).

Field	Description	Values

Device Type	Select a device from the Device Type list.	The following rules apply:
		• You cannot edit the device type for Generic SIP Devices that have Teleworker services assigned.
		• This field is not available if "Hot Desking User" is checked.
		• Enter a device type of "UC Endpoint" for MiCollab Client clients.
		• The following MiVoice Business Device Types are not supported: Analog, Analog-FXS, 5001 IP, 5201 IP, 5401 IP, NetVision IP, Spectralink NetLink, and Superset Devices.
		• Assign the "Phantom" Device Type to any entries that you do not want shared or synchronized with the MiVoice Business via Flow Through Provisioning. For example, you could assign a "Phantom" device to
		  • a mailbox-only entry to allow the mailbox number to be located in the USP directory using the Search feature.
		  • an entry that is programmed in the MiVoice Business database as a system speed call, non-prime broadcast group, or console.
		After you assign a Phantom device type to an entry, the entry is not shared even if you later change the device type to a non-Phantom device.

Field	Description	Values
Device Type *continued*		**Note**: The Device Type field does not apply to the MiVoice Office 250 .
MAC Address	Enter the MAC Address of the Teleworker set in the following format: XX:XX:XX:XX:XX:XX. The MAC Address is printed on a label that is affixed to the base of Mitel IP phones. (This entry is mandatory for Teleworker.) **Note**: This field does not apply when device type "Hot Desk User" or "SIP Generic Device" type is selected.	12 hexadecimal characters separated into 6 pairs by 5 colons.

Field	Description	Values
SIP Device Capabilities	When Generic SIP Device type is selected, this field is enabled with the default SIP Device Capabilities Number of 1. Assign "UC Endpoint" device type for a MiCollab Client Deskphone, MiCollab Client Softphone, or UC360. **Note**: When you select a device type of "UC Endpoint" this field defaults to 71. However, if you are configuring a UC360 you must change the default SIP Devices Capabilities number from 71 to a value between 1 to 60. Then, program the assigned SIP Device Capabilities number on the communications platform with the settings required to support the UC360. See the MiVoice Conference Unit Administrator's Guide on the Mitel Customer Documentation site for the required settings.	Change the Default SIP Device Capabilities number as required.

Field	Description	Values
SIP Password	Enter a SIP device password for the user. When you create or change a user's SIP password, the system automatically sends a Service Info Email with the password to the user. Note: The display on 5505 SIP and 5302 IP sets is limited to eight digits. For these sets, assign a numeric password of eight digits or less.	Up to 26 ASCII characters including numeric, alphanumeric, and special characters. Default is blank. This field is only enabled for SIP devices. SIP device passwords are optional. If this field is left blank, a password is not required to register a SIP device with the MiVoice Business .
Confirm SIP Password	Re-enter the passcode to confirm.	

Advanced Phone Settings		

Service Level	Displays the level of service for this directory number (DN): **Full** - A DN with this service level is assigned to a standard user and device with full telephony service. **IP Device Only** - A DN with this service level is assigned to an unlicensed device that has only basic telephony functionality (emergency or attendant calls). The device becomes functional when a hot desk user or hot desk ACD agent logs into it. **Trusted** - A DN with this service level is assigned to a trusted Mitel application that has full telephony service once it registers with the system. Although the DN can be programmed on the same forms as a Full Service DN, it does not use an IP User License. **Multi-Device** - A DN with this service level is assigned to a user that has only basic telephony functionality (emergency or attendant calls) until programmed as a member of a Multi-device User Group. Multi-Device User Groups (MDUGs) allow a single user to have multiple phones grouped under a common directory number without each phone requiring a full MiVoice Business IP License. There are two types of Multi-Device User Groups:	Full Service

	• *Standard:* allows up to eight phones to be grouped under a common directory number. Only the prime number requires an IP User License. The group itself, requires a MDUG license. In a MDUG, phone functionality is essentially limited to one device in the group at any given time. When one of the user's phones is engaged in call, the other phones are consider busy (in other words, "One Busy All Busy" is always enabled) and have restricted functionality. • *External Twin:* allows only two phones, typically a desk phone and a cell phone, to be twinned. This type of group does not require a MDUG license. It only requires an IP User License and an External Hot Desk User license. The prime number uses the IP User license. The second member must be an External Hot Desk number and consumes the EHDU license.	
Zone ID	Enter a number to identify the Network Zone. The MiVoice Business platform uses Network Zones • for compression and bandwidth management • to associate the zones to time zones for the display of local time on IP sets • to configure the zone's Location Based Number (LBN) prefix for Location Base Call Routing (optional), and • to define the zone's CESID (optional).	Number from 1 to 999. Default is blank. If this field is left blank, the MiVoice Business defaults this setting to Zone 1.

Call Coverage Service Number	Assign the Call Coverage Service Number Call for the MiVoice Business Hot Desk PIN Security feature. The MiVoice Business Hot Desk PIN Security feature ensures that all hot desk users create strong (resistant to guessing) PINs by forcing them to create PINs that adhere to a set of strengthening rules. Hot Desk PIN Security is programmed in the Call Coverage Services form of the MiVoice Business System Administration Tool. This form allows you to assign a Call Coverage Service number that uniquely identifies the type of Call Coverage Service. The number that you enter in this field must exist in the Call Coverage Service form on the MiVoice Business system. If single point provisioning is enabled, the phone's Call Coverage number is automatically updated on the MiVoice Business system. **Note**: This field only applies to MiVoice Business Release 6.0 or later systems.	This field only appears for phones with a "Mitel 3300 ICP Phone" type. If you create a new phone, this field defaults to 1. If you upgrade an existing MiCollab system to MiCollab Release 4.0 SP2 or later, this field also defaults to 1.
Class of Service - Day	Enter a COS number for Day mode.	Number from 1 to 110. Defaults are blank. If you are integrating MiCollab with a MiVoice Business system, enter COS 13 for users without the Record-a-Call feature; enter COS 14 for users with the Record-a-Call feature.

Class of Service - Night 1	Enter a COS number for Night 1 mode.	
Class of Service - Night 2	Enter a COS number for Night 2 mode.	
Class of Restriction - Day	Enter a COR number for Day mode.	
Class of Restriction - Night 1	Enter a COR number for Night 1 mode of service.	
Class of Restriction - Night 2	Enter a COR number for Night 2 mode of service.	

For Other PBX Phone:

Field	Description	Values
Number	Enter the extension number of the phone.	Between 1 and 6 digits in length. Can contain * and #. **Note**: If this user is a Hot Desk user or requires a SIP Authentication password, the DN must not contain * or #.

13.1 Enter Speech Auto Attendant Information

To add or edit Speech Auto Attendant service for a user:

1. Click the **Phones** tab.
2. Complete the required fields as shown below.
3. Click **Save**.

Field	Description	Values
Contact Phone	Select the number that you want to use as your Speech Auto Attendant contact number. Select "None" to unassign your current SAA number.	List of phones currently owned by the user. **Note**: User must have at least one phone service before entries in these SAA fields are enabled.
Private User	Select this option to exclude your phone from SAA recognition. (This means you cannot be reached by having a caller speak your name to the auto attendant.)	You can only select this option after a phone has been selected from the Contact Phone list.

Note:

- These fields are disabled if the Speech Auto Attendant option is not installed.
- New users will not be added to the SAA directory immediately. To see an updated list, you can wait for the nightly NuPoint UM Auto Update or you can force an update using the NuPoint UM Data Source sync function. For more information, refer to the *Update the User Data Source* topic in the online help.
- To add an attendant-recognized Department, see Add or Edit Department Information.

13.2 Configure Groups

Users often have more that one phone. For example, a user could have a desk phone, a cell phone, and a teleworker set. This feature allows you to group a user's phones together under one directory number so that a call to that number rings all of the user's phones. Calls ring the prime extension, which is referred to as the "pilot number" or "prime phone". Other group members are referred to as non-prime phones.

There are two types of groups:

- **Personal Ring Groups (PRGs)** allow two or more phones for a single user to be grouped under a common directory number. The typical scenario is a person's desktop phone and cell phone are twinned

together, where the desk phone is considered the prime extension. Each phone in the PRG requires a full MiVoice Business IP User License.

- **Multi-Device User Groups (MDUGs)** allow a single user to have multiple phones grouped under a common directory number without each phone requiring a full MiVoice Business IP License. There are two types of Multi-Device User Groups:

  - *Standard:* allows up to eight phones to be grouped under a common directory number. Only the prime number requires an IP User License. The group itself, requires a MDUG license. In a MDUG, phone functionality is essentially limited to one device in the group at any given time. When one of the user's phones is engaged in call, the other phones are consider busy (in other words, "One Busy All Busy" is always enabled) and have restricted functionality.
  - *External Twin:* allows only two phones, typically a desk phone and a cell phone, to be twinned. This type of group does not require a MDUG license. It only requires an IP User License and an External Hot Desk User license. The prime number uses the IP User license. The second member must be an External Hot Desk number and consumes the EHDU license.

Each user is only allowed one Personal Ring Group and one Multi-Device User Group. Each group can have up to eight members. From MiCollab , you can only configure the Prime Phone, Secondary Phone, and Other Phone as members. You must configure any additional group phones from the MiVoice Business System Administration Tool.

Note:

Aftercreating users with MDUG/PRG, perform a manual PBX synchronization (**Sync Now**) to *immediately* update the MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization. For information on how to manually perform a manual PBX sync, see the *MiCollab Client Admin Online Help* > *The Administrator Interface* > *Synchronization Tab* section.

Note:

Groups are not supported for MiVoice 5000 or MiVoice MX-ONE integration (**Groups** tab is not present).

Note:

PRGs and MDUGs apply to MiVoice Business platforms only.

Note:

MDUGs are only supported for MiVoice Business Release 6.0 or later.

Add a New Group

1. Assign a Role tp the user that supports PRGs or MDUGs.
2. Assign the user's Mitel 3300 ICP Phones with a Service Level in the **Phones** tab:
   - **Full Service** phones can only be assigned to Personal Ring Groups (PRGs).
   - **Multi-Device Service** phones can only be assigned to Multi-Device User Groups (MDUGs).
3. Click the **Groups** tab.
4. Click **Add New Group**.
5. Select the group type. The available group types depend on the types of phones that are assigned to the user.
6. Select the prime number. Incoming calls to the user's phones will ring the prime number.
7. If the group type is PRG, enable or disable the "One Busy All Busy" option.
8. Select a user's phone from the Phones drop-down menu and click **Add phone**. You can only add phones if you have selected a prime number. The phone number is added to the list.
9. Click **Save**.

Add a Phone to an Existing Group

1. Select a user's phone from the Phones drop-down menu and click**Add phone**. You can only add phones if you have selected a prime number. The phone number is added to the list.
2. Click **Save**.

Delete a Phone from a Group

1. Click the **Groups** tab.
2. In the Groups table, select the number of the group. The phones in the group are listed.
3. Click  to delete a phone. You can only delete non-prime phones. To delete a prime phone, you must delete the group.
4. Click **Save**.

Delete a Group

1. Click the **Groups** tab.
2. Click **Delete Group** and select the extension number of the prime phone from the drop-down menu.
3. Click **Ok**.

Field Descriptions

Field	Description	Default Values
Groups		
Number	Identifies the Pilot phone for the group. The phones are grouped together under the primary phone directory number. This field is read-only.	Primary Phone
Type	Identifies the type of group: • *Personal Ring Group (PRG)*: Allows two or more phones for a single user to be grouped under a common directory number. The phones ring simultaneously (Ring All) when called. The typical scenario is a person's desktop phone and cell phone are twinned together, where the desk phone is considered the prime extension. Both phones require a full MiVoice Business IP User Licence. • *Multi-Device - Standard*: Allows up to eight phones to be grouped under a common directory number. The phones in this group are licensed collectively to a user with a single Multi-device Users license. • *Multi-Device - External Twin*: Allows only two phones, typically a desk phone and a cell phone, to be twinned. This type of group requires an IP User License and an External Hot Desk User license. The prime number uses the IP User license; the second number uses the External Hot Desk User license .	Multi-Device - Standard

Field	Description	Default Values
One Busy All Busy	This option applies to PRGs only. If this option is enabled, busy is returned for all phones if ONE phone in the PRG group is busy. If this option is disabled, then all members of the group are rung even if one or more phones (but not all phones) are busy. You enable or disable this feature against the group prime member and the feature setting is applied to all the group phones.	No
Phones in Group		
Add member	Check the boxes to include phones as members in the group.	By default, both Secondary and Other Phone are included in the group.
Number	Extension number of phone.	
Presence	Enables Presence feature for the PRG or member phone. This feature lets users choose which of their personal answer points they want to receive their calls at by making it 'Present' and the others 'Absent.' If you enable this feature for the pilot number, the feature is enabled for all group phones.	Present
	Click to delete a phone from the group. You can only delete non-prime phones.	Not applicable

13.3 Enter NuPoint UM Information

The **NuPoint Unified Messaging** tab allows you to configure basic messaging information for a user. You must configure the advanced features from the NuPoint UM Web Console. If Flow Through Provisioning is enabled, changes will also be made to the MiVoice Business database.

Add New Mailbox

To add a new mailbox for this user:

1. Click the **NuPoint Unified Messaging** tab.
2. Click **Add New Mailbox**.
3. Complete the required fields (see table below for details).
4. Click **Save**.

Assign Existing Mailbox

To assign an existing mailbox to this user: (You can view and manage unassigned services using the **View** button on the Users and Services directory page.)

1. Click the **NuPoint Unified Messaging** tab.
2. Click **Assign Existing Mailbox**. The Assign dialog box is displayed.
3. Select the number of the existing mailbox that you want to assign.
4. Click **Assign**.
5. Complete the required fields (see table below for details).
6. Click **Save**.

Delete Mailbox

To delete the mailbox for this user:

1. Click the **NuPoint Unified Messaging** tab.
2. Click **Delete Mailbox**. A list of existing mailboxes for the user is displayed.
3. Click the mailbox number you want to delete.
4. Click **Yes** to confirm the deletion.

Note:
First time voice mail users are offered the option to enter four zeroes for a "no password" option. Choosing this option causes the passcode for NuPoint UM to be different from the passcode for all other MiCollab applications. To remove the option from the voice mail prompt, disable FCOS option 125.

Mailbox Field Descriptions

Field	Description	Values
Mailbox Number	Enter a mailbox number or select **Use Extension Number** to use your extension number as your mailbox number (recommended).	1 to 11 digits. Numbers must be unique in the NuPoint UM system. If * or # are included in the original phone number, the system removes them from the mailbox number.
Extension	For MiVoice Business , select your extension number from the list. For MiVoice Office 250 , enter your extension number.	
Use Extension Number for Mailbox	Associates the mailbox with the extension number (recommended). This feature is enabled by default. Clear the checkbox to disable the option and manually enter a mailbox number.	
Attendant Extension	This is the number that is called if user dials 0 to return to the attendant. If an attendant extension is defined, it is assigned to ALL mailboxes being created.	Maximum 15 digits.

Field	Description	Values
Feature COS	The Feature Class of Service (FCOS) controls mailbox user privileges and outside caller functions for the mailbox. Individual privileges and restrictions are designated by numbers, which are referred to as "feature bits". Each FCOS has its own unique combination of these feature bits. For example, a user's ability to make, give, or answer messages is controlled by the FCOS assigned. The FCOS that you specify is assigned to ALL mailboxes being created.	Default is 14. **Note**: Changing the content of FCOS 14 will change ALL mailboxes.
Limits COS	The Limits Class of Service (LCOS) imposes limits on mailboxes. It can be a valuable tool for allocating disk storage space and port use. Each LCOS can set the maximum times allowed for recording mailbox greetings, user messages, caller messages, and mailbox names; it can limit the amount of time a user remains logged in during one session. The LCOS can specify the maximum time that a played or unplayed message can be stored in a mailbox before it is erased by the automatic purge. It can specify the maximum number of messages that a user can accumulate in a mailbox. You can also modify an LCOS to specify secondary language prompts. The LCOS that you specify is assigned to ALL mailboxes being created.	Default is 1. **Note**: Changing the content of LCOS 1 will change ALL mailboxes.

Field	Description	Values
Message Waiting #1	Select the type of message waiting notification from the list.	Default is None.
Message Waiting #2		
3300 Record-A-Call	Select the check box to assign the MiVoice Business "Record-A-Call" Class of Service to this phone.	Default is blank.
Standard Unified Messaging	Select the check box to enable Standard Unified Messaging for the user's mailbox. **Note**: For MiCollab Release 4.0 and later systems, you must enable the Standard UM option using the check box in the NuPoint UM tab of the USP application. You cannot enable the Standard UM option	Default is unchecked. 1. Under **Applications**, click **NuPoint Web Console**. 2. Click **Mailboxes**. 3. Edit the user's mailbox. 4. Clear the email address fields. 5. Return to the USP NP-UM tab and clear the **Advanced Unified Messaging** box. **Note**: The following configuration conditions apply:

Field	Description	Values
	through the NuPoint UM web console. Standard UM provides voice mail and FAX access to Lotus	• The NuPoint UM Feature COS assigned to the mailbox must have the Standard UM feature enabled.

Field	Description	Values
	Notes, Novell GroupWise and Microsoft Outlook e-mail clients, or from the Web View in the user's e-mail client or Web browser. Users can also access	• A Standard UM license is required for each mailbox that requires Standard Unified Messaging.

Field	Description	Values
	voice, FAX, and Record-A-Call messages from the telephone user interface (TUI). When a voice mail message is left in a Standard Unified	• If a UCC license bundle or MiVB Subscription license bundle is assigned to the mailbox user, this option is enabled by default and read-only.

Field	Description	Values
	Messaging mailbox, the system sends messages to the *UM SMTP Email Addresses* that are defined for the user's mailbox. You can define these email addresses in the user's mailbox through the *NuPoint UM Web Console*, or the user can define them through their *MiCollab End User Portal*. Refer to the *Unified Messaging book* in the *NuPoint UM Web Console* online help for additional details.	• If you clear the check box, Standard UM is disabled for the user and the license is removed. Also, the Standard UM email addresses are cleared from the Mailbox page in the user's MiCollab End User Portal.
Advanced Unified Messaging	Select this check box to assign the Advanced Unified Messaging feature to the user's mailbox. Note that users must also enter their Advanced UM Email Alias and password from their end-user portal to enable the feature.	Default is unchecked. **Note**: The following configuration conditions apply:

Field	Description	Values
	Advanced Unified Messaging offers a high level of messaging integration and synchronization between a user's e-mail client	• The NuPoint UM Feature COS assigned to the mailbox must have the Advanced UM feature enabled.

Field	Description	Values
	and NuPoint UM voice mailbox. Full MWI synchronization is provided for voice messages that are accessed through the e-mail client. Message status	• An Advanced UM license is required for each mailbox that requires Advanced Unified Messaging.

Field	Description	Values
	synchronization is provided for e-mails that are listened to from the NuPoint UM voice mailbox (they are marked as "read" in the e-mail inbox).	• If a UCC license bundle or MiVB Subscription license bundle is assigned to the mailbox user, this option is enabled by default and read-only.

Field	Description	Values
	Advanced UM users can access their voice, fax, RAC, and email messages (from their Microsoft Outlook inbox or Lotus Notes 7 inbox, and from the NuPoint UM Voice mailbox) over the phone. Access to email via the Telephone User Interface (TUI) is enabled by integration with the email client, the email server, and text-to-speech (TTS) technology. Refer to the *Unified Messaging book* in the *NuPoint UM Web Console* online help for additional details.	• If you clear the check box, Advanced UM is disabled for the user and the license is removed. Note that before you can clear the box, you must first delete the Unified Messaging email addresses from the user's mailbox:

Note:
New users will not be added to the SAA directory immediately. To see an updated list, you can wait for the nightly NuPoint UM Auto Update or you can force an update using the NuPoint UM Data Source synch function. For more information, refer to the *Update the User Data Source* topic in the online help.

Flow Through Provisioning Changes

- When you **Add New Mailbox**, and assign it to a user, the selected extension's information will be updated on the MiVoice Business .
- When you **Assign Existing Mailbox**, no updates are made to the MiVoice Business as the service already exists. Although both interfaces can be used to perform this task, we recommend that you use the Users and Services application rather than the Web Console.
- When you **Delete Mailbox**, the phone service and COS options for the selected DN on the MiVoice Business are set to values appropriate to the remaining services, and Call Forwarding is removed.

13.4 Enter MiCollab Client Information

MiCollab Client is an application that provides users with access to features such as Dynamic Status, presence, contact management, and collaboration from the web and mobile clients:

The MiCollab Client tab allows you to:

- assign a Feature Profile to the user's MiCollab Client service
- assign the user's desk phone and softphone extension with MiCollab Client service, and
- associate a mailbox with the MiCollab Client service
- assign a Deployment Profile for the deployment of a MiCollab MAC or PC Client without a softphone
- enable or disable MiTeam Classic for Premium UCC licensed users, MiVB Subscription Premier, and MiVB Subscription Elite CX bundles via a check box.

Assign MiCollab Client Service

To assign a user with MiCollab Client service:

1. In the Users and Services directory, click the **User** tab.
   - Click **Add**.
   - Enter User Information
   - Click **Save**.
2. Click the **Phones** tab.
3. Click **Add New Phone** and enter the Phone Information.
4. Configure the user with one or more desk phones and softphones.
5. Click **Save**.
6. Click the **MiCollab Client** tab.
7. Assign a Feature Profile to the user.
8. Select the user's desk phone extension. You can only assign one of the user's desk phones with MiCollab Client service. Leave as "None" if you are configuring a MiCollab MAC or PC client without a desk phone.
9. Select the user's softphone extension. You can only assign one of the user's softphones with MiCollab Client service. Leave as "None" if you are configuring a MiCollab MAC or PC client without a softphone.
10. If required, associate a mailbox with the MiCollab Client account. Select "Other Mailbox" and enter the mailbox number.
11. If you are deploying a MiCollab MAC or PC client without a softphone, select the desired Deployment Profile. By default, this field is set to "Do Not Deploy".
12. For Premium UCC users, MiTeam Classic functionality is enabled by default. To disable MiTeam Classic, clear the check box. The MiTeam Classic check box is only displayed for Premium UCC users. See MiTeam Licensing for details.
13. Click **Save**.

Note:
You can always associate a user's phone with the MiCollab Client service. However, if the user's Feature Profile does not include a desk phone or softphone license, then the MiCollab Client service is not supported.

Configure two softphones for MiCollab PC client and Mobile client

Note:
Please note that this feature is only applicable to UC Endpoint Devices or Generic SIP Devices.

To configure two softphones, one for MiCollab PC Client and the other for MiCollab Mobile Client for a single user, perform the following steps:

1. Create a new user template with two softphones. To create a user template, the following must be considered:
   - Include teleworker service for both softphones
   - Phones must be in MDUG or PRG
   - Select a deployment profile
   - Select UCA feature profile which includes Softphone and Mobile SIP Softphone feature bits. UCC Standard and Premium feature profiles includes these feature bits.
2. Create a new user using this new template.
3. Perform PBX Sync in UCA.
4. Once a user is created, the user should receive two deployment emails for two softphones.
5. Deploy one softphone on PC client and one on Mobile Client.

Assign a User with MiCollab Client Teamwork Mode

Teamwork Mode allows MiCollab Client clients who do not have a desk phone or softphone to use non-telephony MiCollab Client features such as the following:

- Chat
- Collaboration Integration
- Presence
- Contacts
- Instant Messaging
- Dynamic Status
- Visual Voice Mail

Because a user does not have a desk phone or softphone, any MiCollab Client telephony features are not available. Teamwork Mode is not a licensed option.

To assign a user with MiCollab Client Teamwork Mode on the MiCollab system:

1. Log into MiCollab server manager.
2. Under **Applications**, click **MiCollab Client Service**.
3. Click **Configure MiCollab Client Service** and then click **Features**.
4. Add a MiCollab Client "Teamwork" feature profile in the MiCollab Client application with the desired features enabled.

5. Under **Applications**, click **Users and Services**.
6. In the Users and Services directory, click the **User** tab.

   - Click **Add**.
   - Enter the user information. At a minimum, enter the user's first name, last name, login ID, and an initial login password and TUI passcode.
   - Click **Save**
7. If Visual Voicemail is required, click the **NuPoint Unified Messaging** tab.

   - Enter a mailbox number. Note that a voice mailbox license is required.
   - Select the Feature COS required for Visual Voice Mail.
   - Click **Save**.
8. Click the **MiCollab Client Service** tab.

   - In the Feature Profile field, assign the "Teamwork" feature profile.
   - Leave the **Desk phone extension** and **Softphone extension** fields set to "None".
   - Click **Save**.

Field Descriptions

Field	Description
Feature Profile	Assign a Feature Profile to this user. The feature profile defines the group of licensed MiCollab Client features that are assigned to a user. Default is Feature Profile 1.
Desk phone extension	Select the extension that you want to assign with MiCollab Client desk phone service. You can only assign one of the user's desk phones with MiCollab Client service. To remove MiCollab Client service, select **None**.
Softphone extension	Select the extension that you want to assign with the MiCollab Client softphone service. You can only assign one of the user's softphones with MiCollab Client service. To remove MiCollab Client service, select **None**.

Field	Description
Mailbox number	This field displays the directory number of the mailbox that is associated with this MiCollab Client account. If the MiCollab Client account does not have a mailbox, this field is blank. By default, the system associates the first mailbox that you assign to the user with the user's MiCollab Client account. • If multiple mailboxes are assigned to the user, you can associate a different mailbox with the user's MiCollab Client account, by selecting the mailbox number from the drop-down list. • To assign a new mailbox, select **Other Mailbox** and enter a valid mailbox number in the **Number** field. • To remove a mailbox from a user's MiCollab Client account, select **None**.

Field	Description
Deployment profile	This field allows you to select the deployment profile that should be applied when you deploy a MiCollab MAC or PC Client to a user. After you click **Save**, a deployment e-mail is sent automatically to the user. The extension field in the e-mail is set to "None". The user clicks the link in the e-mail to complete the deployment. Default is "Do Not Deploy". Typically, you would select the Default profile. **Note**: If there is no phone for which a deployment profile is selected, users need to provide their password every time they log in to PC and Mobile Clients. **Note**: If a phone with a deployment profile is added later, the user must provide their password for every login to PC and Mobile Clients. However, if the administrator or the user changes the password after the user logs in, the updated password is automatically used for the next login to PC and Mobile Clients. **Note**: If a user is deployed from the MiCollab Client Service page, the Client will prompt for the password. This scenario occurs because the password is not set from MiCollab Server in the deployment configuration for the user. MiCollab Server will not have the password in cleartext during the deployment.

Field	Description
MiTeam Meetings	Allows you to disable or re-enable MiTeam Meetings for the user. This box applies to all UCC license bundles (except Basic bundle) and MiVB Subscription license bundles and users on-boarded to CloudLink. • When you clear this box, the cross launch functionality from MiCollab Client to MiTeam Meetings application is disabled. • When you check this box, the users can click on **Meetings** option in the Client to open the MiTeam Meetings application.
MiTeam Classic	Allows you to disable or re-enable MiTeam Classic for the user. This box only applies to UCC Premium users with an active MiTeam Classic license. By default, this box is checked. • When you clear this box, the MiTeam tab is removed from the user's client. • When you check this box, the MiTeam tab is added to the user's client.

13.5 Enter MiCollab Audio, Web and Video Conferencing Information

The **Audio, Web and Video Conferencing** tab allows you to provision a registered phone for MiCollab Audio, Web and Video Conferencing service.

Note:
For integration with the MiVoice 5000 or MiVoice MX-ONE platforms, the AWV users must be provisioned from the MiVoice 5000 or MiVoice MX-ONE management interfaces. Hence, the fields in this tab are read-only. The deskphone and softphone extension numbers are the same as the primary phone number.

For MiVoice Business integrations, you can use either MiCollab or LDAP to provision MiCollab Audio, Web and Video Conferencing users. You cannot use both methods. If you are using MiCollab to provision MiCollab Audio, Web and Video Conferencing users ensure that the **Use LDAP** check box in the **LDAP Configuration** screen of MiCollab Audio, Web and Video Conferencing is unchecked before you add MiCollab Audio, Web and Video Conferencing users. If you are using LDAP to provision MiCollab Audio, Web and Video Conferencing users:

- The **Use LDAP** check box should remain checked.
- Do not provision users with the MiCollab Audio, Web and Video Conferencing services through MiCollab .
- Do not duplicate LDAP user accounts and MiCollab MiCollab Audio, Web and Video Conferencing user accounts; otherwise, end users will be unable to log into MiCollab Audio, Web and Video Conferencing collaboration sessions.

Add MiCollab Audio, Web and Video Conferencing Service

To add MiCollab Audio, Web and Video Conferencing service to this user:

1. Click the **Audio, Web and Video Conferencing** tab.
2. Click **Add** .
3. In the **Registered Phone** field, enter the extension of the phone to use for MiCollab Audio, Web and Video Conferencing , or select a previously-configured phone from the list.
4. Select **DialOutAllowed** to allow this user to make system calls through the CO. (Default setting is enabled.)
5. Select **DenyMultipleLeaders** to restrict this user from having multiple callers using the leader access code on collaboration calls. (Default setting is disabled.)
6. Select **Executive** to allow this user access to ports that are reserved for the exclusive use of high priority users. (Default setting is disabled.)
7. In the **Reservationless Calls** list, select one of the following options:

   - **Reservationless calls allowed, leader not required**: (default) This user can make reservationless calls and a leader code is not required to access the call.
   - **Reservationless calls allowed, leader required:** This user can make reservationless calls, but a leader code is required to access the call.
   - **Reservationless calls not allowed:** This user cannot make reservationless calls.
8. In the **Email Type** field, select one of the following:

   - **Generic Long**: Use this setting for e-mail clients (for example, Microsoft Outlook) that allow for long form inserts (usually more than one line).
   - **Generic Short:** Use this setting for e-mail clients that only allow short form inserts (usually one line).
9. Click **Save** .

Note:
User must have an email address before MiCollab Audio, Web and Video Conferencing service can be added. If the email address of this user matches a currently unassigned MiCollab Audio, Web and Video Conferencing service, then the unassigned service will be assigned to this user automatically.

Assign Existing MiCollab Audio, Web and Video Conferencing Service

To assign an existing MiCollab Audio, Web and Video Conferencing service to this user: (You can view unassigned services using the View button on the Users and Services directory page.)

1. Click **Assign** . The Assign dialog box is displayed.
2. Choose an MiCollab Audio, Web and Video Conferencing service to assign to this user.
3. If this user already has an email address assigned, you are prompted to do one of the following:

   - set the user's current email address to the email address specified in the MiCollab Audio, Web and Video Conferencing service
   - keep the users' current email address and change the address specified in the MiCollab Audio, Web and Video Conferencing service. Note that changing an MiCollab Audio, Web and Video Conferencing user's email address deletes the original MiCollab Audio, Web and Video Conferencing account, including collaboration history.
4. Click **Assign** .
5. Click **Save** .

Edit MiCollab Audio, Web and Video Conferencing Service

To edit MiCollab Audio, Web and Video Conferencing service and defaults for a user:

1. Select the user to edit from the directory.
2. Click **Edit** .
3. Click the **Audio, Web and Video Conferencing** tab.
4. Change settings for this user as required.
5. Click **Save** .

Note:
Email address is not editable in the MiCollab Audio, Web and Video Conferencing interface. To edit, administrators use the Users Services and Provisioning application in the Administrator Portal. Users can edit their email addresses from their MiCollab End User Portal .

Delete MiCollab Audio, Web and Video Conferencing Service

To delete MiCollab Audio, Web and Video Conferencing service from a user:

1. Select the user from the directory.
2. Click **Edit** .
3. Click the **Audio, Web and Video Conferencing** tab.
4. Click **Delete Service** . A confirmation dialog is displayed.
5. Click **Yes** to confirm the deletion.

13.6 Enter MBG Information

MBG is a software application that provides teleworker services. This application connects a remote office to the corporate voice network to provide remote users with full access to voice mail, collaboration, and all the other features of the office phone system.

Note:
For MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400 deployments, you cannot add a teleworker service from the Users and Services application or MiVoice Border Gateway (changing a UCC bundle from Entry to Standard or Premium is not supported).

To add/edit MBG teleworker service for a user on a MiVoice Business communications platform:

1. Click the **Teleworker** tab.
2. Click **Add New Teleworker**.
3. Select a phone from the drop-down menu. You must assign a teleworker compatible phone; otherwise, you will receive the following error when you attempt to add teleworker service: "This user does not have any available teleworker-compatible phones to assign".
4. Complete the required fields (described in table below).
5. Click **Save**.
6. If you assign the Teleworker service to a SIP phone, thesystem automatically configures a corresponding SIP service on the MiVoice Border Gateway. The **Set-side username** on the MiVoice Border Gateway is set to <username-DN> (for example smithj-7328).MiCollab sends a randomly generated **Set-side password** to the user in a Service e-mail for the SIP Phone. After logging in using the generated password, the user is prompted to replace it with a strong password. The passwords for other existing phones are not changed.

To assign an existing MBG teleworker service to a user's device: (You can view unassigned services using the View button on the Users and Services directory page.)

1. Click the **Teleworker** tab.
2. Click **Assign Existing Service**.
3. Select an existing extension from the list.
4. Modify the data as required.
5. Click **Save**. MiCollab sends a randomly generated password to the user in a Service e-mail. After logging in using the generated password, the user is prompted to replace it with a strong password.

To delete MBG teleworker services from a user's device:

1. Click the **Teleworker** tab.
2. Click **Delete Service**. A list of existing extensions for the user is displayed.
3. Click the extension number to delete.
4. Click **Yes** to confirm the deletion.

Field Descriptions - MBG

Field	Description	Values
Phone		
Phone	Select the type of phone (for example Office or Home Phone) that hosts the teleworker service.	If you want to assign teleworker service, you must select a phone type that supports teleworker.
Status	Status of the teleworker service.	Enabled or disabled
MAC Address	Displays the MAC Address of the teleworker set in the following format: XX:XX:XX:XX:XX:XX. The MAC Address is printed on a label that is affixed to the base of Mitel IP phones. (In order to assign teleworker service to a phone, you must first enter the phone's MAC Address in the **Phone** tab.) **Note**: This field does not apply when device type "Hot Desk User" or "SIP Generic Device" type is selected.	12 hexadecimal characters separated into 6 pairs by 5 colons.

Field	Description	Values
Last Connected Server ID	When MiCollab is deployed with remote teleworker service, the MiCollab server in the LAN is clustered with an MBG server in the DMZ. Both the MiCollab server (master) and the MBG server (slave) have the teleworker application installed. However, the Teleworker phones are supported by the MBG server in the DMZ. The Teleworker application on the MiCollab server is only used to remotely manage the Teleworker phones on the MBG server. This field identifies the MBG server that is providing the Teleworker service to this phone.	Domain name of the MBG server. Click the Details link to access the Teleworker application that is running on the MBG server.

13.7 Enter Vidyo Information

Vidyo is a video conferencing solution that provides user with high definition, low-latency video to mobile phones, desktops, and meeting rooms.

Pre-requisites:

1. Complete the following tasks. Refer to the *Vidyo Product Documentation*and the *Mitel Vidyo Quick Reference Administrator Guide*for instructions:
   - Deploy and license the Vidyo Portal. Licensing is not controlled from the Mitel Application Management Center (AMC). Vidyo licenses must be installed on the Vidyo system.
   - Assign the Vidyo Portal with a Fully Qualified Domain Name (FQDN) that is resolvable within the network.
   - Create a Vidyo administrator account.
2. Complete the Vidyo Settings page in the MiCollab server Manager. Use HTTPs to prevent the administrator credentials from be passed in the clear over HTTP. After you save the form MiCollab confirms the URL, connectivity, and credentials.
3. After the MiCollab system connects successfully to the Vidyo system, the Vidyo services are enabled and the Vidyo licenses are listed in the Licensing Information page of the MiCollab server manager.

Adding or Deleting Vidyo Services

To add Vidyo service for a user:

1. In the Users and services directory, select a user and click **Edit** existing user
2. Click the **Vidyo** tab.
3. Click the **Create Vidyo Room for User** box.
4. Select a service type (described below).
5. Click **Save** .

Note:
If you receive the following error message: " **Vidyo Portal error: Invalid Extension - Extension does not start with Tenant Prefix"**, you must correct the Tenant Dialing Prefix.

To delete Vidyo service from a user's device:

1. In the Users and services directory, select a user and click **Edit** existing user
2. Click the **Vidyo** tab.
3. Clear the **Enable Vidyo Service** box.
4. Click **Save**. If the user is in a Vidyo session when the account is deleted, the user is presented with the login screen. Any attempts to log in again will fail because the account no longer exists.

Field Descriptions - Vidyo

Field	Description	Default
Enable Vidyo Service	Check the box to enable the service. Clear the box to disable.	Disabled
Service Type	**Normal**: Assign this setting to regular users. It allows a user to host personal Vidyo meetings from a desktop device or mobile device. VidyoMobile and VidyoDesktop users can also host meetings or join with other Vidyo users and room systems.	Default is Normal

Field	Description	Default
	Vidyo Room: Assign this setting to meeting rooms. Meeting rooms must be equipped with a Vidyo supported device. **Note**: Vidyo supports their own room systems and devices. The MiVoice Video Phone can connect to a Vidyo conference via the Vidyo Gateway product (which supports connecting SIP enabled video devices to Vidyo's proprietary video codec environment). The MiVoice Video Phone user must dial into the Vidyo conference using the "Dial by URI" feature.	
	Executive: Assign this setting to priority users. It allows them to connect from any VidyoMobile or VidyoDesktop enabled device without a concurrent use license.	
	Panorama: Assign this setting to meeting rooms that are equipped with multiple screens (up to nine high-resloution screens are supported).	

13.8 Enable Google Integration Features

If your system is integrated with Google Apps, you can enable the following features for MiCollab users:

- **Gmail Integration**: Allows users to initiate a call from one of their telephones by clicking a gadget in their Google Gmail email client.

- **Google Calendar Integration**: Allows users to transform a Google Calendar event into a MiCollab Audio, Web and Video Conferencing session by selecting a gadget. Conferences created in this manner can be accessed from the invitation email or the Calendar event.

See About Google Apps Integration.

13.9 Add External Numbers

You can add external numbers (such as a user's cell phone number or home number) to the MiCollab Client corporate directory so that other MiCollab Client users can place calls to the numbers.

External numbers can be added either

- manually from the Users and Services applications, or
- automatically from Active Directory server via Integrated Directory Services, or
- from a CSV file (see Bulk Import from File)

Requirements and Conditions

- MiCollab must be configured with MiCollab Client in integrated mode.
- For Teamwork Mode users, the primary, secondary, and mobile numbers also appear in the MiCollab Client clients.
- For Integrated Directory Server integrations, any contacts that are imported from the Active Directory server will also have the Mobile Phone 2 number added to their MiCollab Client.

Limitations

- On upgrade to MiCollab Release 7.2 SP1 or later, external numbers for existing ‘Other PBX Phones’ in the MiCollab database are NOT migrated into the MiCollab Client corporate directory. External numbers must be added either manually or via Integrated Directory Services.
- Although you can configure a DID Service Number for the Primary Phone of a MiVoice Business user, this number is not added to the MiCollab Client corporate directory. Only DID numbers that you enter in the ‘Other PBX Phone’ field are added. The DID Service number field and ‘Other PBX Phone’ field are separate and distinct. The numbers in these fields are not synchronized.
- External numbers are available in the corporate directory of MiCollab Clients and are listed under the user's **Account > Phones** tab in MiCollab Client Service administration interface. External numbers are not listed in the Corporate Directory tab.

Adding External Numbers Manually

To add an external number (such as a cell phone) for a user:

Note:
This procedure applies to MiCollab with MiVoice Business platforms only.

1. Access the User and Services user directory.
2. Edit the user record.
3. Click the **Phones** tab.
4. Click **Add New Phone**.
5. Select "Other PBX Phone" as the Phone Type.
6. Enter the external number.
7. Click **Save**. The External number is available in the corporate directory of MiCollab Clients and is listed under the user's **Account > Phones** tab in MiCollab Client Service administration interface.

Adding External Numbers via Active Directory

External numbers can also be added from Active Directory using Integrated Directory Services.

1. Configure Integrated Directory Services.
2. Ensure that the Direct Inward Dial Number and Mobile Phone Number 2 attributes are mapped to the corresponding Active Directory attributes.
3. Perform an IDS synchronization. The DID numbers and the Mobile Phone 2 numbers are automatically created as ‘Other PBX Phones’ for the users in the Users and Services directory. The numbers now appear in the corporate directory of MiCollab Clients.
4. If you change the DID number and Mobile Phone 2 phone in Active Directory, the change is reflected in the MiCollab Client corporate directory.

About MiTeam Classic 14

This chapter contains the following sections:

- MiTeam Classic Licensing
- MiTeam Classic Configuration
- Provision MiTeam Classic

MiTeam Classic is a Mitel's Cloud-based collaboration tool that provides mobile users with the ability to access features, such as:

- **Collaborate:**Manage collaboration Classic streams
- **Chat**: Hold chat sessions and receive chat notifications
- **Pages**: Add white-board pages
- **To-Do**: Create to-do lists
- **File Sharing**: Store and share files, and
- **MiTeam Meet:**Perform audio and web sharing within a team.

Requirements

- MiTeam Classic is supported for UCC Premium users on MiCollab Release 7.2 and later systems.
- The MiCollab server requires bi-directional access to the MiTeam Classic solution on the Internet at the following top-level MiTeam FQDNs: miteam.micloudoffice.com and api.micloudoffice.com. Because Internet access is required, MiTeam Classic is not available to Dark Data Centers. Note that in a private cloud these FQDNs will be different.
- Port 443 must be open for incoming and outgoing traffic. The MiCollab server communicates with the MiTeam Classic solution via Port 443.
- Users must be supported under the same OrganizationID in order to join chat, share files and so forth. The OrganizationID is an identifier for your company in the MiTeam Classic service provider.
- Peered servers must share the same OrganizationID if MiTeam Classic is enabled. The OrganizationID is used group the UCC Premium users from the servers into a cloud user group.
- MiTeam Classic users cannot log into the cloud service directly at https://miteam.micloudoffice.com/ (Moxtra's public Web Client).
- MiVoice Border Gateway Release 9.3 or later is required.
- In order for users to use MiTeam Meet, the Audio, Web and Video application must be configured and active. The maximum duration of a MiTeam Meet is 2 hours. This maximum duration is not configurable.
- Do not enable the Audio, Web, and Video Enable Port Reservations option if MiTeam Classic is required. These two features are mutually exclusive. When the **Enable Port Reservations** option is enabled, MiTeam Classic users are unable to join a Classic stream.

Browser Support

To use MiTeam Classic from the web client, users must allow third-party cookies in their browsers. If cookies are disabled, users are unable to open Classic streams.

Chrome

1. Click  .
2. Click **Settings** > **Show advanced settings** > **Content Settings**.
3. Enable "Allow local data to be set (recommended)".
4. Disable "Block third-party cookies and site data"
5. Click **Finished**.

FireFox

1. Under **Options** > **Privacy** > **History**.
2. Check "Accept cookies from sites".
3. Set "Accept third-party cookies" to "Always".
4. Set "Keep until they expire".

Safari

1. Click **Settings**.
2. Click **Privacy**.
3. Set **Cookies and Website-Data**: to “just from websites I visit” or “Always allow”.

Microsoft Edge

1. Click . . .
2. Click **Settings**.
3. Click **Show Advanced Settings**.
4. Click **Cookies**.
5. Enable **Do not block any cookies**.

Supported Clients

MiTeam is supported with the following MiCollab Clients:

- MiCollab for PC Client (Windows 7 and 10 only)
- MiCollab Web Client (Windows/MAC only)
- MiCollab for Mobile Client (iOS/Android only).

The following minimum operating systems are required:

- iOS 9+ (not supported on iPad or iPod)
- Android Phone 4.4 +

MiTeam Classic is not supported on the following MiCollab Clients:

- Legacy Web Client
- Blackberry Client

- Windows Phone Client

Supported Communication Platforms

MiTeam Classic is supported for single and multiple MiCollab server deployments on the following Mitel communication platforms:

MiVoice Business

MiVoice MX-ONE

MiVoice 5000

MiVoice Office 400

MiTeam Classic is only supported in MiCollab Client Integrated Mode. It is not supported for MiCollab Client Co-located mode or on MiCollab Client stand-alone systems.

Note:
If you have UCC Premium users on a MiCollab system where MiCollab Client is in co-located mode and then run the MiCollab Client Integration Wizard to place MiCollab in integrated mode, MiTeam is not automatically enabled for the users. You must manually enable MiTeam Classic from the MiCollab Client tab of the User and Services application.

14.1 MiTeam Classic Licensing

With MiCollab 8.0 and later, MiTeam Classic licensing is driven by license keys. MiTeam Classic licenses (MiTeam Uplifts) can be ordered through MitelCPQ. All existing UCC Premium users will have a license automatically added to their account by Mitel as part of the transition to MiCollab 8.0 and later.

Notification – Expiry of License

Ensure that your administrator's e-mail address is entered in the **E-mail settings** page in the server manager to allow the system to send you MiTeam Classic licensing notifications.

Two months before the expiry of your license,you will receive a monthly e-mail notification that your MiTeam Classic licenses are due to expire. Take appropriate action to ensure that MiTeam Classis services continue and there is no loss of account data. The e-mail includes a link to a report that lists the users and their MiTeam Classic status, as well as a link to the MiCollab Licensing Information page.

Note:
Notifications are not provided if MiCollab is a cloud service provider integrated with Oria.

MiTeam Classic Status Report

You can generate a report of the MiTeam Classic user status.

14.2 MiTeam Classic Configuration

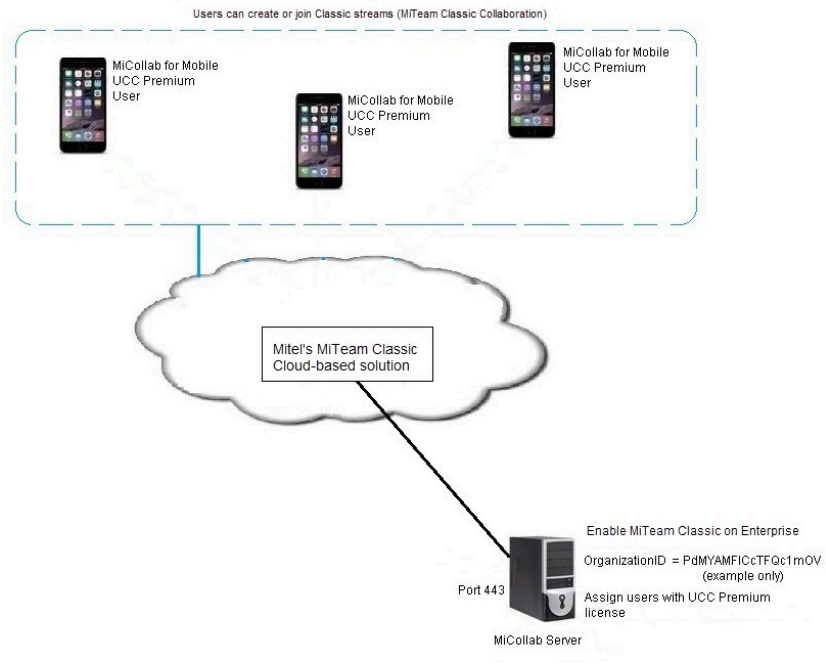
MiTeam Classic is supported in the following deployments

- Enterprise Configuration - Non-Peered
- Enterprise Configuration - Peered

Enterprise Configuration - Non-Peered

This section describes MiTeam Classic configuration for non-peered Enterprise deployments. If your Enterprise has peered servers, see the following section.

Figure 5: MiTeam Classic – Enterprise Configuration (Non-Peered)



By default, MiTeam Classic is disabled. To enable MiTeam Classic on an Enterprise:

1. Log into the MiCollab server manager.
2. Under **Applications**, click **MiCollab Client Service**.
3. Click **Configure MiCollab Client Service**.
4. Click the **Enterprise** tab.
5. Enter your e-mail address in the Administrator e-mail field to allow the system to send you MiTeam Classic licensing notifications.
6. Under **MiTeam Classic Configuration Settings**, check the **MiTeam Classic Configuration** box. Access to MiTeam Classic is granted to all new and pre-existing premium users after you enable this check box in the Enterprise tab.
7. Click **Apply**.
8. Click **Show** to display the OrganizationID. The OrganizationID is an identifier for the company in the MiTeam Classic service provider. The Organization ID is used to facilitate services. Do not change the OrganizationID

CAUTION:
If you have already enabled MiTeam Classic on an Enterprise, and then you delete the Enterprise, recreating the Enterprise will not restore MiTeam Classic on that Enterprise.

Note:
If a failure occurs, collect the log files and diagnostics (sosreport<file>.tar.gz) from the server manager **View Log File** page for Product Support. To have an OrganizationID reset, you must contact Product Support.

CAUTION:
Perform a database backup after you enable MiTeam Classic. If you restore a backup that was taken before MiTeam Classic was enabled, you will be unable to re-enable MiTeam Classic. You will require Mitel Product Support to help you re-enable MiTeam Classic.

To give users MiTeam Classic functionality:

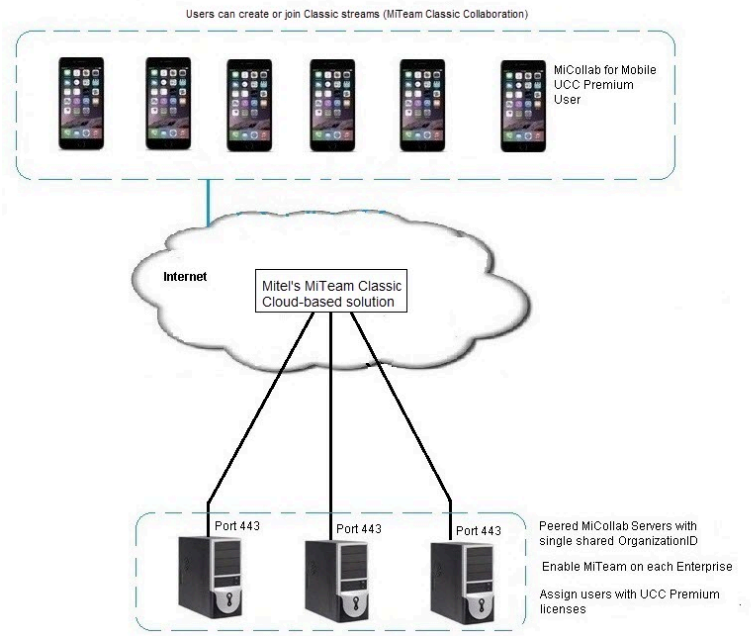
- assign MiVoice Business users with license bundles that provide UCC Premium licenses and MiVB Subscription Licenses
- assign MiVoice 5000, MiVoice MX-ONE, or MiVoice 400 users with Roles that provide UCC Premium licenses.

Enterprise Configuration - Peered

In a peered Enterprise solution, all peered Enterprises must have the same MiTeam Classic OrganizationID in order for all UCC Premium users with active MiTeam Classic license subscriptions to join

Classic streams. The following figure shows an example of a peered configuration with MiTeam Classic services:

Figure 6: MiTeam Classic – Peered Enterprise Configuration



Adding MiTeam Classic Services to a Peered Enterprise

1. After peering is set up, check the **MiTeam Classic Configuration** box on one of the peered Enterprises. Then, the MiCollab server copies the MiTeam Organization ID to the other peered Enterprises. Do not enable MiTeam Classic on the Enterprise servers until after they have been peered.
2. Enable the **MiTeam Classic Configuration** box on each of the other peered Enterprises. If MiTeam Classic configuration fails, a warning banner will be displayed in the MiCollab server manager. See Resolving Conflicting OrganizationIDs.
3. Perform a database backup.

Adding Peering between Existing Enterprises

Peering is unidirectional from server to server. To allow all Premium UCC users on a site to participate in all Classic streams, a fully meshed network of peered servers is recommended.

1. Check the **MiTeam Classic Configuration** box on one of the peered Enterprises only. The OrganizationID is then propagated to the other peered Enterprises.
2. Next, check the **MiTeam Classic Configuration** box on each of the other peered Enterprises.
3. When peering is being added, the Enterprises will compare their OrganizationIDs and if they are different then peering will fail to be configured. If the MiTeam Classic configuration fails, a warning banner will be displayed in the MiCollab server manager. See *Resolving Conflicting OrganizationIDs*.
4. Perform a database backup.

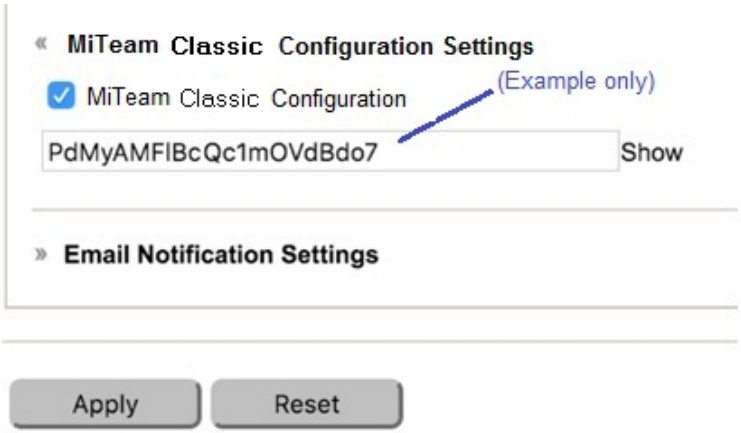
Resolving Conflicting OrganizationIDs

If Enterprises have different OrganizationIDs, you must choose one of the Organization IDs, copy it, and paste it into the field under the MiTeam Classic Configuration heading on each of the other Enterprises.

Caution: If you change an OrganizationID, existing users will lose their chats, Classic streams, and files that are associated with that OrganizationID.

1. Log into the server manager of the server that has the OrganizationID that you want to use for the site.
2. Under **Applications**, click **MiCollab Client Service**.
3. Click **Configure MiCollab Client Service**.
4. Click the **Enterprise** tab.
5. Under **MiTeam Classic Configuration**, click **Show** to display the OrganizationID.
6. Copy the OrganizationID value. The figure below shows an example:

Figure 7: OrganizationID Example



7. Log into the server manager of the server where the OrganizationID needs to be replaced.
8. Click **Show** to display the OrganizationID.
9. Replace it with the one copied from the above step and click **Apply**.
10. Replace the OrganizationID on any other Peered Enterprises.

14.3 Provision MiTeam Classic

To provision MiTeam Classic functionality, assign the user with a UCC Premium license through:

- MiCollab Users and Services
- Integrated Directory Services
- MiVoice 5000 Provisioning Manager, or
- MiVoice MX-ONE Provisioning Manager

Users must be assigned with a bundle or role that provides a UCC Premium license and must have an active Mitel Classic license subscription.

After you add users with UCC Premium licenses or upgrade users to UCC Premium licenses, MiTeam Classic functionality is supported on their clients. Users will need to restart their client to activate MiTeam Classic. Refer users to the *MiTeam Reference Guide* available on the Mitel Customer Documentation web site.

When you change a user's UCC Licensing bundle from Premium to another level (such as UCC Standard, Entry or Basic), MiTeam Classic is disabled for that user. If the bundle is changed back to Premium and the MiTeam Classic box is checked, MiTeam Classic service is restored and the user's content is still present.

Disable or Re-enable MiTeam Classic

By default, MiTeam is enabled for eligible users (see MiTeam Classic Licensing for details).

Note:
If there are no MiTeam Classic licenses available, you can assign a UCC Premium license bundle to the user but cannot enable **MiTeam Classic** option.

You can choose to disable a user's MiTeam Classic functionality to:

- pre-empt the automatic disabling and deleting of a user's MiTeam Classic account before the free period ends, or
- transfer a paid license from one user to another by disabling MiTeam Classic for one user and then enabling it for another.

To disable or re-enable MiTeam Classic from the MiCollab Users and Services application:

1. Under **Applications**, click **Users and Services**.
2. Display the user(s) in the directory.
3. Select the user and click **Edit**.
4. Click the **MiCollab Client** tab.
   - To disable **MiTeam Classic** deselect the box.
   - To enable **MITeam Classic** select the box. The MiTeam menu item is added to the user's Client.
5. Click **Save**.
   - If **MiTeam Classic** checkbox is deselected, the MiTeam menu item is removed from the user's Client.
   - If **MiTeam Classic** checkbox is selected, the MiTeam menu item is added to the user's Client.

Delegate Classic Streams

You can delegate Classic Streams from one MiTeam Classic user account to another MiTeam Classic user. Classic Streams delegation is also possible from a MiTeam Classic disabled user (but has Classic Streams) to another MiTeam Classic enabled user.

Note: All the Classic Streams will be delegated from one user to another user. You cannot select individual Classic Streams to delegate.

Conditions and Limitations

- The user from whom the Classic Streams are delegated has Classic Streams listed in the MiTeam menu in the Client.
- The cache for a MiTeam Classic user is refreshed automatically after every six hours. Any changes made to the user will get reflected after six hours. The server will be out-of-sync from Moxtra for these six hours. The cache can be refreshed manually by navigating to **Users and Services** > **Show All** menu.

To delegate Classic Streams:

1. Go to **MiCollab Server Manager**.
2. Under **Applications**, click **Users and Services**.
3. Select the user from whom the Streams are to be delegated.
4. Under **MiCollab Client**, click **Delegate Classic Streams**.
5. Select the **From** and **To** users from the dialog box, to delegate the Streams.

> **Note**:
> Enter the e-mail address of the user to delegate the Classic Streams.

6. Click **OK**.

All Classic Streams are delegated to the **To** user. The delegated Classic Streams are displayed in the Client main menu for the user.

Classic Streams Warning

If the user has Classic Streams in the Client, a warning widow is displayed when you:

- delete the user.
- disable the MiTeam Classic for the user.
- change the e-mail id of the user.
- change UCC license bundle from Premium to Entry or Standard.

Warning:

Deleting a user, removing MiTeam Classic for an user, or changing e-mail id of an user, will result in deletion of their Classic Streams in 30 days. To keep the Classic Streams, you must delegate them to another user within the 30 days window.

About MiTeam Meetings 15

This chapter contains the following sections:

- Provision MiTeam Meetings

MiTeam Meetings application is Mitel's Cloud-based collaboration tool (based on CloudLink infrastructure) that provides MiCollab users with the ability to initiate Mitel Meetings from their MiCollab Client.

- **Collaborate:**Manage collaboration meetings
- **Chat**: Hold chat sessions and receive chat notifications
- **File Sharing**: Store and share files
- **MiTeam Meeting:** Perform audio, video, and web sharing

All UCC bundle templates will be updated to have check-box field for **MiTeam Meetings.**

For information on MiTeam Meetings end-user features, see *MiCollab Client End-User Online Help*.

Supported Clients

MiTeam Meetings is supported with the following MiCollab Clients:

- MiCollab for PC Client
- MiCollab for Mac Client
- MiCollab Web Client
- MiCollab for Mobile Client (iOS/Android only)

Supported Communication Platforms

MiTeam Meetings is supported for single and multiple MiCollab server deployments on the following Mitel communication platforms:

MiVoice Business

MiVoice MX-ONE

MiVoice 5000

MiVoice Office 400

MiTeam Meetings is only supported in MiCollab Client Integrated Mode. It is not supported for MiCollab Client Co-located mode or on MiCollab Client stand-alone systems.

15.1 Provision MiTeam Meetings

Users must be assigned with a UCC bundle or role that provides a MiTeam Meetings license.

By default, MiTeam Meetings option is disabled for MiCollab users.

To enable or disable MiTeam Meetings for a new user

1. Under **Applications**, click **Users and Services**.
2. On the **Users** tab, click **Add** or **Quick Add** and Enter User Information.
3. Select a UCC bundle to apply the services and application licenses to the user.

Note:
Use Quick Add when you want to add a new user and override some of the template settings.

Note:
Make sure **MiTeam Meetings** is enabled in MiCollab Client Service option in the template.

4. Click **Save**.

A welcome e-mail is sent to the user with the MiTeam Meetings feature enabled status. Click on the link provided in the welcome e-mail to create a password for your MiTeam Meetings account.

To enable or disable MiTeam Meetings for an existing user

1. Under **Applications**, click **Users and Services**.
2. Display the user(s) in the directory.
3. Select the user and click **Edit**.
4. Click the **MiCollab Client** tab.

   - Enable the **MiTeam Meetings** checkbox to activate the MiTeam Meetings feature.
   - Disable the **MiTeam Meetings** checkbox to deactivate the MiTeam Meetings feature.
5. Click**Save**.

   - If **MiTeam Meetings** checkbox is enabled, the cross launch functionality from MiCollab Client to MiTeam Meetings application is enabled.
   - If **MiTeam Meetings** checkbox is disabled, the cross launch functionality from MiCollab Client to MiTeam Meetings application is disabled.

Note:
When **Disconnect CloudLink** operation is performed from MiCollab Settings, bulk request is sent to CloudLink to untag the users and thus disables the **MiTeam Meetings** application cross launch for the users.

Note:
If MiCollab is upgraded, the default and the existing UCC templates will have the new **MiTeam Meetings** checkbox in disabled state.

To enable MiTeam Meetings for users in bulk

The bulk user provisioning feature is applicable for all PBXs in integrated mode.

1. Under **Applications**, click **Users and Services**.
2. In the **Users and Services** page, select the **Bulk User Provisioning** tab.
3. From the Mode drop-down, select the **Bulk User Edit** option**.**
4. Select **Load User** button or from the **Tools** drop-down button select **Import from File** option .
5. Select users for whom the MiTeam Meetings should be enabled.
6. Once done, select the **Enable MiTeam Meeting** option.
7. A confirmation pop-up appears on the screen. Click **OK.**

In case of a failure, a pop-up appears on the screen, listing the error. To view each error report, click on the error icon. The failed list of users remains on this screen.

To verify the MiTeam Meetings feature enablement:

- Navigate to**Users and Services**and select a user. Click the**MiCollab Client**tab and verify if the**MiTeam Meeting**setting is checked.
- Log in to the MiCollab Client application, click on the **Meeting** menu. MiTeam Meetings application home page is opened.

Generate User Summary or MiTeam Classic Status Report

16

This chapter contains the following sections:

- Generate Report of MiCollab Client Accounts

The **Reports** button allows you to generate one of the following reports:

- User Summary Report
- MiTeam Classic Status Report
- MiTeam Meeting Status Report

User Summary Report

This report lists the following information for the MiCollab users:

- User's First Name
- User's Last Name
- Email Address
- UCC Bundle
- Department
- Location

Note:
Users who are assigned with Premium bundles are entitled to MiTeam capability.

MiTeam Classic Status Report

This reports provides the following information for MiTeam Classic users:

- User's First Name
- User's Last Name
- E-mail address
- MiTeam Classic status: Entitled Yes/No/Blank (Blank field indicates user has been deleted)
- Current Stage: Free or Grace
- Expiry date of free period.

By default, the report is sorted by expiry date.

MiTeam Meetings Status Report

This reports provides the following information for MiTeam Meeting users:

- User's First Name
- User's Last Name
- E-mail address
- MiTeam Meeting status - Enabled : Y/N
- Failure reason - Reason stated if any or else mentioned as N/A

Generating a Report

If the report information does not contain UTF-8 characters, you can use the following procedure:

1. In the User Directory, click the **User** tab.
2. Click **Reports** and select the desired report

   - **User Summary Report**
   - MiTeam Classic Status Report, or
   - MiTeam Meetings Status Report
3. If desired, sort the information.

If the report information contains UTF-8 characters, you must first save the report as a Notepad file and then open it in Excel in order for the UTF-8 characters to be displayed properly:

1. In the User Directory, click the **User** tab.
2. Click **Reports** and select the desired report:

   - **User Summary Report**
   - MiTeam Classic Status Report, or
   - MiTeam Meetings Status Report
3. Select **Open with Other . . .** and then select **Notepad**.
4. Click **OK**.
5. Save the CSV file to your PC.
6. Open it with Excel.
7. If desired, sort the information.

16.1 Generate Report of MiCollab Client Accounts

You can generate real-time reports of USP and MiCollab Client account information. The report can be generated when MiCollab is in either integrated or co-located mode.

To generate these reports, you need a basic knowledge of Linux commands.

USP Accounts Report

To generate this report:

1. Log into the MiCollab server console as "root" using the administrative password.
2. Enter the following command to access the directory that contains the required script:

   / usr/mas/bin/ db_report_helper_scripts
3. Run the report by entering following command: **java -jar UserAndServicesDump.jar > {filename}.csv**

   For example: **java -jar UserAndServicesDump.jar > {amtc_report}.csv**
4. Copy the file to your PC.
5. Open the file in a spreadsheet editor.

Note: The report may not display UTF-8 characters properly depending on the editor being used. For instance, Excel may not display UTF-8 characters properly. Other editors such as Sublime or Word may display them in readable format.

A sample report is shown below:

	B	C	D	E	F	G	H	I	J	K	L	M	N
1	firstname	lastname	loginid	email_address	department	location	phone	mailbox	uca	mca	uc_mobile	saa	tw
2	Berry	Smith	smithb	berry_smith@amtc.com	Sales	5B-34	18888	18888			18889		
3	Sally	Green	greens	sally_green@amtc.com	Sales	5A-23	18109	18109	TRUE	TRUE	18101		
4	Amir	Naidar	naidara	amir_naidar@amtc.com	Tech Support	3C-44	18222	18222	TRUE	TRUE			
5	Pierre	Julian	julianp	pierre_Julian@amtc.com	Purchasing	2D-33	18428	18428	TRUE	TRUE			
6	Jay	Cheng	chengj	jay_cheng@amtc.com	Sales	5F-22	18001	18001	TRUE	TRUE			18002
7	Will	MacDonald	macdonaldw	will_macdonald@amt.com	Tech Support	3D-33	18213	18213	TRUE	TRUE			18214

The USP report fields are described below:

Field	Description
index	Record number
firstname	First name for the account holder
lastname	Last name for the account holder
loginid	Login ID that the account holder will use to log in to the Desktop Client
email_address	E-mail address of account holder
department	Department of account holder
location	Location of account holder
phone	Extension number of account holder
mailbox	Voice mailbox extension of account holder
uca	TRUE: Service is enabled or {blank}: Service is disabled
mca	
saa	Speech Auto Attendant extension
tw	Teleworker extension of account holder

MiCollab Client Accounts Report

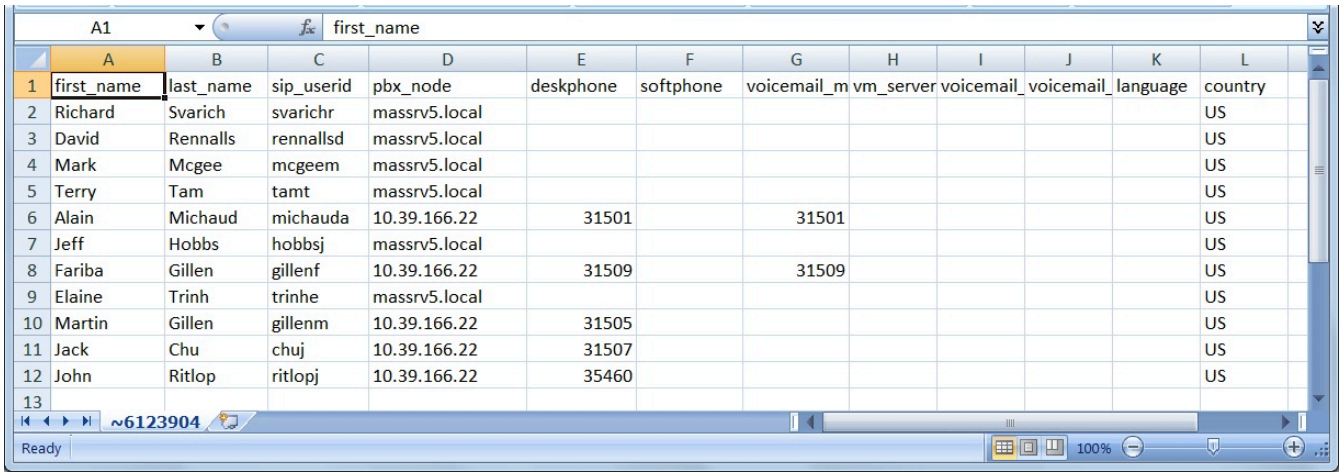
To generate this report:

1. Log into the MiCollab server console as "root" using the administrative password.
2. Enter the following command to access the directory that contains the required script:

   cd /usr/mas/bin/db_report_helper_scripts
3. Save the report to a file by entering following command: **sh ./dump_uca_account.sh > {full path and file name}**

   For example: **sh ./dump_uca_account.sh > /tmp/output.csv**
4. Copy the file to your PC.
5. Open the file in a spreadsheet editor.

Note: The report may not display UTF-8 characters properly depending on the editor being used. For instance, Excel may not display UTF-8 characters properly. Other editors such as Sublime or Word may display them in readable format.



A1 | first_name

	A	B	C	D	E	F	G	H	I	J	K	L
1	first_name	last_name	sip_userid	pbx_node	deskphone	softphone	voicemail_m	vm_server	voicemail_	voicemail_	language	country
2	Richard	Svarich	svarichr	massrv5.local								US
3	David	Rennalls	rennallsd	massrv5.local								US
4	Mark	Mcgee	mcgeem	massrv5.local								US
5	Terry	Tam	tamt	massrv5.local								US
6	Alain	Michaud	michauda	10.39.166.22	31501		31501					US
7	Jeff	Hobbs	hobbsj	massrv5.local								US
8	Fariba	Gillen	gillenf	10.39.166.22	31509		31509					US
9	Elaine	Trinh	trinhe	massrv5.local								US
10	Martin	Gillen	gillenm	10.39.166.22	31505							US
11	Jack	Chu	chuj	10.39.166.22	31507							US
12	John	Ritlop	ritlopj	10.39.166.22	35460							US
13												

~6123904

Ready 100%

The MiCollab Client report fields are described below:

Field	Description
first_name	First name for the account holder
last name	Last name for the account holder
login_id	Login ID that the account holder will use to log in to the Desktop Client
pbx_node	Password that the account holder will use to log in to the desktop client
desk_phone_extension	Extension for the account holder's desk phone
soft_phone_extension	Extension for the account holder's softphone
voice_mail_server	Voice mail server configured for the PBX node associ ated with this account

Field	Description
voice_mail_number	Voice mail extension for the account holder's PBX node
voice_mail_public_number	Extension for the account holder's mailbox extension
language	Language setting of user's account
country	Country setting for the account holder

Deploy Mobile Client for Mobile 17

This chapter contains the following sections:

- Deploy Mobile Client for EHDU
- Deploy MiCollab MAC or PC Client (without Softphone)

Before MiCollab Client can be deployed to users, you must first configure the MiCollab Client Deployment application. Refer to the *MiCollab Client Deployment* application online help for instructions. After you program a user with a MiCollab Client softphone (UC Endpoint) in the Users and Services application, the softphone is automatically deployed.

To re-deploy MiCollab Client for Mobile:

1. Under **Applications**, click **Users and Services**.
2. Click **Deploy MiCollab Client** and select **for all users**. This action selects all users that are eligible for MiCollab Client deployment.

   OR

   Click **Show All**, select the desired users from the directory list, click **Deploy MiCollab Client**, and select **for selected users**.
3. A confirmation dialog box appears. Click **Deploy**. If there is a failure to deploy a user, the server continues to deploy to the remaining users and a dialog box with an error summary is displayed after deployment has completed. Users are automatically sent a deployment e-mail. Users scan the QR code in the e-mail to complete deployment.

17.1 Deploy Mobile Client for EHDU

Before you can deploy MiCollab Client for External Hot Desk Users (EHDU) from the Users and Services application, you must first configure the MiCollab Client Deployment application. Refer to the *MiCollab Client Deployment* application online help for instructions.

For a MiCollab Client EHDU, the user requires a EHDU license and MiCollab Client service.

To deploy MiCollab Client for External Hot Desk Users:

1. Under **Configuration**, click **MiCollab Settings**.
2. Click the **MiCollab Client Deployment** tab.
3. Select the MiCollab Client deployment profile that you want applied to the External Hot Desk Users. By default, the deployment profile is set to "Do Not Deploy". Select the desired deployment profile and click **Save**, The users are not deployed at this stage.
4. Under **Applications**, click **Users and Services**.

5. Click **Deploy MiCollab Client** and select **for all users**. This action selects all users that are eligible for MiCollab Client deployment.

   OR

   Click **Show All**, select the desired users from the directory list, click **Deploy MiCollab Client**, and select **for selected users**.
6. A confirmation dialog box appears. Click **Deploy**. If there is a failure to deploy a user, the server continues to deploy to the remaining users and a dialog box with an error summary is displayed after deployment has completed. Users are automatically sent a deployment e-mail. Users scan the QR code in the e-mail to complete deployment of their EHDU devices. After the client logs in, the EHDU device is present in the dynamic statuses and the user can select the EHDU device to make outgoing office-link calls.

Note the following:

- To un-deploy a EHDU, clear the External Hot Desk box for the Hot Desk User or delete the device. The MiCollab Client does not log out if the EHDU is not deployed.
- If you change the device type to UC Endpoint, the deployment profile for this device is set to Default and the softphone is deployed.
- If you change device to an EHDU, the deployment profile is set to the selection made under MiCollab Settings.

17.2 Deploy MiCollab MAC or PC Client (without Softphone)

You can deploy a MiCollab MAC or PC Client without a softphone from the Users and Services application. Before you can deploy a MiCollab MAC or PC Client, you must first configure the MiCollab Client Deployment application. Refer to the *MiCollab Client Deployment* application online help for instructions.

To deploy:

1. Under **Applications**, click **Users and Services**.
2. Under the **Users** tab, select the user and click **Edit**.
3. Click the **MiCollab Client** tab.
4. Select the desired **Deployment Profile**. This field only applies to MiCollab MAC or PC Clients without softphones.
5. Click **Save**.
6. From the **Users and Services** page**,** click the **Users** tab.
7. Select the users and click **Deploy MiCollab Clients > for selected users**.

A confirmation dial box appears. Click **Deploy**. If there is a failure to deploy a user, the server continues to deploy the remaining users and a dialog box with an error summary is displayed after deployment is completed.

Users are automatically sent a deployment e-mail. The MiCollab MAC or PC Client are not associated with phones, so the extension in the e-mail is listed as "None". Users click on a link in the e-mail to complete deployment.

This setting can be chosen concurrently with one or more deployed devices. Devices are deployed separately using the selected deployment profile.

Correcting Errors 18

This chapter contains the following sections:

- Managing Detained and Failed IDS Operations
- Unable to Delete a User's Extension
- Unable to Add Phone After Deletion
- Pop-up Error in Chrome

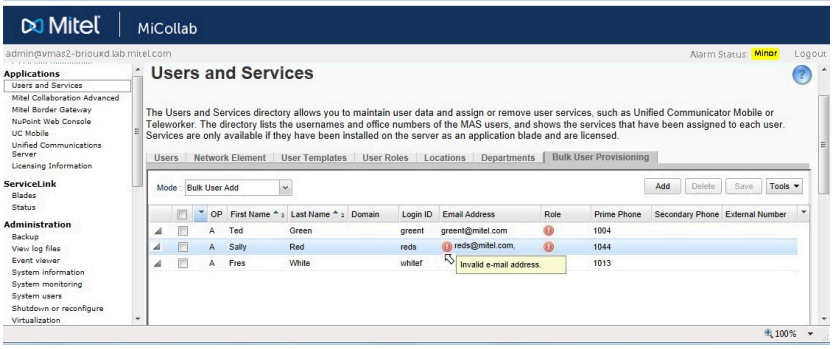
If errors occur during a bulk data import, they are listed in the Bulk Provisioning Tool screen and indicated by icons:

 indicates a field entry error. To display the error, hover your cursor over the icon. The error message provides the corrective action.

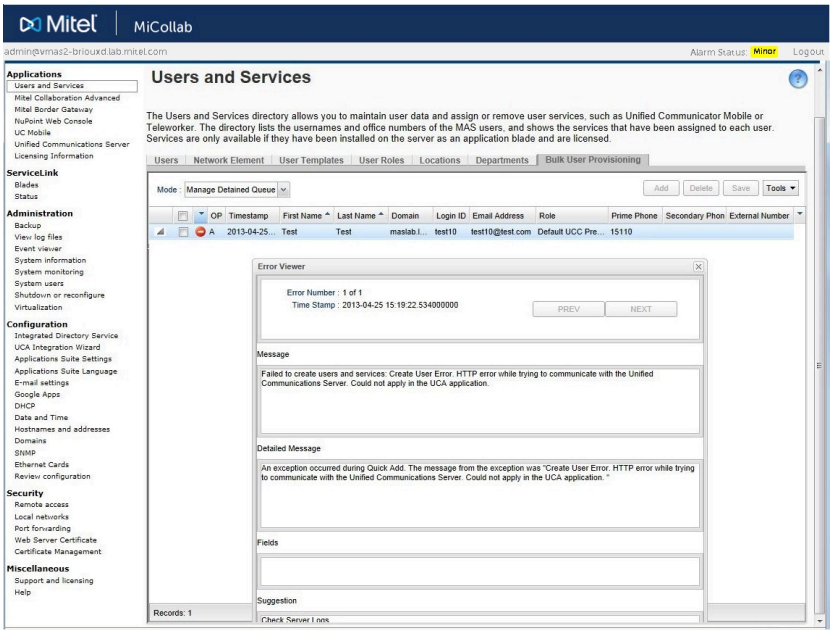
 indicates a data import failure. To display the error, click the icon for details. The error report provides the corrective action. If multiple errors exist against the update, click **Next**.

You can also click the icon next to an entry to review a detailed summary of any errors. You must resolve the errors before you can save an entry to the directory.

Example of a Field Entry Error



Example of a Data Import Error



18.1 Managing Detained and Failed IDS Operations

The *Manage Detained Queue* in the *Bulk User Provisioning* tool lists the detained and failed IDS operations:

- Detained IDS operations are operations that have been performed on the directory server that have not been applied to the USP database yet.
- Failed IDS operations are directory server updates that the MiCollab system could not apply to the USP database.

Failed IDS operations are also

- listed in the Event log in the MiCollab server manager
- indicated in the Manage IDS Connection page for the last successful sync (if errors were detected, the connection is highlighted in red).

The Manage Detained Queue lists a maximum of 2500 detained entries in the grid. Any additional detained entries beyond the 2500 limit are stored on the system. After you process detained entries, any additional detained entries are added to the grid when you reload the Manage Detained Queue view.

Note:
Data mismatches that occur between telephony fields are not sent to the Managed Detained Queue because they cannot be reconciled from MiCollab . The following telephony fields are ignored during a synchronization update: Role, Home Element, Mobile Phone Directory Number; Primary Phone Directory Number and Secondary Phone Directory Number.

Note:
When you create a new connection to the directory server, the 'detain always' option is enabled by default. Therefore, during a synchronization all users on the directory server (including Administrator and Guest accounts) are sent to the detained queue. You must remove or ignore the administrator or guest entries from the queue.

Managing IDS Operations

To manage detained and failed IDS operations:

1. Under **Applications,** click **Users and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the Mode field, select **Manage Detained Queue**.
4. Click **Tools**, then click **Reload Detained Queue** to refresh the grid with the latest detained entries from the directory server.
5. Review the list of **A** (Add), **U** (Update) and **D** (Delete) operations. Errors are identified by icons. Hover your cursor over the icons for a description of the error.

   For **U** (Update) operations, the field values that will be deleted or modified are indicated by strike though text; the new values appear in **bold** text; and any values that will not be changed appear in normal text. Hover your cursor over an update field to display any additional details.
6. Click
   
   next to an entry to review a detailed summary of the changes that will be applied to the database. If there are any errors associated with the record, a detailed summary of the error is provided. Click **Done**.
7. Correct any errors caused by invalid data.
8. Select any operations that you do not want applied to the database and click **Delete**. Click **OK** to confirm the deletion of the operation from the grid.
9. Select the operations that you want to apply to the database and click **Save**. The Operation Progress window opens and displays the import progress. After the import is complete, the Operation Progress window closes.
10. Perform another IDS sync and check the Manage Detained Queue again to see that the errors are indeed fixed and do not reappear.

Emptying the Detained Queue

You can remove all entries from the Detained Queue quickly using the **Empty Detained Queue** menu option.

To remove all detained entries from queue at once:

1. Under **Applications,** click **Users and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the Mode field, select **Manage Detained Queue**.

4. Click **Tools**, then click **Empty Detained Queue**.

> **Note**:
> If you empty the queue, the entries are removed permanently. You cannot recover them.

5. Click **OK** to proceed. The list is emptied.

18.2 Unable to Delete a User's Extension

Symptom: You are unable to delete a user's extension.

Sample Error Message: "Failed to delete DN: 20004 (FourTwo,FourTwo) on ICP: Tenant04 (10.40.190.29). (ICP Error: Cannot delete phone service 20004 because it is configured as the primary phone service for FourTwo FourTwo. Users with multiple phones must have their primary phone changed from 20004 before the delete is possible.) The approximate system time on the ICP is: 19:03:28 on 2014/Mar/07." .

Cause: You cannot delete the primary phone service from a user who has multiple phones. One of the phones, must be assigned as the primary phone.

Corrective Action: Log into the MiVoice Business system administration tool and change the primary phone to one of the user's other extensions. Then delete the extension.

18.3 Unable to Add Phone After Deletion

Symptom: After you delete a phone (for example, extension 1000) from a user, you are unable to add the phone back into the system using the same extension number.

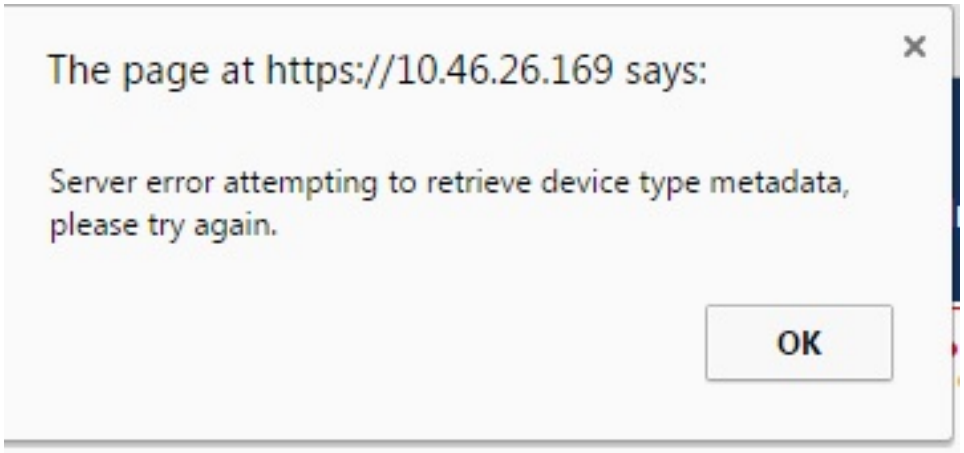
Cause: The phone extension is currently programmed as a member in the Personal Ring Group of another user (for example, extension 1001).

Corrective Action: Delete the phone (extension 1000) from the MiCollab Client Accounts tab of the other user (extension 1001)

1. Under **Applications**, click **MiCollab Client Service**.
2. Click **Configure MiCollab Client Service**.
3. Click **Accounts**.
4. Click the account of the user with the PRG (extension 1001).
5. Under **Phone Numbers** delete the phone (extension 1000).
6. You can now add the phone extension 1000 back into the system through USP. Note that on the next MiCollab Client PBX sync, the phone (extension 1000) will be added back into the PRG of the other user (extension 1001).

18.4 Pop-up Error in Chrome

Symptom: While editing a user's phone in the Users and Services application, you receive an error dialog similar to the following:



Cause: Issue with Chrome browser.

Corrective Action: Click **OK** to proceed. Use another browser (for example FireFox) or upgrade to Chrome 46.0.2490.33 beta-m.

MiCollab Audio, Web and Video Conferencing Introduction

19

This chapter contains the following sections:

- What's New in this Release
- VMware View

Formerly known as Mitel® Collaboration Advanced (MCA), MiCollab Audio, Web and Video Conferencing provides an integrated application to create audio and Web conferences using corporate directories and personal address books from Microsoft® Outlook® and Lotus Notes®. MiCollab Audio, Web and Video Conferencing is packaged on the MiCollab server, (formerly known as Mitel® Applications Suite (MAS)) which is linked by an Ethernet connection to the IP network. A link on the MiCollab server provides access to a Web-based administrator interface for configuring MiCollab Audio, Web and Video Conferencing, scheduling conferences, viewing conference calls, and administering collaboration controls. You can access all interfaces through either HTTP or HTTPS.

Authorization and authentication allows only valid users to access the services. To meet the highest security requirements, MiCollab Audio, Web and Video Conferencing uses Secure Sockets Layer (SSL) encryption for secured messages, server-side digital certificates, and Comprehensive Lightweight Application Security (CAST) 128-bit encryption for data transmission during Web conferences.

MiCollab Audio, Web and Video Conferencing provides:

- Instant, flexible calling: Initiate an instantaneous call or to create a conference call from a two-party call. A conference call can also be pre-scheduled.
- Complete call control and management: Add and drop other call participants as well as mute, hold, or transfer the call directly from the desktop. A call detail record (CDR) provides a log of all calls. The CDR includes the dates and times of all calls call duration of all calls for billing purposes.
- Cost-effective conferencing: Delivers the most cost-effective group calling, with ultimate flexibility to customize solutions to best meet individual needs.
- Web-based collaboration tools: Facilitate online meetings, training, and presentations with features designed for sharing your desktop or individual applications. Enhance conferences to increase participation and understanding by using interactive markup tools, user polling, and video-conferencing. Use the file transfer utility to immediately share the outcome of online collaborative sessions by transmitting updated files and presentations to conference participants.
- Conference archiving: Create recordings of conference calls and collaborative sessions for playback later.

Refer to Setting up a conference for information about conference settings configured by the user.

A single logon to the Web interface as the MiCollab Audio, Web and Video Conferencing administrator allows you to navigate and access all the MiCollab Audio, Web and Video Conferencing options. Select from the options listed under Configuration, Provisioning, Monitoring or Reporting in the pane on the left side of the MiCollab Audio, Web and Video Conferencing administration page to display the specific item.

Hardware, software, network, and communication platform specifications and requirements for MiCollab Audio, Web and Video Conferencing are defined in accordance with MiCollab Server specifications. Because MiCollab Audio, Web and Video Conferencing must be installed on a MiCollab Server (v5.0 or later), hardware requirements for the server are determined by MiCollab requirements.

MiCollab Audio, Web and Video Conferencing hardware requirements for single and multi-application configurations are the same. For detailed hardware requirements information, refer to the *MiCollab Engineering Guidelines* on the Mitel Document Center Web site.

See the New Features, Enhancements, and Changes topic to see what is new for this release of MiCollab Audio, Web and Video Conferencing .

This help system provides information about the MiCollab Audio, Web and Video Conferencing Administrator interface, which is used to configure MiCollab Audio, Web and Video Conferencing. For initial set up, program the following sections before you configure the rest of MiCollab Audio, Web and Video Conferencing :

- Configure Web Conferencing Settings
- Configure System Options
- Configure SIP Server for the appropriate platform:
    - MiVoice Business
    - MiVoice Office 250
    - MiVoice 5000 or MX-ONE
    - MiVoice Office 400

After completing these areas, configure the remainder of the MiCollab Audio, Web and Video Conferencing in any order you choose.

For additional information, refer to the *MiCollab Audio, Web and Video Conferencing Configuration and Maintenance Manual* located on the Mitel Web site. The file is in PDF format. An Adobe® Acrobat® Reader is required to view the PDF file.

19.1 What's New in this Release

For a list of new functionality, see What's New in This Release on the Mitel Customer Documentation site.

19.2 VMware View

The following MiCollab Audio, Web and Video Conferencing user interfaces can be presented by VMware View:

- UI presentation, including MiCollab Audio, Web and Video Conferencing Web Portal and streaming video (receive only) through the MiCollab Audio, Web and Video Conferencing Collaboration Client application running in the virtual desktop. All Web-based conferencing and collaboration features are fully supported. Collaboration Client application and screen sharing features are fully supported.

Note:
See *Virtual Appliance Deployment Guide* at Mitel Document Center for description, requirements and configuration information specific to virtualization environment.

Configuration Guidelines for Secure Conferencing 20

This chapter contains the following sections:

- Web Conferencing Settings
- Port Reservation Settings
- System Options
- LDAP Configuration
- Voice Prompts
- Country Tone Plan
- Music-On-Hold Settings
- Licensing
- User Interface Wizard
- Edit DAS Rules
- Google Apps Integration for MiCollab Audio, Web and Video Conferencing
- Google Gadget Configuration

To minimize the risk of toll fraud and unauthorized access to information via Audio, Web and Video conferences, perform the following configuration:

1. Ensure that users publish password-protected conferences:
   - Click **System Options**.
   - Ensure that **Allow users to publish conference only with password** is enabled.
2. Unpublish all Conferences that have been published without passwords:
   - Under **Monitoring**, click **Manage Published Data**.
   - In the "Conferences Published without a Password" table, click **Unpublish All**. This action removes public access to the conferences, documents, and recordings.
3. Enable the **Leader Required** option for all conferences. After this option is set, a leader must be present even for one-time and recurring conferences. This requirement is applied to all users for all previously scheduled conferences and new conferences.
   - Under **Provisioning**, click **Default User Settings**.
     a. Under **Conference Settings** dropdown menu, select **Reservationless calls allowed, leader required**.
     b. Click **Save** and then click **OK**.
     c. Click **Restore all Users to Defaults**.

4. Disable the ability to dial out at the server level:

   a. Clear the **Dial out allowed** box to disable this functionality. Note that this prevents dialing out to clients including the AWV PC client, dialing out from the Conference Join page, and dialing out to the UC360.
   b. Click **Save** and then click **OK**.
   c. Click **Restore all Users to Default**
5. On the PBX, apply a Class of Restriction (COR) on the AWV extensions that disallows international calls (if acceptable).

In addition, to the above settings, instruct users to apply the following parameters when setting up conferences:

1. Require approval for conference access:

   a. Log into MiCollab End User Portal.
   b. Click **Audio, Web and Video Conferencing**.
   c. Click **Set up A Conference**.
   d. Select a type of conference.
   e. Under **Call Features**, **Personal ID** check the **Conference access requires approval** box.
   f. Click **OK**. Users will need to enter a Personal ID to join the conference. A non-user can generate a guest id. The system then sends an e-mail to the conference owner, which the owner must approve before the user can join. The Leader can also approve users from his or her portal from the Approval tab in the conference. This setting restricts access to the join flow page which supports dialing out.
2. Set a password at conference level:

   - Under **Password Protection** assign a Conference password. Users must enter the password to join the conference and to gain access to the join flow page which supports dialing out.

20.1 Web Conferencing Settings

To configure Web Conferencing:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Web Conferencing Settings** in the navigation pane.
2. Edit or view the settings on this page.

Setting	Description
Internal Port	The port that internal (local network) attendees con nect to for Web Conferencing. The local network must allow access to this port for internal users. Port 4443 is the default internal port. Setting the internal port to port 443 is not recommended.
External Port	The port that external attendees connect to when joi ning a Web conference. Port 443 is recommended b ecause it is a common port open on firewalls.

Setting	Description
	In case of single public IP, set the external port same as internal port. Port 4443 is recommended and it must be opened on firewall. For more information to migrate to single public IP, see "Appendix B" in the *MiCollab Engineering Guidelines* available on the Mitel Web site.
Web Conferencing Name	The additional hostname designated for the Web Conferencing server. The hostname must resolve to a public IP address that is externally accessible. The internal DNS must resolve the hostname to the local IP address of MiCollab Audio, Web and Video Conferencing. For more information, refer to "Firewall and DNS Server Configuration" in the *MiCollab Engineering Guidelines* available on the Mitel Web site. **NOTE:** In case of single public IP, additional hostname for the Web Conferencing server is not required. Set the Web Conferencing name to MiCollab server hostname.
Domain Name	Configured on the MiCollab server, the Domain Name cannot be edited through the MiCollab Audio, Web and Video Conferencing interface. This is the URL or IP address for users to access the Web page of the MiCollab Audio, Web and Video Conferencing inter face. The name must be accessible to everyone who will be invited to attend a Web conference, both inside and outside of your local network.

3. Click **Save**, and then click **Ok** at the prompt.

20.2 Port Reservation Settings

The Port Reservations feature allows you to monitor and manage port usage for conferences. The Port Reservations Report provides conference related information on MiCollab Audio, Web and Video Conferencing for the date and time range selected when Port Reservation Settings are configured.

To preserve ports on the server for one-time and recurring conferences, Mitel recommends that you do the following if you select **Enable Port Reservations**:

- Make sure the **Allow user to schedule conference if conflict occurs** option (below) is not selected.
- Select **Reservationless Calls Not Allowed** under the **Conference Settings** option under Default User Settings.

Note:
Do not enable Port Reservations if MiTeam, MiCollab Microsoft Outlook Plugin, or Ad-hoc Meeting is required. When the **Enable Port Reservations** option is enabled, MiTeam users are unable to join a stream and users will be unable to create a conference with the MiCollab Microsoft Outlook Plugin.

To configure port reservation settings:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Port Reservation Settings** in the navigation pane.
2. Configure the following options:

- **Enable Port Reservations**: When you select the Enable Port Reservations option, the MiCollab Audio, Web and Video Conferencing server tracks how many audio and web conferencing ports are scheduled for use at any given date and time. Note the following for the Enable Port Reservations option:

  - When you select Enable Port Reservations:

    - All prior scheduled conferences are set to 0 (zero) ports available. All currently scheduled conferences must be modified to reserve conference ports.
    - Mitel recommends that you select “Reservationless Calls Not Allowed” under Default User Settings to preserve ports on the server for one-time and recurring conferences.
    - The “To listen to this recording using your telephone” area on the Recording page is hidden and is not available to the user. This prevents ports from being used that may conflict with ports reserved for scheduled conferences.

    Note:
    Audio (Listen only and 2-way audio) need a audio port and **Web Share** needs a web port to start sharing.

  - When you do not select Enable Port Reservations, the “Conference Size” field on the One-time, Recurring, and Reservationless Conference Web pages is hidden. The conference size is not relevant when the server does not track port resources.

Note:
To preserve ports on the server for one-time and recurring conferences, Mitel recommends that you do the following when you select Enable Port Reservations:

- Make sure the **Allow user to schedule conference if conflict occurs** option is not selected.

- Select **Reservationless Calls Not Allowed** under the **Conference Settings** option under Default User Settings.

- **Allow user to schedule conference if conflict occurs**: If the “Enable Port Reservations” is selected, selecting the “Allow user to schedule conference if conflict occurs” option allows users to schedule a meeting even if the total number of attendees exceeds the number of licensed ports available. When the number of ports is exceeded, the user is prompted that not all attendees for the meeting may get in the conference if they choose to schedule it for that specific date and time. However, the user will still be allowed to schedule the conference.
- **E-mail administrator on scheduling conflicts**: If the “Allow user to schedule conference if conflict occurs” option is selected, selecting the “E-mail administrator on scheduling conflict” option provides the MiCollab Audio, Web and Video Conferencing administrator with an e-mail message any time a user chooses to schedule a conference after they are warned about potential port licensing conflicts.

3. Click **Save**, and then click **Ok** at the prompt.

20.3 System Options

To configure system options:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Options** in the navigation pane.
2. Edit or view the settings on the page.

Note:
When Enable DAS Rules is set, type only digits 1 through 9, 0 and the ”+” or ”-” characters. Do not use special characters or spaces. For example: +1-480-961-1234 or +1-4809611234 You can also use 4809611234 and the software will format it to +1-480-961-1234.

When Enable DAS Rules is ***not*** set, the format for this box is free-form, special characters and spaces are allowed. When free-form format is applied, what is typed in the Dial-In Phone Number boxes appears "as is" in the user Web interface and e-mail invitations.

Note:
The MiCollab Audio, Web and Video Conferencing media server does not support SRTP.

For MiVoice MX-ONE integrations:

When MiVoice MX-ONE is selected as the platform, the following fields are disabled:

- International Dialing Prefix
- Country Code
- Outgoing Prefix
- Enable DAS Rules
- National Dialing Prefix
- Max Extension Length

When joining a conference, end users must provide an outdial number including all outgoing dial codes, including national, international, and outside line dial. As the MiCollab Audio, Web and Video Conferencing administrator, you may be required to provide this information to end users.

Option	Description
Dial-In Phone Number 1	Type the first telephone number assigned to MiCollab Audio, Web and Video Conferencing that users dial to join conferences. This is typically a Direct Inward Dialing (DID) telephone number, but it can be any number used to dial into a conference. This value is included in the "Dial-In numbers" section of the Meeting Details displayed by the MiCollab Audio, Web and Video Conferencing Clients and included in the default contents of the Conference invitation. **Note**: E.164 number formatting is not supported.
Dial-In Phone Number 1 Label	Type the label associated with the first telephone n umber. This label is included in the "Dial-In numbers" section of the Meeting Details displayed by the MiCol lab Audio, Web and Video Conferencing Clients

Option	Description
Dial-In Phone Number 2	Type the second telephone number assigned to MiCollab Audio, Web and Video Conferencing that users dial to join conferences. This is typically a toll-free telephone number, but it can be any number used to dial into a conference. This value is included in the "Dial-In numbers" section of the Meeting Details displayed by the MiCollab Audio, Web and Video Conferencing Clients and included in the default contents of the Conference invitation. **Note**: E.164 number formatting is not supported.
Dial-In Phone Number 2 Label	Type the label associated with the second telephone number. This label is included in the "Dial-In numbers" section of the Meeting Details displayed by the MiCollab Audio, Web and Video Conferencing Clients.
Dial-In Phone Number 3	Type the third telephone number assigned to MiCollab Audio, Web and Video Conferencing that users dial to join conferences. This is typically an extension or hunt group number, but it can be any number used to dial into a conference. This value is included in the "Dial-In numbers" section of the Meeting Details displayed by the MiCollab Audio, Web and Video Conferencing Clients and included in the default contents of the Conference invitation. **Note**: E.164 number formatting is not supported.
Dial-In Phone Number 3 Label	Type the label associated with the third telephone number. This label is included in the "Dial-In numbers" section of the Meeting Details displayed by the MiCollab Audio, Web and Video Conferencing Clients.

Option	Description
International Dialing Prefix	Type the digits used before dialing international calls (for example, 011). This is based on the site where the MiCollab Audio, Web and Video Conferencing s erver is located.
National Dialing Prefix	Type the digits required to make domestic toll calls.
Country Code	Type the country code of the location where MiCollab Audio, Web and Video Conferencing is located. The d efault is 1 (for United States).
Webserver Administrator Email	Type the e-mail address of the MiCollab Audio, Web a nd Video Conferencing administrator. Web server aler ts are sent to this address.
Outgoing Prefix	Type the number used by the communications platform (switch) to seize a CO trunk for outgoing calls. This prefix is pre-pended to the digits when the number dialed by a user is greater than the Max Extension Length. When Enable DAS Rules is set this setting is not applicable.
Max Extension Length	Type the maximum number of digits MiCollab Audio, Web and Video Conferencing should use to determine an extension. If the number dialed is more than the maximum length, MiCollab Audio, Web and Video Conferencing sees it is an external call and appends it to the Outgoing Prefix. When Enable DAS Rules is set this setting is not applicable.
Enable DAS Rules	Set this option if DAS rules apply to MiCollab Audio, Web and Video Conferencing ; the DAS Rules option shows in the navigation pane.
Active Speaker Indication	Set this option to allow the audio conference leader to view the current speaker in the conference. When set in System Options, the leader can set or clear this fea ture for each audio conference. The default for this opt ion is set.
General Alarm E-mail	Type the e-mail address of the person who gets notif ied of general alarms (typically the system administrato r).
General Alert E-mail	Type the e-mail address of the person who gets notif ied of general alerts (typically the system administrato r).
Port Usage Notification Threshold	Type the number of concurrent ports being used on th e server, so that when this value is reached, an alert e -mail is sent to the e-mail address specified in the Alert Email field when the threshold is reached.

Option	Description
Executive Ports	Type the number of audio ports on the system you want to reserve for the exclusive use of conferences created by executive users. If the number of Executive Ports is non-zero, when someone joins a conference created by a non-executive user, the **number of ports available is decreased by the number of Executive Ports**. Refer to "Managing a User Profile" for information on how to configure a user to be an executive user. **Note**: Executive port settings are disregarded when Port Reservations are enabled.
Prompts Language	Select from the list the language that is used for the audio voice prompts. Custom Language 1 and Custom Language 2 are used for selecting a language other than those provided in the prompts list, which are uploaded from the Voice Prompts page.
Conference URLs	Select whether conference URLs will be protected (encrypted) by SSL (https) or not protected (http). If you select https, be sure that port 443 is open on any firewall placed between the server and the Internet.
Document Timeout	Type the length of time that uploaded documents will remain on the server after a call has expired. The server periodically deletes documents that are on the server past this time-out period.
User Login Timeout	Type the period of time of user inactivity before a browser session with the server is automatically terminated. Because a session may remain open during a conference call, and because that session may be used for call control at some point well after that call has started, this should be set long enough so that users will not be logged out during a call. It should be set short enough so that an open session does not constitute a potential security issue. The default is 8 hours.
Custom Access Codes Allowed	Select this option to enable custom access codes to be created when setting up conferences.

Option	Description
Use HTTPS Only	Select this option to force a secure connection for users that access the conference. This setting overrides the Conference URLs setting. **Note**: You must set Use HTTPS Only for MiCollab Audio, Web and Video Conferencing hyperlinks to work when MiCollab is configured in LAN mode with a MiVoice Border Gateway (MBG) Web Proxy. For more information about the MBG Web Proxy, refer to the MiCollab documentation available on the Mitel Web site.
Platform	Select the communication system platform being used with this installation of MiCollab Audio, Web and Video Conferencing .
Dial 1 to join outbound calls	When selected, a user added to the conference call is prompted by the system to press 1 to join the conferen ce. The user must respond correctly within the speci fied time or the system drops the outgoing call attempt.
G.729 Port Limit	Audio Compression port limit valid values are 0-100 (default is 100). Uncompressed audio ports will be used once the maximum has been reached. A value of 0 indicates G.729 audio compression ports are disabled. **Note**: 2-way Client Audio feature introduced in MiCollab Audio, Web and Video Conferencing 5.0 will only use G.711 voice encoding ports (it will not use G.729 ports).
Prompt for Access Code First	When selected the Access Code will be required befor e the Personal ID when accessing the Audio portion o f a conference.

Option	Description
DTMF Payload Type	Set the DTMF Payload Type to be used by MiCollab Audio, Web and Video Conferencing server. Default values are: • 101 for MiVoice Business , MiVoice 5000 and MiVoice MX-ONE • 96 for MiVoice Office 250 The range is 96-127.
Allow HD Video Resolutions	**OFF** by default. Clients will not be presented with the ability to select HD resolutions. **ON**: This will enable HD resolutions for all clients in all conferences. Client PC profiling will still occur, however this must be enabled before any client can select HD resolution.
Email Admin informing when the AWV disk space utilized reaches % of XX GB	This option allows the administrator to be notified by email when the MiCollab Audio, Web and Video Conferencing server disk space reaches xx% utilization. This option is checked (enabled) by default with a value of 80%. The administrator also has the option of disabling this option. **Note**: The disk space allocated to the MiCollab Audio, Web and Video Conferencing conference recordings and documents is 40% of the total available disk space on the MiCollab / MiCollab Audio, Web and Video Conferencing server. The 40% of the entire disk space is determined when the page loads. For example, on a system with 100GB disk space, the option will read "Email Admin informing when the MiCollab Audio, Web and Video Conferencing disk space utilized reaches _____ % of the 40GB alloted to recordings and documents".

Option	Description
Auto Disconnect in	When selected, all participants on the conference call are disconnected from the call after the leader has left the conference. The options are 1 minute, 5 minutes, and 10 minutes after the leader leaves the call.
Prompt to extend conference <x> minutes prior to its end time	When selected, the End of Conference Prompting (EOCP) minutes box becomes active. The value sele cted in this box determines the number of minutes pr ior to the end of a conference that the user receives a prompt to extend the conference or it will end at the sc heduled time.
Allow users to publish conference only with password	When enabled, this setting requires users to assign password protection to published conferences. By default, this option is enabled. Caution: When a password is not set for a published conference, the conference and any documents or recording associated with the conference are vulnerable to unauthorized access. Note that the following behaviors apply: • This setting applies to all types of Audio, Web and Video published conferences. • If you disable this setting, users will not be required to assign password protection to published conferences. In addition, users can remove password protection from any of their existing published conferences. • After you disable this setting, the user interface does not warn users of the risks associated with publishing unprotected conferences. • If you disable and then enable this setting, any conferences that were published without a password remain unprotected. However, if the user subsequently saves changes to an unprotected conference, the user will then be required to assign a password. • You can remove conferences that have been published without a password from the public domain. Under **Monitoring**, click **Manage Published Data** and then click **Unpublish All**.

Option	Description
Allow users to record audio-only conferences	When enabled, the users will have an option to record audio-only conferences from the end-user portal. By default, this option is enabled.

3. Click **Save**, and then click **Ok** at the prompt.

20.4 LDAP Configuration

LDAP Authentication is enabled when a user attempts to log on to the MiCollab Audio, Web and Video Conferencing server, a Lightweight Directory Access Protocol (LDAP) query authenticates that user. Rather than querying its own internal database to see if the username and password are authorized, an LDAP query is launched against the corporate directory. If the response indicates the username/password combination is legitimate, the server allows that user to access the system for scheduling and placing calls. Under this arrangement, the user's password is not stored on the server, and you do not need to administer the user database on the server (except to change some enhanced service features for users).

The server also uses the LDAP query process to enable auto-provisioning. If the LDAP query indicates the username and password are legitimate but the username has not yet been identified as a user on the server, then the server automatically establishes an account for that user. The user is set up with the default level of authorization to use the system's special features and is able to start using the system immediately. You set these user defaults when the system is initially configured (see Default User Settings).

If a user requires authorizations that differ from the system defaults, you can use the administrator Web client to change that user's profile. See Managing a User Profile.

Note:
To use LDAP authentication with Active Directory, you must have Active Directory set up prior to configuring MiCollab Audio, Web and Video Conferencing. Contact the site administrator to view the Active Directory configuration, and then verify the following.

An Active Directory user exists that is used as the LDAP Admin ID. The user does not need any special rights or permissions.

Users with name, password, and e-mail information exist as Active Directory users.

You can ping the MiCollab Audio, Web and Video Conferencing server by hostname from the Active Directory server.

The most common LDAP authentication uses an Active Directory database. Click to view the instructions for configuring an Active Directory database.

To use LDAP authentication with Active Directory, you must have Active Directory set up prior to configuring the MiCollab Audio, Web and Video Conferencing server. Contact the site administrator to view the Active Directory configuration and verify the following.

- An Active Directory user exists that can be used as the LDAP Administrator ID. The user does not need any special rights or permissions.
- Users with name, password, and e-mail information exist as Active Directory users.
- You can ping the MiCollab Audio, Web and Video Conferencing server by hostname from the Active Directory server.

To configure LDAP authentication with Active Directory:

1. To use an LDAP server to store the user database, select **Use LDAP**.
2. Type the server name where Active Directory resides in the **LDAP Server Name** box.
3. Leave the **LDAP Port No.** at the default (389). However, for installations with a large Active Directory database or if there is a need to authenticate users from multiple/nested organizational units (OU) or containers (CN), you may need to change this setting to the global catalog port number (3268).
4. Type the LDAP Search Base information in the box using the format:

   CN=<userdirectory>,DC=<domain>,DC=<com>

   Note:
   Entered text must be lower case except for DC, OU, CN, which must be upper case. Using upper case letters for anything else may cause the LDAP integration to fail. *If not using the standard Users folder*, use OU instead of CN for the folder names. *If OUs are in sub-folders*, list them in reverse order separated by commas. *If authenticating users from multiple/nested OUs or CNs*, LDAP Search Base must be a folder that is a parent of all OUs or CNs in which users exist. For example, specify the top domain level as LDAP Search Base: DC=<domain>,DC=<com>.

5. Type the LDAP Administrator ID information in the box using the format:

   CN=<active directory administrator ID>,CN=<userdirectory>,DC=<domain>,DC=<com>

Note:
Entered text must be lower case except for DC, OU, CN, which must be upper case. Using upper case letters for anything else may cause the LDAP integration to fail. *If not using the standard Users folder*, use OU rather than CN for the folder names. *If OUs are in sub-folders*, list them in reverse order separated by commas.

When entering the information, the first entry for CN must be the CN name of the user account that is the administrator ID, not the username or the display name. The username, display name, and CN names are typically the same however, it is possible that they could be different.

6. Type the active directory administrator's password in the **LDAP Administrator ID Password** box.
7. Type sAMAccountName in the **LDAP UID** box.
8. Type the e-mail domain as <*yourdomain.com*> in the **Email domain** box.
9. Select **Auto synchronize** and leave Sync interval at **5** (minutes).
10. Click **Submit**, and then click **Ok** at the prompt.

To enter or edit LDAP authentication and auto-provisioning:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **LDAP Configuration** in the navigation pane.
2. Select **Use LDAP** if you use an LDAP server to store the user database. Otherwise, leave this option cleared and the user database is stored on the MiCollab Audio, Web and Video Conferencing server.

Note:
When Use LDAP is set, Add User and Bulk Provision Users are ***not*** available in the MiCollab Audio, Web and Video Conferencing navigation pane.

When Use LDAP is cleared, the user database is stored on the MiCollab Audio, Web and Video Conferencing server and the settings on this page do ***not*** affect authentication.

3. If you select **Use LDAP** (in step 2), enter or edit the following LDAP server configuration options.

   - LDAP Server Name
   - LDAP Port No.
   - LDAP Search Base
   - LDAP Administrator ID
   - LDAP Administrator ID Password
   - LDAP UID Field
   - E-mail Domain
   - Auto synchronize
   - Sync interval (in minutes)

4. Click **Submit**, and then click **Ok** at the prompt.

To verify LDAP authentication is functioning:

1. Log on using the username (not the e-mail address) of a user listed in the Active Directory, along with their Active Directory password. The MiCollab Audio, Web and Video Conferencing server checks the Active Directory for authentication and allows the user to log on.

Note:
The name and password are sent as plain text and present a possible security risk.

2. After the user has logged on, they are automatically added to a list of users that can be viewed and administered through the MiCollab Audio, Web and Video Conferencing admin Web client.

20.5 Voice Prompts

MiCollab Audio, Web and Video Conferencing includes the voice prompts that are played for audio conferences. The audio prompts are available in multiple languages and the default prompt language is determined by the MiCollab Language set on the server. MiCollab Audio, Web and Video Conferencing also allows you to upload custom voice prompts and substitute those prompts or upload an entire set of custom language prompts, which are played instead of the existing prompts. The individual files are listed and include a brief description of the voice prompt, which helps you identify the file to change. For the complete list of the voice prompts, refer to the *MiCollab Installation and Maintenance Manual*. Click here for more information about recording custom prompts.

Note:
After uploading custom prompts, you must restart MiCollab Audio, Web and Video Conferencing before new prompts are played for a conference.

To upload a custom voice prompt file:

Note:
When replacing multiple prompts you can save all of them to a .zip file that you can upload to MiCollab Audio, Web and Video Conferencing as a batch file. When selected, the batch mode process unzips the file, and then replaces the corresponding prompt files for the language selected. However, if any file is not named correctly, the same as the file it is replacing, it is ignored during the upload and the existing prompt is played. Mitel recommends that you verify the file names before uploading them to MiCollab Audio, Web and Video Conferencing.

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Voice Prompts** in the navigation pane.
2. Select a language from the Prompts Language list.
3. Select **File** for the Mode.
4. Select the prompt from the **Voice Prompt File** list that you want to change.

Note:
The file name must match the existing file it is replacing. For example, the ”Welcome” prompt file name is 01.wav and "ENTER_PIN" is 02.wav and so on, therefore, the file replacing it must be named 01.wav or 02.wav...

5. Click **Choose File** to locate the file you want to use in place of the existing file.
6. Click **Upload**, and then click **Ok** at the prompt.

Note:
If necessary, click **Revert This Prompt to Default** to return to the default file for the selected prompt. This feature is only available for English language prompts and will not restore prompts for Custom Language 1 or Custom Language 2.

To upload custom voice prompt batch files:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Voice Prompts** in the navigation pane.

2. Select a language from the Prompts Language list that you are replacing.

> **Note**:
> You can upload custom prompts to replace all or some of the existing prompts.

3. Select **Batch** for the Mode.
4. Click **Choose File** to locate the .zip file for the prompts you are replacing.

> **Note**:
> File names in the .zip file must match the existing files they are replacing. If a file name does not match that file is ignored and the existing prompt is used.

5. Click **Upload**, and then click **Ok** at the prompt.
6. After the custom prompts are uploaded to MiCollab Audio, Web and Video Conferencing , go to the System Options page, and then select the language from the Language Prompts list.

20.6 Country Tone Plan

You can select the appropriate Country Tone Plan for your system.

1. From the MiCollab Audio, Web and Video Conferencing administrator page, click **Country Tone Plan** in the navigation pane.
2. Select the country from **Country Variant** list.
3. Click **Save**.

To upload custom tones:

1. Select the country from **Country Variant** list.
2. Select the **Upload Mode**. Select **File** to upload a single file or select **Batch** to upload a batch file.
3. Select the **Tone File**.
4. Click **Choose File** to locate the file you want to use.
5. Click **Upload**.

Note:
For countries not listed in the Country Variant list, you can select the closest country tone plan, or upload the audio files for Dialed number Busy, Invalid number dialed and Dialed number unavailable.

20.7 Music-On-Hold Settings

The MiCollab Audio, Web and Video Conferencing application includes a couple of files for Music-On-Hold (MOH). You can configure MiCollab Audio, Web and Video Conferencing so music is heard when users are placed on hold, and the music which is played. MOH files are stored in a 8 KHz, 8-bit, monophonic mu-law .wav file format.

To enable MOH:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Music-On-Hold Settings** in the navigation pane.
2. Select the **Enable Music-On-Hold** check box.
3. Select a file from the **Music-On-Hold File Name** list.
4. Click **Save**, and then click **Ok** at the prompt.

To upload a new MOH file:

1. Enter the path name or click **Browse** to select a new file.
2. Click **Upload**, and then click **Ok** at the prompt. The file is added to the end of the **Music-On-Hold File Name** list.

20.8 Licensing

Server port and user capacity is controlled by a license file through the Applications Management Center (AMC), which is installed on the MiCollab server at the time of installation. The Licensing page shows the current number of ports available. You can create as many MiCollab Audio, Web and Video Conferencing user accounts on the system as MiCollab will allow, typically about 4,000. Additional Audio-only or Web-only licensing can be purchased and installed on the MiCollab server.

MiCollab Audio, Web and Video Conferencing 4.0 requires an Enhanced Video License to use the higher resolution video provided by the H.264 codec.

Communications Platform License requirements

- MiVoice Business
  - One SIP User License per MiCollab Audio, Web and Video Conferencing User License
- MiVoice Office
  - One Category C License per MiCollab Audio, Web and Video Conferencing User License
  - One IP Enabler Unit License per MiCollab Audio, Web and Video Conferencing User License

    or One IP Enabler System License
  - System OAI Events License
  - System OAI Third-party Call Control License

For information about adding licenses, refer to the latest *MiCollab Installation and Maintenance Guide*.

To view the licensing information:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Licensing** in the navigation pane.
2. The Licensing page appears displaying MiCollab Audio, Web and Video Conferencing licensing information.

20.9 User Interface Wizard

The User Interface Wizard allows an administrator to customize the appearance of the MiCollab Audio, Web and Video Conferencing graphical user interface (GUI).

Note:
Only users that do ***not*** have an MiCollab Audio, Web and Video Conferencing account will see the custom top banner logo, background, and Welcome page image.

To view the server UI settings:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **UI Wizard** in the navigation pane.
2. Click **View Current** under the item to see the current graphic.

To change a graphic:

1. Click **Browse** and a window opens for you to navigate to the location of the new file.
2. Select the new file, and then click **Open**. The file path appears in the User Interface Wizard page. Select any additional files to change, if desired.

3. Click **Save**, and then click **Ok** in the confirmation dialog box to make the change.

To restore default settings:

1. Click **Restore All Defaults** to select all settings to change back, or select the **Default** check box next to the individual items.
2. Click **Save**, and then click **Ok** in the confirmation dialog box to restore the defaults.

20.10 Edit DAS Rules

Note:
The DAS Rules options are available in the MiCollab Audio, Web and Video Conferencing navigation pane only when you set Enable DAS Rules on the Systems Options page. When DAS rules are applied, Outgoing Prefix and Max Extension Length settings in System Options are not applicable.

DAS rules allow the product to dial outside numbers and internal PBX extensions. You can configure MiCollab Audio, Web and Video Conferencing with rules to handle a wide range of call routing and dial plan requirements. These rules can handle international dialing, PBX extension calling, and sophisticated SIP call processing.

DAS rules are a set of up to 20 UNIX regular expressions that are applied to dialed digits. The rules are applied the order in which they are listed in the DAS Rules table. The output of each rule is the input to the next rule. The result is used as the dialed digits that are processed through the MiCollab Audio, Web and Video Conferencing server call processing.

DAS rules are processed by the Perl Compatible Regular Expressions (PCRE) library distributed as libpcre. Details on this library are available from http://www.pcre.org/. MiCollab Audio, Web and Video Conferencing supports only the 'g' flag.

Click to view dialing plan configuration considerations.

Check for special or specific dialing plans for your company. For example, if you have access codes to connect to branch offices, remote locations, or international offices.

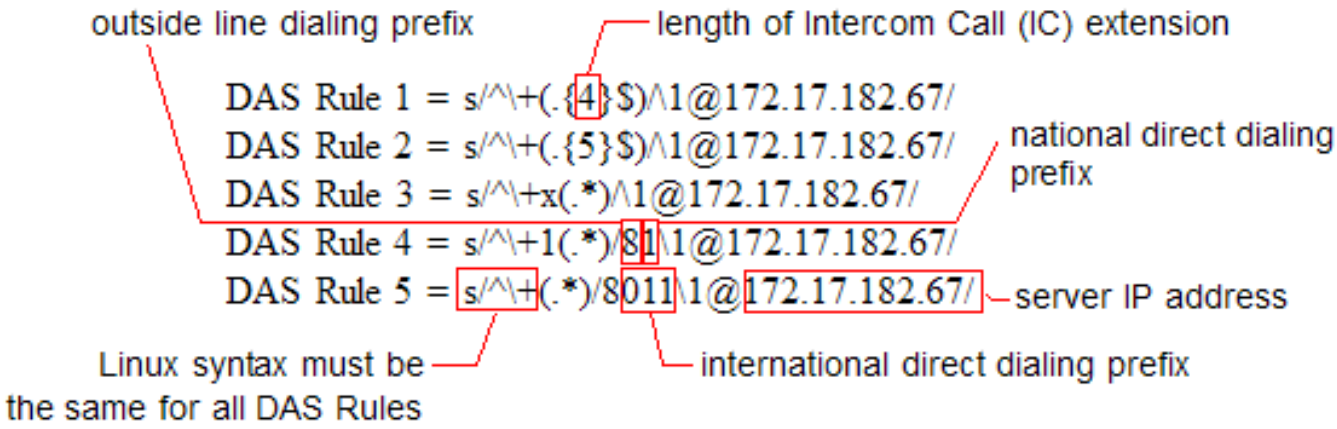
Check for blocked area codes (such as 800 or 900) and if so, what numbers that are blocked.

Check that all call processing programming has been completed, including Automatic Route Selection (ARS), dial rules, and other related information.

Note:
Performing this procedure disconnects all active calls.

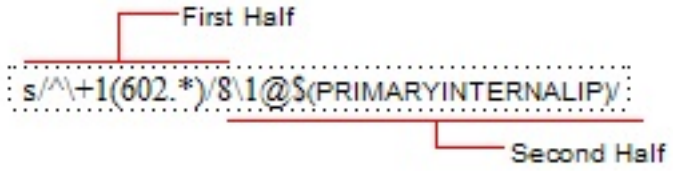
To configure dialing rule parameters:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Advanced Settings** in the navigation pane.
2. Click **Edit DAS Rules** to open the DAS Rules page.
3. Enter the specific rules you want the conferencing server to follow when processing dialed digits or SIP addresses. (Click to view an example.)



Note:
When configuring MiCollab Audio, Web and Video Conferencing for use with a Mitel MiVoice Office 250 , use 8 for the outside line dialing prefix. When configuring MiCollab Audio, Web and Video Conferencing for use with a Mitel 3300 system, use 9 (preferred) for the outside line dialing prefix.

Consider adding additional DAS rules to reflect your calling area. In this example, 602 is an area code in Phoenix, Arizona.



For additional explanation, click here.

4. **First Half**: What is being searched for (between "s/" and the second "/").

- **^** : Beginning of string to search.
- **\+1**: Phone numbers that start with a "1"
- **(602.*)**: Grab any phone number that starts with a "602" and save it.

5. **Second Half**: The replacement (between second "/" and third "/")

- **8**: The first number dialed to get an outside line, typically is either 8 or 9.
- **\1**: This is the "(602.*)" that was saved in the first half (i.e., the complete phone number.
- **@**: literally, the "@" sign
- **(PRIMARYINTERNALIP)**: The variable for the main IP address configured in TCP/IP Settings.

The result is any phone number starting with 1602 will have the leading "1" stripped off, replacing it with an "8", then the number, then @, then the IP address.

Click here for additional descriptions for the DAS rules.

Character	Description
$	End of the string
^	Beginning of string
. (period)	Any character
*	0 (zero) or more items. For example, a* means 0 or more number of a in the string.
?	0 (zero) or one item.
+	1 or more number items
\1, \2, \3, ...	Equivalent to the corresponding set of parentheses matches
()	Used to group matching characters in a string that can be referred to later
[]	Used to define a range. Example: [0-9] matches any digit
{n}	Exactly n occurrences of the previous item Examples: a{4} matches aaaa, and .{4} matches any four characters

Character	Description
{n,}	At least n occurrences of the previous item Example: a{4,} matches aaaa or aaaaa or aaaaaa, etc.
{n,m}	At least n but not more than m occurrences of the previous item Example: a{4,5} matches only aaaa or aaaaa

6. Click **Save**, and then click **Ok** at the prompt.

20.11 Google Apps Integration for MiCollab Audio, Web and Video Conferencing

With this release, MiCollab Audio, Web and Video Conferencing can be integrated with Google Apps. This enables users to transform their Google Calendar events into one-time conferences simply by clicking a gadget. In future releases, more features will be added such as the ability to initiate calls from Google Calendar.

Preconditions:

- In the System Options, select **Use HTTPS Only**. You must then configure a third-party SSL certificate in the MSL Server Manager. Note that you may not employ the self-signed certificate; using it will cause Google Apps integration to fail.
- In the Web Conferencing Settings, enter 80 for the **Internal Port** and 443 for the **External Port**.

Administrator tasks

Enable Google Apps Integration with MiCollab Audio, Web and Video Conferencing

The administrator must do the following:

1. Configure OAuth 2.0 for Service Accounts on page 2013

   When you set up an OAuth 2.0 API project with a service account for the Google Calendar application, you enable MiCollab Audio, Web and Video Conferencing to prove its identity to Google. The two systems can then communicate without involving end users.
2. Configure the Gadget Address

   The gadget address is the publicly accessible FQDN or IP address of the gadget service. After you configure it on the MSL server, users can download the Google- MiCollab Audio, Web and Video Conferencing gadget and transform their Google Calendar events into conferences with a single click. Users will receive a link to the address in their Welcome Email (see next step).

3. Send the Service Information (Welcome) Email

   The Welcome Email contains communications settings such as the user's login credentials, email address and phone number, along with instructions on how to download and configure the Google-MiCollab Audio, Web and Video Conferencing gadget. You should ensure that the Welcome Email is sent to all new and existing users.
4. Configure the Web Proxy

   You must configure your web proxy server to provide a secure interface between Google on the Internet and the MiCollab server on the LAN. If your enterprise is using MiVoice Border Gateway as a proxy server, access the LAN server proxy list and select **MiCollab** as the LAN server and **Google Calendar Integration to AWV** as the user interface (for configuration details, refer to the *MBG online help*). If your enterprise is using a proxy server from another manufacturer, configure it to forward Google Apps traffic (i.e. traffic that includes "google" as part of the FQDN in HTTPS requests) to the MiCollab server.

End-User tasks

Change the Password and Enable MiCollab Audio, Web and Video Conferencing Conference Functionality

Each user must do the following:

1. In your Welcome Email, click the link to the MiCollab End User Portal : https://< MiCollab server address>/portal
2. Log in to the portal using your account information (ID and password).
3. Change your password:

   - Select **Portal Password**.
   - Enter your old password and your new password in the appropriate fields.
   - Confirm your new password and then click **Save**.
4. In your Welcome Email, click the link to enable MiCollab Audio, Web and Video Conferencing conference functionality in your Google Calendar.
5. Select **Yes** to download and install the gadget.
6. Configure the gadget for use:

   - Click **Permissions** and then, in response to the prompt, click **Allow access**.
   - Enter your **Login ID** and **Password**.
   - Click **Save** to complete the configuration.

To create an MiCollab Audio, Web and Video Conferencing conference, access your Google Calendar, select a one-time or recurring event and click **Collaboration** check box in the gadget.

After setup is complete, you can join the conference simply by clicking on the event. Any changes you make to the event, such as adding more guests or changing the start time, will be reflected in the MiCollab Audio, Web and Video Conferencing conference.

Note:

- If you have just upgraded your system to include Google Apps integration, re-send the Welcome Email to all existing users.
- A conference that was created using the Google- MiCollab Audio, Web and Video Conferencing gadget can be viewed on the My Conferences Tab of the MiCollab Audio, Web and Video Conferencing Web Interface. However, if you edit this conference in the MiCollab Audio, Web and Video Conferencing interface, your updates will *not* be reflected in the Google Calendar.
- The Google- MiCollab Audio, Web and Video Conferencing gadget is available only for English variants of the product.
- To enable Google- MiCollab Audio, Web and Video Conferencing conferencing functionality, you must complete all three steps of the above-noted procedure.
- This feature can be expected to behave differently on different devices and browsers. It is optimized for operation on Google Chrome in a desktop environment. If you are using Internet Explorer and the MiCollab server is not equipped with proper certificates, you will need to install the Mitel Root Certificate in your browser.

  Internet Explorer

  Note:
  Steps may vary based on your browser, but the intent is to install the Mitel Root Certificate in the **Trusted Root Certification Authorities** store.

  1. Save the Mitel Root Certificate on your PC hard drive.
  2. Launch Internet Explorer.
  3. Select **Tools** and then click **Internet Options**.
  4. Click the **Content** tab and then click the **Certificates** button.
  5. Select **Trusted Root Certification Authorities** and click **Import**. The Certificate Import Wizard opens.
  6. Click **Next**.
  7. Click **Browse** and browse to the **mitelcert.cer** file and click **Open**.
  8. Click **Next**.
  9. Select **Place all Certificates in the following store**.
  10. Click **Browse** and select **Trusted Root Certification Authorities**.
  11. Click **OK**.
  12. Click **Next**.
  13. Click **Finish**.
  14. Click **Yes**. An Import was successful dialog appears.
  15. After the certificate is installed, restart Internet Explorer.
- In some circumstances, a user's Google Calendar may fall out of synchronization with MiCollab Audio, Web and Video Conferencing. For example, if the user creates a new Google- MiCollab Audio, Web and Video Conferencing conference and then quickly closes their Google Calendar or internet browser, MiCollab Audio, Web and Video Conferencing may fail to create a corresponding conference. Similarly, if the user creates a new Google- MiCollab Audio, Web and Video Conferencing conference while the MiCollab server is being rebooted, a corresponding conference

will not be created in MiCollab Audio, Web and Video Conferencing . To correct an out-of-sync error, the user should delete the event in Google Calendar and then recreate it.

20.12 Google Gadget Configuration

Google provides a framework for users and third parties to implement enhancements to Google Apps called "gadgets." MiCollab Audio, Web and Video Conferencing provides a gadget which users can employ to transform their Google Calendar events into one-time conferences with a simple click.

Note:
For complete instructions concerning how to implement the Google gadget, see the Google Apps Integration for AWV topic.

Address Configuration

Use this procedure to configure the publicly accessible address of the gadget service. Typically, this is external address of the firewall (IP address or FQDN), which should be configured to forward HTTP requests to the gadget service.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Google Apps**.
3. Select the **Gadget Configuration** tab.
4. Click **Edit**.
5. Enter the **External FQDN or IP address** of the MSL server. Typically, this is the publicly accessible address configured on the enterprise firewall configured to forward requests to the MSL server. The MiVoice Border Gateway can provide this service if it is configured to function as a web proxy for the Google Calendar integration to AWV.

   Note:
   Google gadget users will receive a link to this address in their Service Information (Welcome) Email

6. Click **Save**.

MiVoice Business SIP Server Configuration

21

This chapter contains the following sections:

- Configure MiVoice Business for MiCollab Audio, Web and Video Conferencing
- MiVoice Office 250 SIP Server Configuration
- MiVoice 5000 or MiVoice MX-ONE SIP Server Configuration
- MiVoice Office 400 SIP Server Configuration

Use these settings only when configuring MiCollab Audio, Web and Video Conferencing with a MiVoice Business system. Configure the MiVoice Business system first. Refer to the *MiCollab Installation and Maintenance Guide* for more instructions.

After you configure the MiVoice Business system for MiCollab Audio, Web and Video Conferencing, configure SIP Server settings in MiCollab Audio, Web and Video Conferencing using the account information from the MiVoice Business system configuration.

To configure the SIP component for the MiVoice Business:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Options** on the navigation pane.
2. In System Options – Platform, select **MiVoice Business** for the system connected to MiCollab Audio, Web and Video Conferencing .
3. Click **Save**, and then click **Ok** at the prompt to restart the server.
4. Click **Configure SIP Server** on the navigation pane. The MiVoice Business SIP Server Configuration page appears.
5. Enter the following information:

   - **Extension First:** Type the extension number of the first IP device in the hunt group used by the MiCollab Audio, Web and Video Conferencing server to register itself with the MiVoice Business.
   - **Extension Last**: Type the extension number of the last IP device in the hunt group used by the MiCollab Audio, Web and Video Conferencing server to register itself with the MiVoice Business.
   - **SIP Password**: Type an alphanumeric User PIN for the MiCollab Audio, Web and Video Conferencing ports on the MiVoice Business. This field is NOT mandatory.
   - **SIP Domain**: This can be the domain name, fully qualified domain name (FQDN), or the IP address of the Mitel 3300 system used to register the MiCollab Audio, Web and Video Conferencing SIP ports. If you do not know the domain name or FQDN, type the MiVoice Business system IP address.
   - **IP Address**: Type the IP address of the MiVoice Business system. Alternatively, type the FQDN of the MiVoice Business system.

     Note that when typing the FQDN, only the first IP Address value returned by the DNS lookup will be used.
   - **SIP Port**: Type the SIP port number of the MiVoice Business system. The port number is typically 5060.
   - **Registration Period**: Type the number of seconds for the registration period used by the MiCollab Audio, Web and Video Conferencing when it registers itself with the MiVoice Business. Note that this value also controls the registration refresh rate, which is normally half of the Registration Period.

Note:
AWV SIP Extension numbers must consist of digits 0 to 9 only. The * and # characters are not supported.

6. Click **Save**, and then click **Ok** at the prompt.
7. Verify the results of the SIP registration process, see Proxy Extension Status.

21.1 Configure MiVoice Business for MiCollab Audio, Web and Video Conferencing

Prerequisite in MIVB

- Set **Extended Hunt Groups** to **Yes** under **License and Option Selection** form.
- Select a **Class of Service (COS)** and **SIP Devices Capabilities** number from **System Properties** to be used for MiCollab Audio, Web and Video Conferencing.
- Set **Replace System based with Device based In-Call Features** to **Yes** under **SIP Devices Capability** assignment form.
- Set **Suppress Simulated CCM after ISDN Progress** to **Yes** under **Class of Service Option (COS)** form.

Note:
See *MiVB System Administration Tool Online Help* for more information on the assignment form.

Configuration on MiVoice Business platform

1. Navigate to **Users and devices** > **Advanced Configuration** > **IP Telephones** > **Multiline IP sets**, configure the number of virtual extension with device type as **Generic SIP Phone**.
2. Assign the COS and SIP Devices Capabilities number selected for MiCollab Audio, Web and Video Conferencing to the configured extensions.
3. Under **Hunt Groups** form, create a hunt group of type **Voice**. Assign the same COS number selected for MiCollab Audio, Web and Video Conferencing .
4. Add the configured virtual extensions as the members of the hunt group.

Configuration on MiCollab Server for MiCollab Audio, Web and Video Conferencing

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Options** under **Configuration**.
2. Enter the hunt group number (configured in MiVB) in the **Dial-In Phone Number** field.
3. Under **Platform** drop-down list, select **MiVoice Business**.
4. Click **Save**, and then click **Ok** at the prompt.
5. Click **Configure SIP Server** under **Configuration**.
6. Enter the first virtual extension DN (created in MiVB) in the **Extension First** field.
7. Enter the last virtual extension DN (created in MiVB) in the **Extension Last** field.
8. Enter the **SIP Domain** name and **IP address** of the MiVoice Business system used to register the MiCollab Audio, Web and Video Conferencing SIP ports.
9. Enter the **SIP Port** number of the MiVoice Business system. The port number is 5060.
10. Click **Save**, and then click **Ok** at the prompt.

Additional setting

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Web Conferencing Settings** under **Configuration**.
2. Enter the MiCollab Server IP in the **Web Conferencing Name** field.
3. Click **Save**, and then click **Ok** at the prompt.

Note:
End-user must verify if the MiCollab Audio, Web and Video Conferencing Client is installed correctly.

Note:
Create a new conference from the end-user portal and verify the conference by joining using the access codes.

Additional settings for SIP video support

This setting is enabled to support SIP video option during a MiCollab Audio Web and Video conference. Configure the following on MiVoice Business platform.

1. Navigate to **System Properties > SIP Device Capabilities.**

2. Under the SDP Option tab, the Allow Device to Use Multiple Active M-Lines option should be set as Yes.

21.2 MiVoice Office 250 SIP Server Configuration

The MiVoice Office 250 system must be configured first, before entering information for the SIP Server configuration. Refer to the *MiCollab Platform Integration Guide* for details about configuring the Mitel MiVoice Office 250 with MiCollab Audio, Web and Video Conferencing. After the Mitel MiVoice Office 250 is configured, enter the SIP Server settings in MiCollab Audio, Web and Video Conferencing using the account information from the Mitel MiVoice Office 250 system configuration.

To configure the SIP component for the Mitel MiVoice Office 250 :

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Options** on the navigation pane.
2. In System Options – Platform, select **Mitel CS250** for the system connected to MiCollab Audio, Web and Video Conferencing .
3. Click **Save**, and then click **Ok** at the prompt to restart the server.
4. Click **Configure SIP Server** on the navigation pane. The Mitel MiVoice Office 250 SIP Server Configuration page appears.
5. Enter the following information:

- **Extension First**: Type the extension number of the first IP device used by the MiCollab Audio, Web and Video Conferencing server to register itself with the MiVoice Office 250 .
- **Extension Last**: Type the extension number of the last IP device used by the MiCollab Audio, Web and Video Conferencing server to register itself with the MiVoice Office 250 .
- **Node Number**: Type the node number of the Mitel MiVoice Office 250 that is connected to MiCollab Audio, Web and Video Conferencing. If the Mitel MiVoice Office 250 is configured as a single node, type **1**, the default node number of the Mitel MiVoice Office 250 .
- **5000 IP Address**: Type the IP address of the Mitel MiVoice Office 250 system. If the system is configured as a Mitel 5600, type the IP address of the Base Server.
- **OAI IP Address**: Type the IP address of the server that provides OAI and SIP for the Mitel MiVoice Office 250 .
  - *If the system uses a CT Gateway*, type the IP address of the of the gateway.
  - *If the system has a PS-1*, type the IP address of the PS-1.
  - *If the system does* ***not*** *have a PS-1*, type the same IP address you entered for Mitel MiVoice Office 250 .
- **OAI Port**: Type the port number used on the Mitel MiVoice Office 250 for OAI. Default is 4000.
- **OAI Password**: Type the password used for OAI connection to CT Gateway.

Note:
AWV SIP Extension numbers must consist of digits 0 to 9 only. The * and # characters are not supported.

6. Click **Save**, and then click **Ok** at the prompt.
7. Verify the results of the SIP registration process; see Proxy Extension Status.

21.3 MiVoice 5000 or MiVoice MX-ONE SIP Server Configuration

Use these settings only when configuring MiCollab Audio, Web and Video Conferencing with a MiVoice 5000 or MiVoice MX-ONE system. Configure the MiVoice 5000 or MiVoice MX-ONE system first, and then configure the SIP server.

Configure the SIP Server settings in MiCollab Audio, Web and Video Conferencing using the account information from the MiVoice 5000 or MiVoice MX-ONE configuration.

To configure the SIP component:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Options** on the navigation pane.
2. In System Options – Platform, select **MiVoice 5000** or **MiVoice MX-ONE** for the system that is connected to MiCollab Audio, Web and Video Conferencing .
3. Click **Save**, and then click **Ok** at the prompt to restart the server.
4. Click **Configure SIP Server** on the navigation pane. The SIP Server Configuration page appears.
5. Enter the following information:

- **Extension First:** Type the extension number of the first IP device in the hunt group used by the MiCollab Audio, Web and Video Conferencing server to register itself with the PBX.
- **Extension Last**: Type the extension number of the last IP device in the hunt group used by the MiCollab Audio, Web and Video Conferencing server to register itself with the PBX.
- **Extension PIN**: This PIN is used for SIP MD5 authentication. If authentication is activated on the MiVoice 5000, this field is mandatory and is equal to the SIP password for subscriber "Extension First" to "Extension Last".
- **SIP Domain**: This can be the domain name, fully qualified domain name (FQDN), or the IP address of the PBX system used to register the MiCollab Audio, Web and Video Conferencing SIP ports. If you do not know the domain name or FQDN, type the PBX system IP address.
- **IP Address**: Type the IP address of the PBX system. Alternatively, type the FQDN.

  Note that when typing the FQDN, only the first IP Address value returned by the DNS lookup will be used.

Note:
AWV SIP Extension numbers must consist of digits 0 to 9 only. The * and # characters are not supported.

6. Click **Save**.

21.4 MiVoice Office 400 SIP Server Configuration

The MiVoice Office 400 system must be configured first, before entering information for the SIP Server configuration. Refer to the *MiCollab Platform Integration Guide* for details about configuring the Mitel MiVoice Office 400 with MiCollab Audio, Web and Video Conferencing. After the Mitel MiVoice Office 400 is configured, enter the SIP Server settings in MiCollab Audio, Web and Video Conferencing using the account information from the Mitel MiVoice Office 400 system configuration.

To configure the SIP component:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Options** on the navigation pane.
2. In System Options – Platform, select **MiVoice 400** for the system that is connected to MiCollab Audio, Web and Video Conferencing .
3. Click **Save**, and then click **Ok** at the prompt to restart the server.
4. Click **Configure SIP Server** on the navigation pane. The SIP Server Configuration page appears.
5. Enter the following information:

   - **Extension First:** Type the extension number of the first IP device in the hunt group used by the MiCollab Audio, Web and Video Conferencing server to register itself with the PBX.
   - **Extension Last**: Type the extension number of the last IP device in the hunt group used by the MiCollab Audio, Web and Video Conferencing server to register itself with the PBX.
   - **Extension PIN**: This PIN is used for SIP MD5 authentication. If authentication is activated on the MiVoice Office 400, this field is mandatory and is equal to the SIP password for subscriber "Extension First" to "Extension Last".
   - **SIP Domain**: This can be the domain name, fully qualified domain name (FQDN), or the IP address of the PBX system used to register the MiCollab Audio, Web and Video Conferencing SIP ports. If you do not know the domain name or FQDN, type the PBX system IP address.
   - **IP Address**: Type the IP address of the PBX system. Alternatively, type the FQDN.

     Note that when typing the FQDN, only the first IP Address value returned by the DNS lookup will be used.

Note:
AWV SIP Extension numbers must consist of digits 0 to 9 only. The * and # characters are not supported.

6. Click **Save**.

Recording Retention Settings 22

The Recording Retention Settings allows an administrator to set:

- auto-clean mechanism, this will set the number of days before the **system automatically deletes** the recording.

To view the server Recording Retention Settings:

- From the MiCollab Audio, Web and Video Conferencing main page, click **Recording Retention Settings** in the navigation pane.

To change the server Recording Retention Settings:

1. Options to **Delete Records After xx Days** (the range is from 30-365 days, default value is 60 days).
2. Options to **Send email alert to the user xx Days before deletion** (the range is from 1-30 days, default is 7 days)
3. Click **Save**.

Note:
Upgraded systems from MiCollab Audio, Web and Video Conferencing 4.0 or earlier will automatically have their recordings from the old version set as permanent records.

Client Only Delivery 23

The Client Only Delivery (Manage Clients) panel allows you to control the versions of the MiCollab Audio, Web and Video Conferencing client applications that are available to users.

To upgrade or downgrade an MiCollab Audio, Web and Video Conferencing client application version:

1. From the MiCollab Audio, Web and Video Conferencing main page, under **Configuration** , click **Manage Clients** .
2. Click **Browse** to open the File Upload window.
3. Navigate to the new MiCollab Audio, Web and Video Conferencing client file (.rpm extension) to upload.
4. Click **Upload New Client** to place the new client version on MiCollab Audio, Web and Video Conferencing server, which will automatically make it available for the users.
5. Once the client package has been successfully uploaded and installed, a success message is displayed.
6. When a new client package is uploaded, the following validation checks are performed on the package before the package is installed:

    a. Verify the package is a valid RPM file
    b. Verify the RPM has not been corrupted
    c. Verify the RPM is a valid MiCollab Audio, Web and Video Conferencing client RPM
    d. Verify the RPM version is not already installed

Note:
If any of these validation steps fail, then the RPM is not installed and an error message containing the reason for the failure is displayed

To restore an original client version:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Manage Clients** in the navigation pane.
2. Click **Restore Original** , button next to the client package to restore.
3. Once the client package has been successfully restored to its original version, a success message is displayed.

Two-Way Audio Settings 24

About MiCollab AWV Two-Way Audio

As a MiCollab user in Audio, Web and Video conference (AWV), with the introduction of the feature of two-way audio mode, the user can use the AWV web client for two-way audio functionality, similar to an AWV desktop client.

This topic provides instructions on how to integrate and configure the two-way audio feature with the supported PBXs.

Two-Way Audio Integration

The user will see the two-way audio option in AWV web client if the feature is configured on the MiCollab server and if the WebRTC supported browsers and operating systems are used.AWV web client uses MiVoice Border Gateway (MBG) anonymous call WebRTC capability.

Two-way audio integration with MiCollab is a three-step process:

- AWV Configuration
- MBG Configuration
- PBX Configuration

Note:

The supported platforms for two-way audio are MiVoice Business, MiVoice 5000, and MX-One.

Note:

The two-way audio on MX-One is supported only on Standalone MBG.

Note:

The MBG WebRTC settings should be configured on AWV for the two-way audio to work.

Note:

MBG should be provisioned with an additional RAM and CPU for proper functioning of two-way audio WebRTC calls. For more information on memory and CPU usage, see **MiCollab Engineering Guidelines** > **MiVoice Border Gateway Guidelines** section.

Requirements for Two-Way Audio from the Web Client

Component	Requirement
Mobile Device Operating System	Android (Mobile/Tablets)
Web Browser	• Mozilla Firefox® Standard Release 115 or higher • Google Chrome™ 115 or higher
Operating System	• Windows 10 and 11 • Mac™
Devices	Surface Pro

To Enable Two-Way Audio

AWV Configuration

Configure the following fields for MBG WebRTC Settings under **Server Manager > Audio, Web and Video Conferencing > Configuration > Two-Way Audio Settings**.

- **MBG Server Name**- Enter the name of the MBG server.
- **MBG WebRTC Port**- Enter the port number of WebRTC. The default value of MBG WebRTC port is 5063.

- **Web Server Shared Secret**- This value should be same as the WebRTC value for MBG configuration.
- **SIP URI** - Enter the SIP URI details from the MiVoice 5000 PBX configuration. Note that this field is case sensitive. This field is visible only when MiVoice 5000 is selected.

Note:
The AWV hunt group number of PBX must be configured under the **Dial-In Phone Number 1** field which is present in the system options of the AWV admin portal.If that value does not match the MiVB AWV Hunt Group Number, MBG will be unable to connect with audio.

To view and update the MBG WebRTC settings, see **Server Manager > MiVoice Border Gateway > Teleworking > WebRTC**.

MBG Configuration

1. Log in to MiCollab Server Manager and navigate to **MiVoice Border Gateway >Teleworking >WebRTC**.
2. Select the **Enabled** checkbox to enable the WebRTC Service.
3. Under **Licenses**, make sure you have active **Anonymous calls** licenses. If this value is “0” then purchase the following license from AMC and sync MiCollab licenses.

   “MBG: 1 SIP Trunking Channel License”.

Note:
Purchasing 1 SIP Trunking Channel License will allow you only one 2-way audio connection. You will need to buy enough licenses to meet your expected usage.

4. Change the **Hosting mode** to **anonymous and subscriber**.
5. Configure the **Webserver shared secret** password.
6. Click **Save**

For detailed description of WebRTC settings, see **Configuration** > **WebRTC** section in the MBG online help document.

PBX Configuration

The SIP trunking configurations on different PBX is explained in below sections:

Note:

Make sure SIP trunk is established between MBG and the PBX, and anonymous call is allowed in the PBX.

MiVoice Business Configuration

1. In the MiVoice Business System Administration Tool, click **View by Category**.
2. Add licenses using the following procedure:

   a. Access the **License and Options Selection** form.
   b. Under **Trunking Networking**, enter the number of SIP Trunk licenses for your implementation. This is the maximum number of concurrent trunk sessions that can be configured.
3. Configure a network element for MBG:

   a. Access the **Network Elements** form and add a new entry.
   b. Configure the following fields:

Field	Description
Name	Enter a unique name of up to nine characters for the network element (e.g. WebRTC).
Type	Select **Other**.
FQDN or IP Address	Enter the LAN IP address of MBG, provided that MBG is operating in Server-Gateway mode.

   c. Record the network element Name. You will require it in step 5, below.
   d. Select the SIP Peer check box and configure the following fields:

Field	Description
SIP Peer Transport	Select **UDP**
SIP Peer Port	Enter 5064

SIP Peer Status	Select **Always Active**

e. Click **Save**.

4. Configure the SIP trunk attributes:

a. Access the **Trunk Attributes** form and select a trunk service number that is available to be changed.

b. Configure the following fields:

Field	Description
Non-Dial-In Trunks Answer Point - Day	Enter the destination number (answer point) to which incoming WebRTC trunk calls are routed during the Day service. This can be a station, hunt group pilot number, DISA number, or System Speed call number on the ICP.
Non-Dial-In Trunks Answer Point - Night 1	Enter the same value as specified above.
Non-Dial-In Trunks Answer Point - Night 2	Enter the same value as specified above.
Trunk Label	(Optional) Enter the character string to identify the trunk.
For anonymous mode WebRTC calls, the trunk must use the same answer point for each mode of service.	

c. Click **Save**.

d. Record the Trunk Service Number that you have modified. You will require it in the next step.

5. Configure the SIP peer profile.

a. Access the SIP Peer Profile form and add a new entry.

b. Configure the following fields:

Field	Description
SIP Peer Profile Label	Enter the name of the network element (e.g. WebRTC).
Network Element	Select the network element that you created for the MBG

Address Type	Select **IP Address**
Trunk Service	Enter the SIP **Trunk Service Number** that you modified in the previous step.

c. Click **Save.**

d. Record the SIP Peer Profile Label. You will require it in the next step.

6. Configure the SIP Peer Profile Assignment by Incoming DID:

a. Access the **SIP Peer Profile Assignment by Incoming DID** form and add a new entry.

b. Configure the following fields:

Field	**Description**
Incoming DID Range	Enter the destination number (answer point) to which incoming WebRTC trunk calls are routed on the ICP.
SIP Peer Profile Label	Select the **SIP Peer Profile Label** that you added in the previous step.

c. Click **Save.**

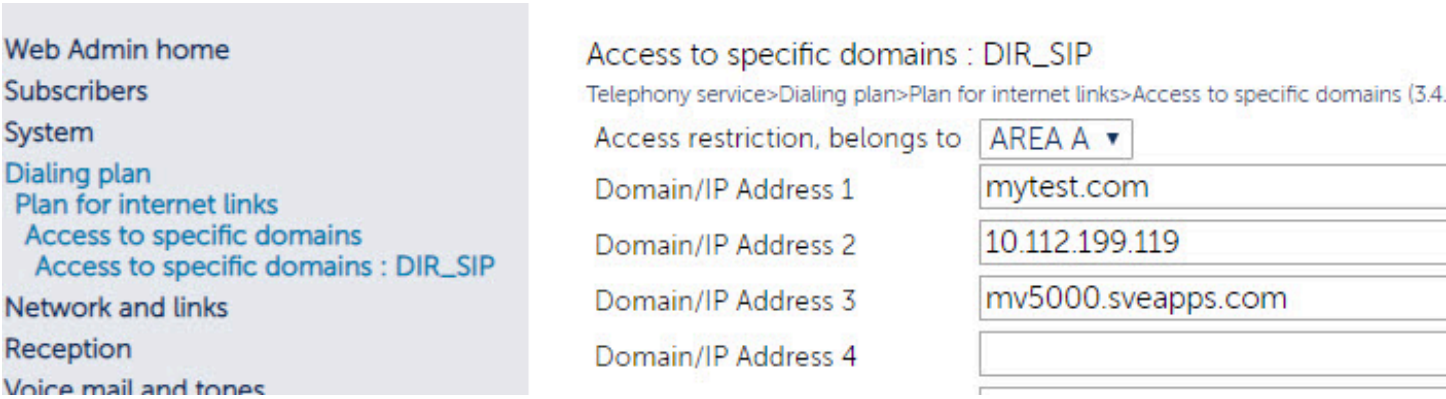
MiVoice 5000 Configuration

1. Log-in to the MVoice 5000, navigate to **Dialing Plan** > **Direction names** and configure the **Associated direction**.

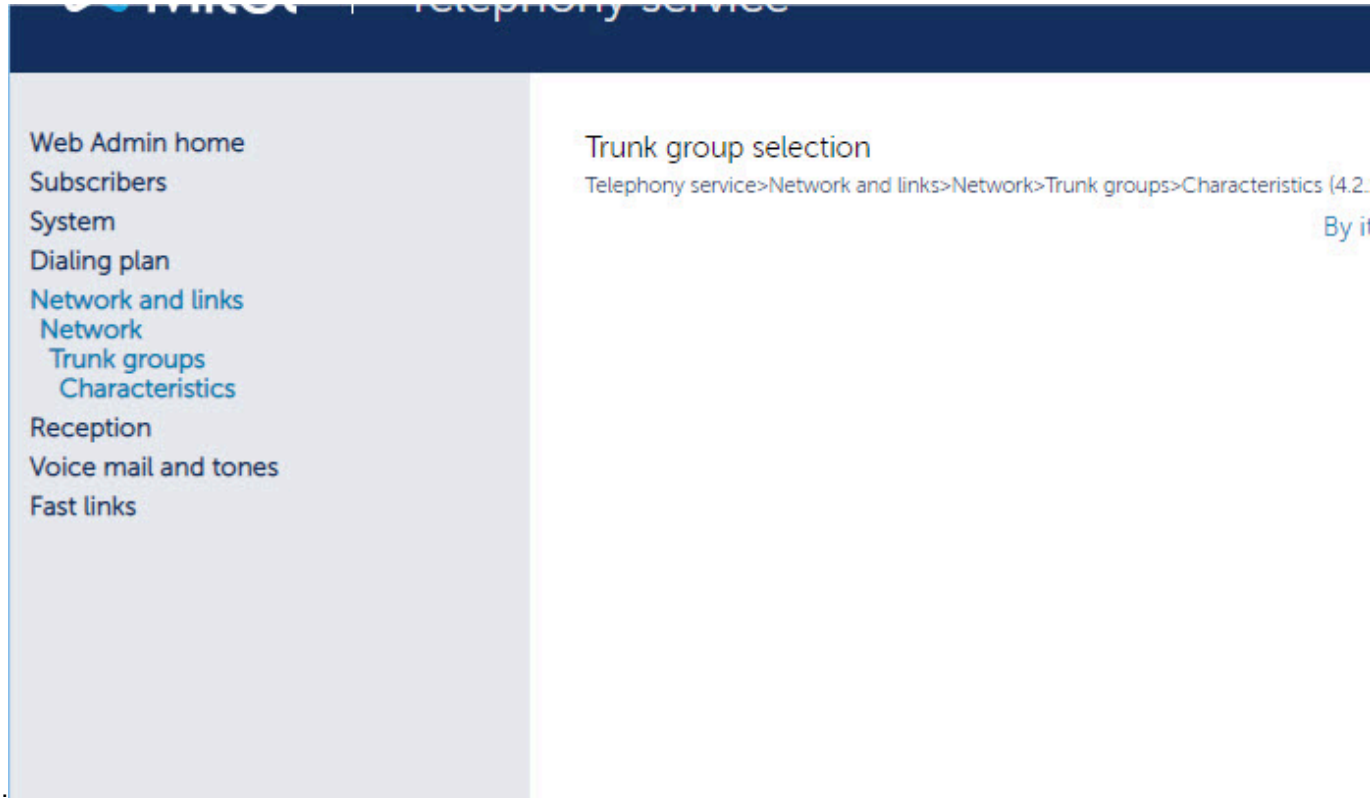
Enter the Private direction value in the textbox (for example, DIR_SIP).



2. Navigate to **Dialing Plan** > **Plan for Internet links** > **Access to specific domains**, enter the domain name or IP address under the **Domain/IP Address 1** textbox (for example, mytest.com).



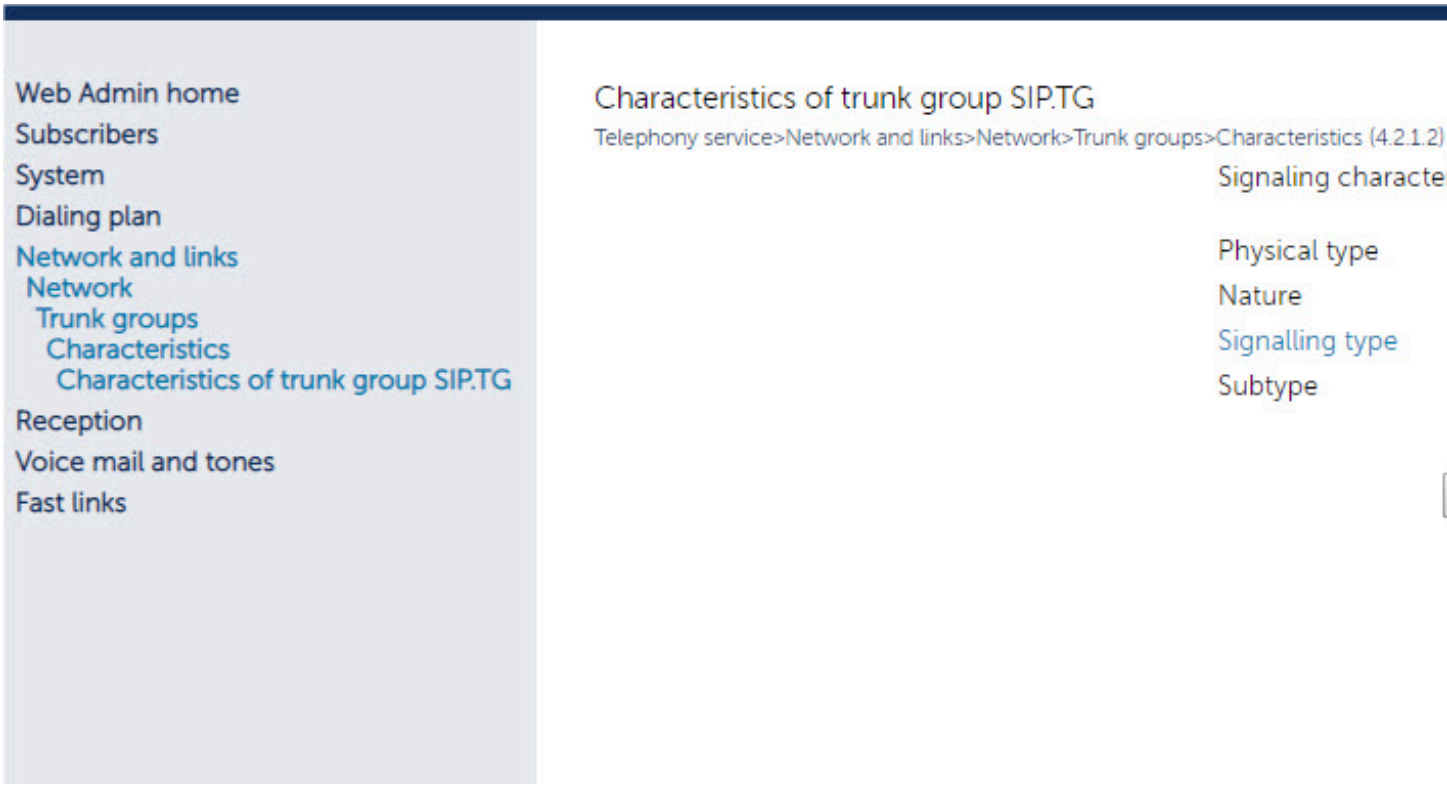
3. Navigate to the **Trunk Group**. In the Trunk group selection page, click on the **Select the item** button.



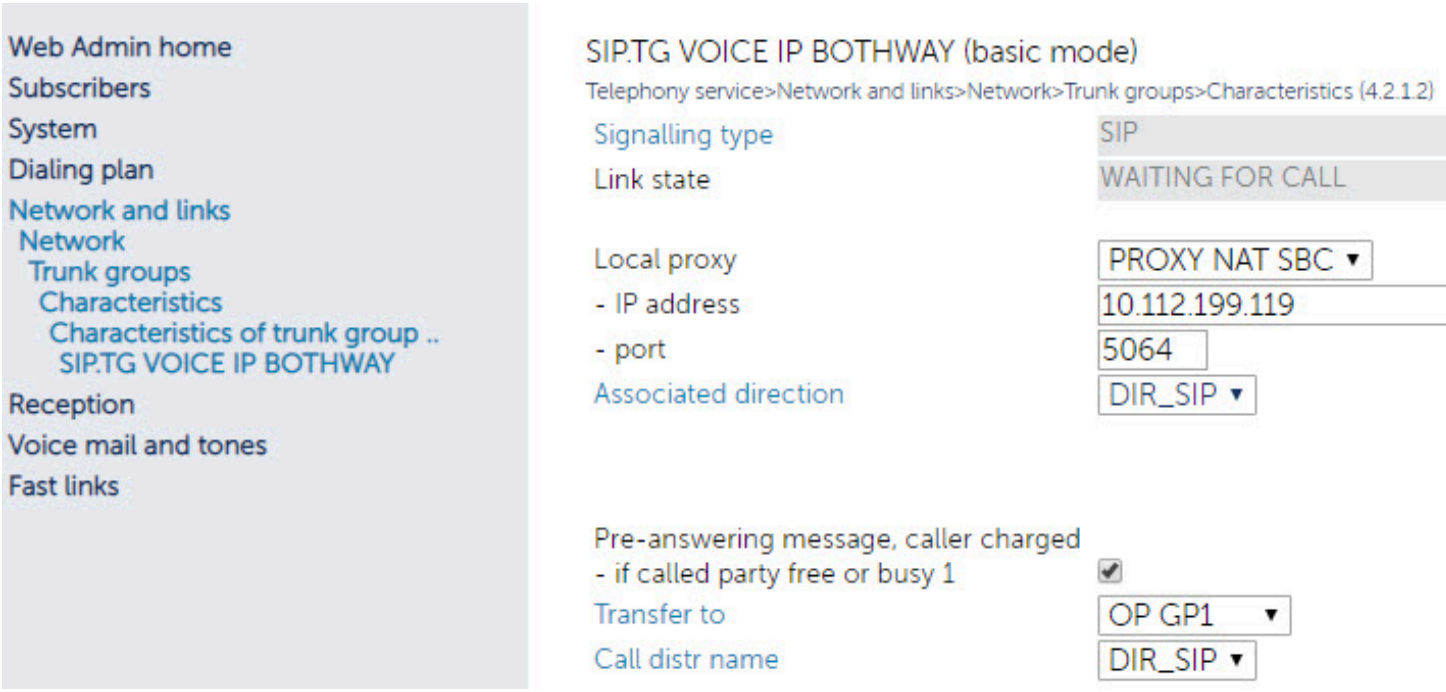
4. Select the following fields:

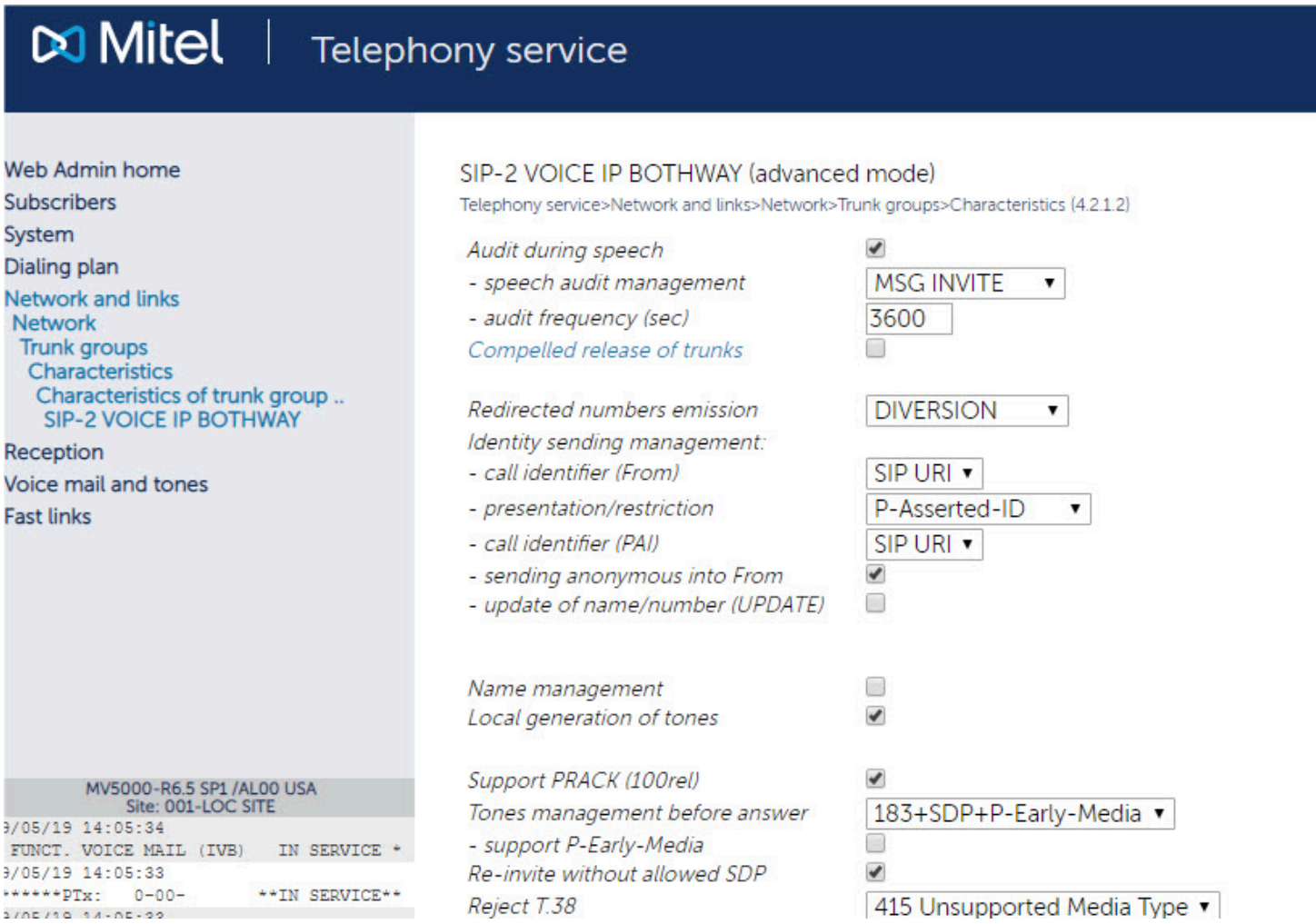
   a. • Signaling type as SIP.
   b. • Subtype as Internet Link.

5. Click the **Characteristics** button.

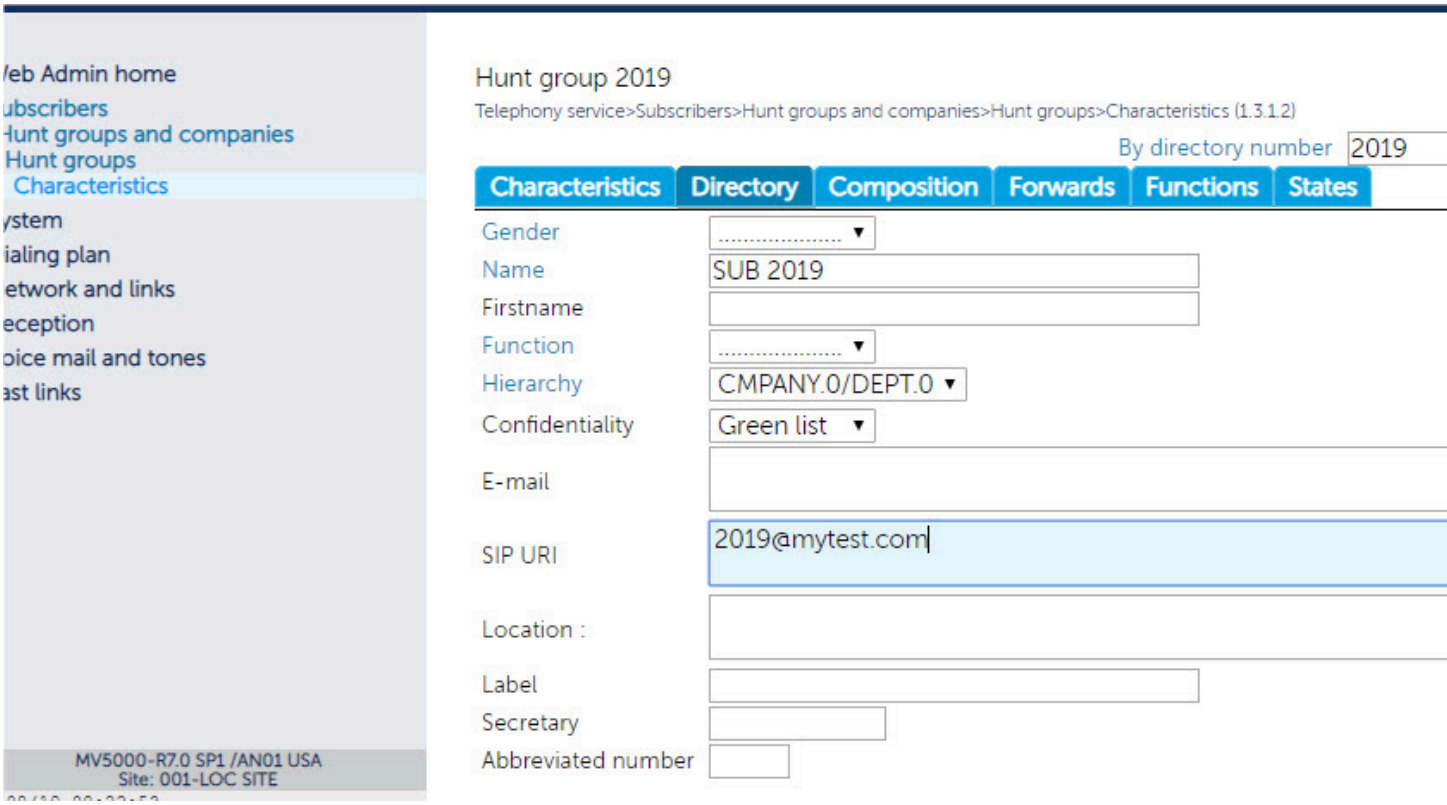


6. Enter the values as displayed in the screenshots below (for example, IP address: MBG's IP) and then click the **Advanced mode** icon (on top of the page) to view and configure the settings.




Mitel
Telephony service
Web Admin home
Subscribers
System
Dialing plan
Network and links
Network
Trunk groups
Characteristics
Characteristics of trunk group ..
SIP-2 VOICE IP BOTHWAY
Reception
Voice mail and tones
Fast links
MV5000-R6.5 SP1 /AL00 USA
Site: 001-LOC SITE
9/05/19 14:05:34
FUNCT. VOICE MAIL (IVB) IN SERVICE *
9/05/19 14:05:33
******PIx: 0-00- **IN SERVICE**
SIP-2 VOICE IP BOTHWAY (advanced mode)
Telephony service>Network and links>Network>Trunk groups>Characteristics (4.2.1.2)
Audit during speech
- speech audit management
MSG INVITE
- audit frequency (sec)
3600
Compelled release of trunks
Redirected numbers emission
DIVERSION
Identity sending management:
- call identifier (From)
SIP URI
- presentation/restriction
P-Asserted-ID
- call identifier (PAI)
SIP URI
- sending anonymous into From
- update of name/number (UPDATE)
Name management
Local generation of tones
Support PRACK (100rel)
Tones management before answer
183+SDP+P-Early-Media
- support P-Early-Media
Re-invite without allowed SDP
Reject T.38
415 Unsupported Media Type

7. Open the Hunt group page and enter the SIP URI details AWVHuntGroup@mytest.com) as shown below:



MiVoice MX-One Configuration

Note:
The two-way audio on MX-One is supported only on Standalone MBG.

Run the below commands on MX-One server (using MDSH commands) for creating SIP trunking between MX-One and MBG. Fill *MBG-IP, MX-One-IP, MBG's FQDN,* and *RouteNo* (any free Route) values in below mentioned commands:

set _ECHO=yes

sip_route -set -route RouteNo-profile 'MBG-anonymous-webRTC' -uristring0 'sip:?@MBG-IP' -uristring1 'sip:+?@MBG-IP' -remoteport '5064' -fromuri0 'sip:!?@Mxone-IP' -fromuri1 'sip:+!?@Mxone-IP' -accept FROM_DOMAIN -match 'MBG's FQDN' -challenge no

ROCAI:ROU=RouteNo,SEL=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4,SERV=3100001001,BCAP=0

RODAI:ROU=RouteNo,TYPE=TL66,VARI=00000000,VARC=00000000,VARO=00000000;

ROEQI:ROU=RouteNo,TRU=1-1&&1-9;

set _ECHO=no

To Disable Two-Way Audio in AWV

In the **Two-Way Audio Settings** page, when you click the **Reset** option,All fields are cleared, except the MBG WebRTC Port value of 5063, which is saved.

1. In the **Server Manager** page, under **Application** click on **Audio, Web and Video Conferencing.**
2. Click on the **Two-Way Audio Settings.**
3. In **Two-Way Audio Settings** page, click on **the Reset** button.

   A warning message is displayed, which states that resetting will restart the call server, resulting in the loss of all the current calls.
4. Click **OK** to confirm or click **Cancel** to terminate the task.

Troubleshooting

Scenarios for AWV Web Client errors

Sl No	AWV WebClient Error Messages Reported by User	Possible correction steps for Admin/User
1	Failed to reach MBG audio gateway. Please check your network connection and try again. If problem persists, contact the administrator.	• The user should check the network connection, which should be in working condition and stable. • MBG FQDN and PORT should be accessible from the user's system • The administrator should check if the MBG FQDN and PORT configured in MBG WebRTC settings are correct.
2	MBG audio gateway authentication has failed, please contact the administrator.	• The Web Server shared secret provided in MBG WebRTC Settings isn’t valid. • To retrieve the currently used Webserver shared secret key, go to **Admin Portal>MBG>Teleworking>WebRTC>Download SDK**. Extract the downloaded file, open config.php file, look for $websocket_passphrase entry. The value against it is the secret key. Use this key for configuring MBG WebRTC in AWV. • Admin can set a new secret key in **Admin Portal>MBG>Teleworking>WebRTC**, and use that in MBG WebRTC in AWV.

3	Failed to establish connection with MBG audio gateway. Please try again. If problem persists, contact the administrator.	• In case of this error, the user should download the Web Client logs from,**More > Web Client Logs**, and share it with the support team.
4	An error occurred while joining the audio. Please refresh your browser and try again. If problem persists, contact administrator.	• If refreshing the browser doesn't resolve the issue then Web Client logs should be downloaded from,**More > Web Client Logs**, and shared with the support team.
5	No audio device detected on system. Please check your system audio settings and try again.	• User needs to attach an audio device to the system and recheck. • If audio device is already attached to the system, then user needs to check and configure it in System Audio Setting.
6	User reports about audio getting silent in an on-going call	• User needs to reconnect the audio call. If that doesn't work then refresh the Web Client. • If the user is continuously facing this issue, the AWV Web client logs should be collected and shared with the support team.

To know more about on how to configure WebRTC on MBG and configure ICP for WebRTC, see Configure ICP for WebRTC and Configure MBG for WebRTC.

Refer the MiCollab Engineering Guidelines for MBG hardware resource requirement for supporting WebRTC Audio Calls in AWV.

Manage or Delete a User Profile 25

This chapter contains the following sections:

- Add User
- Add Guest User
- Administer User
- View Scheduled Conferences
- View Call Activity Report
- Schedule a Reservationless Conference
- Add a Delegate
- Support for Apostrophes
- List Users
- Bulk Provision Users
- Bulk Provision Reservationless Conferences
- Default User Settings
- Broadcast Email
- Billing Codes
- Active Calls
- Proxy Extension Status
- Manage Published Data
- Manage Recordings
- License Usage
- SIP Logs
- Call Activity Reports
- VoIP Utilization Statistics
- Scheduled Conferences
- System Alerts Log
- Install History Log
- Port Reservations Report
- Downloading Web Sharing Logs

In the user profile screen, you can change user settings or delete the user from the system. When a user profile is deleted, the MiCollab Audio, Web and Video Conferencing account is no longer accessible for that user. This also deletes all associated conference access codes for the user.

System Users

To manage a system user profile:

1. Select the system user account that you want to manage. To select a user, refer to Administer User.

2. Click **Manage User Profile**. Click here for a description of the user profile screen:

- **New Password**: Indicates the password used to log on to their MiCollab Audio, Web and Video Conferencing account. Type information in this box only when you want to change the password for this user.
- **Registered Phone**: Indicates the telephone number of the user that MiCollab Audio, Web and Video Conferencing will call when calling out to the User ID. Type the extension number, for example 1000, and the software adds an *x* before the number.
- **Personal ID**: Select a 3 to 5 digit identification number. Left leading zeros are allowed, for example ID 123 is not the same as ID 0123.
- **Dial out allowed**: Indicates this user can dial out (CO call) to others using the system. The default is selected.
- **Deny multiple leaders**: Indicates this user may not have multiple callers using the leader access code on conference calls. Only one leader will have the access code. The default is cleared.
- **Executive**: Conferences created by Executive users have access to audio ports reserved as executive ports. Refer to System Options for more information about this feature. The default is cleared.
- **Conference Settings**: Reservationless conferences do not expire for up to six months. Select from the following three options:
- *Reservationless calls allowed, leader not required*: (default) This user can make reservationless calls and a leader code is not required to access the call.
- *Reservationless calls allowed, leader required:* This user can make reservationless calls, but a leader code is required to access the call.
- *Reservationless calls not allowed:* This user cannot make reservationless calls.
- **Invitation Handler**: Indicates which e-mail invitation type is being used:
- *Default Programs*: This setting is typically for Microsoft Outlook users (or any other application that supports ICS files). Note that although other third-party clients may be compatible, only Microsoft Outlook is officially supported.
- *Google*: This setting is meant for calendar entries composed via Google Calendar and e-mail handled via Gmail.

- **Invitation Length**: Select either of the following e-mail invitation length:
- *Generic Long*: Use this setting for e-mail clients (for example, Microsoft Outlook) that allow for long form inserts (usually more than one line).
- *Generic Short*: Use this setting for e-mail clients that only allow short form inserts (usually one line).

3. Click **Save Changes**, and then click **Ok** at the prompt.

To delete a user profile:

1. Select the user account that you want to delete. To select a user, refer to Administer User.
2. Click **Manage User Profile**.
3. Click **Delete User** at the bottom of the user profile screen, and then click **Ok** at the prompt.

Guest Users:

To manage a guest user profile:

1. Select the guest user account that you want to manage from List User.

2. Modify the **Personal ID**: Select a 3 to 5 digit identification number. Left leading zeros are allowed, for example ID 123 is not the same as ID 0123.
3. Click **Save Changes**, and then click **Ok** at the prompt.

To delete a guest user profile:

1. Select the guest user account that you want to manage from List User.
2. Click **Delete User** at the bottom of the user profile screen, and then click **Ok** at the prompt.

25.1 Add User

You can create an account for a user that allows that user to access MiCollab Audio, Web and Video Conferencing .

Note:
Do **not** add new MiCollab Audio, Web and Video Conferencing users, delete existing MiCollab Audio, Web and Video Conferencing users, or manage accounts from the MiCollab Audio, Web and Video Conferencing administrator interface. Instead, configure users from the MiCollab administrator interface, Server Manager – Users and Services. If you create new users through the MiCollab Audio, Web and Video Conferencing administrator, they will appear as an Unassigned service associated with MiCollab Audio, Web and Video Conferencing. Use the Users and Services application to manage user accounts.

Note:
The Create User Password field does not accept the Apostrophe (‘) or Backslash (\) characters.

Note:
The Add User option does ***not*** appear in the navigation pane when Use LDAP is set.

25.2 Add Guest User

Guest users are created to accommodate individuals who regularly access conferences and therefore would benefit from having their own user profile. These guest users cannot create conferences.

NOTE: Guest User Accounts must be created on MiCollab Audio, Web and Video Conferencing, they cannot be created via MiCollab administrator interface.

To add individual guest user:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Add Guest User** in the navigation pane.
2. Type a **Display Name** and **Email** for this user. The Email must be in a valid e-mail address format, for example name@host.com.
3. Type a **Personal ID**: Select a 3 to 5 digit identification number. Left leading zeros are allowed, for example ID 123 is not the same as ID 0123.
4. Type the **Registered Phone** number for this user. For non-extensions, enter the full number, with area code and it will be formatted automatically.
5. Click **Create User**. A prompt appears confirming that the new user has been added to the system.

25.3 Administer User

After a user account is created, you can view, modify or delete information by selecting from the following options.

- Manage User Profile
- View Scheduled Conferences
- View a Call Activity Report
- Schedule a Reservationless Conference
- Add a Delegate

Before you can view, modify or delete user account information, you must first select a user.

To select a user account:

From the MiCollab Audio, Web and Video Conferencing main page, do one of the following:

- Click **Administer User** from the navigation pane to open the User Lookup page.
- Type the **Username** of the account you want to modify. If you type a partial user name, it can return multiple results.

> **Note**:
> An option to include non-system users (guest users) can be selected.

- Click **Search** to view search results, and then click the user name. The user options screen opens for the selected user.
- Click **List Users** from the navigation pane, and then select the user name account that you want to access. The user options screen opens for the selected user.

25.4 View Scheduled Conferences

This selection allows you to view a list of the user's scheduled conferences, including date, time, and access codes.

To view scheduled conferences:

1. Select the user account that you want to view conferences. To select a user, refer to Administer User.
2. Click **View Scheduled Conferences**.
3. Select a date range for the scheduled conferences to view.
4. Click **View** to see a list of conferences scheduled by the user for those dates selected.

25.5 View Call Activity Report

This selection allows you to view daily usage statistics to track server usage, system conferencing information, or a list of the user's scheduled conferences, including date, time, and access codes.

To view scheduled conferences:

1. Select the user account that you want to view a report. To select a user, refer to Administer User.
2. Click **View Call Activity Report**.
3. For the date range, do one of the following:

   - Select from the **Date Range** list.
   - Click one of the **Shortcuts**.
   - Select **Start Date/Time** and **End Date/Time** from the lists.
4. (*optional*) Type a specific **Project Code** or **Department Code** to filter the data based on the parameters entered. A project code and department code may be entered when a user creates a conference.
5. The user name of the profile you are managing is displayed in the **User** box.
6. Select from the **Sort By** list to determine how you want the report to appear.
7. Select a format, either **Web Report** (default) or **CSV Report**, and then click **View**.

   - *If you select Web Report for the format*, the results are displayed on the screen.
   - *If you select CSV Report for the format*, click **Save** at the prompt to save the file to a location or click **Open** to display the results in your default text editor for example, Microsoft® Excel®.

25.6 Schedule a Reservationless Conference

You may establish reservationless conferences for users. This feature allows users to hold conferences at anytime, without having to schedule them in advance and without having to use the Web client.

If Custom Access Codes have been enabled, you have the option of defining the leader and participant access codes. These custom access codes can be three to five digits in length. If Custom Access codes have not been enabled, you have the option of pre-defining a user's participant access code. This code, given to participants dialing into the conference, must meet the minimum IVR access code length which is defined by the system as 7 digits.

To set up a reservationless conference:

1. Select the user account that you want to set up conferences. To select a user, refer to Administer User.
2. Click **Schedule a Reservationless Conference**.
3. If Custom Access Codes have been enabled on the System Options page, you can type a three, four, or five digit access code for both the leader and participants. These access codes cannot begin with zero.

   If Custom Access Codes have NOT been enabled on the System Options page, type a seven-digit participant access code (starting with 01) in the box. If the box is left blank, the system will use a random access code.

> **Note**:
> If the participant access code you requested is already in use on the system, a prompt informs you that the access code is not available. Try a different code. If Custom Access Codes have not been enabled, MiCollab Audio, Web and Video Conferencing automatically generates a leader code that is unique. If Custom Access Codes have been enabled, but you do not specify them, the system automatically creates seven digit access codes for both the leader and participants.

4. Select **Create interactive Web Conference** if the conference also includes a Web conference.
5. If Port Reservations are enabled, type a value in the **Conference Size** box for the number of participants.
6. Click **Create**. Make a note of the resulting participant and leader access codes for this user.

25.7 Add a Delegate

A delegate is a user who can view and create conferences and change another user's call schedule. Delegates are often administrative assistants, but they may be any registered user on the system.

To assign a delegate:

1. Select the user account that you want to assign a delegate. To select a user, refer to Administer User.
2. Click **Add a Delegate**.
3. Type the delegate's user name, and then click **Assign**. The user name must be in a valid e-mail format, for example name@host.com.

25.8 Support for Apostrophes

The following support is provided for apostrophes in e-mail addresses and Login IDs:

- You can
  - import users with apostrophes in e-mail addresses or Login IDs from Active Directory into the MiCollab Users and Services directory
  - add users with apostrophes in e-mail addresses and Login IDs from MiCollab Users and Services
  - add users with apostrophes in e-mail addresses from the AWV admin portal
  - manage the users from the administration portal.
- If users are imported from User and Services containing AWV services, users that have an apostrophe in their user name or e-mail address can log into their End User portal and manage their conferences.
- If users are imported into the AWV administration portal, added manually, or added via LDAP, then those users that have an apostrophe in their e-mail address are not able to login to their End User portal. Note that this deficiency will be corrected in a future release.
- Users with an apostrophe in the user name or e-mail address are able to use AWV features and functionality with the following exceptions (these exceptions are targeted to be removed in MiCollab Release 7.3 and later):
  - Users cannot look up personal IDs with e-mail from the conference URL page.
  - Users who join a conference as a web client by entering name in the conference URL page cannot have an apostrophe in the entered name. AWV allows them to join with the apostrophe in the name. The name will be truncated.
  - Users cannot configure AWV PC launcher with ‘Display name’ as the option if an apostrophe is in the name.
  - Users that join a conference where a personal ID is required are allowed to join with an apostrophe in the name. The name will be truncated.
  - From the End User Portal, clicking the **Join** link to join a conference directly is not supported.
  - From the End User Portal,changing the display name from **Settings > Personal ID** is not supported.
- Users with an apostrophe in their e-mail address or login ID can schedule conferences and join conferences if they configure them under **Options** in the AWV PC Launcher.

25.9 List Users

To view the list user accounts:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **List Users** in the navigation pane.
2. The User List page appears that displays all of the currently configured system and guest users defined within the database.
3. **System Users**: Displays a list of all system users including their Display Name, User Name Phone Number and Personal ID

4. **Guest Users**: Displays a list of guest users including their Display Name, Personal ID, Email address, Date when ID was created, conference ID of the Last Conference attended and well as the Total number of conferences attended.

> **Note**:
> If the guest user leaves and rejoins the same conference without switching to another conference during a 24 hour period, the total number of conferences does not increase each time the guest user rejoins the same conference.

5. Select a user from the list by clicking their name. A page appears that allows you to select user settings to modify. For details about user settings, refer to Administer User.

25.10 Bulk Provision Users

> **Note**:
> Although you can bulk provision from MiCollab Audio, Web and Video Conferencing administration, Mitel recommends configuring Bulk User provisioning from the MiCollab administrator interface.

To bulk provision/modify user accounts:

The bulk-provision feature is used to create multiple user accounts in a single step. Also, when users are created in this manner, a reservationless conference can be created for each user as well. The account and optional reservationless conference information is read from an ASCII text, comma-separated values (.csv) file that you prepare in advance. Each user is represented by one line in the file. Refer to the notes provided on the page about the format of the bulk provision file for instructions to assemble the file.

> **Note**:
> To import entries containing ISO-8859-1 characters, you must import them from a CSV file that supports UTF-8 encoding. Use an editor (for example, Notepad++) that supports UTF-8 encoding to create the CSV file. Do not use Excel to edit the file. Excel does not display ISO-8859-1 characters properly in CSV files, even if the encoding is set to UTF-8.

Note:
The Bulk Provision Users option does not appear in the navigation pane when Use LDAP is set.

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Bulk Provision Users** in the navigation pane.
2. Click **Browse** to locate the .csv file with the user information you created previously.
3. Indicate if you want to encrypt passwords, and then click **Process File**. The status of the creation of each user (and their optional reservationless conferences) is displayed.

25.11 Bulk Provision Reservationless Conferences

As the administrator, you can set up reservationless conferences for MiCollab Audio, Web and Video Conferencing users. If the reservationless conference is configured, users do not need to set up their own conferences using their Web client interface.

If Custom Access Codes have been enabled on the System Options page, you can create access codes for both the leader and participants in the conferences. If Custom Access Codes have not been enabled, the bulk provisioning process lets you select a participant access code, which must be seven digits and start with 01. If you specify the participant access code, the corresponding leader access code is automatically generated. If you do not specify either a leader or participant code, the codes are automatically generated.

In either case, the process is performed using a text file, in .csv format. The file must have a header line as the first line of the file, or it will be rejected. Each line starts with a registered username, and (if selected) a desired participant access code. If Custom Access Codes have been enabled, the leader access code is also included, as the last parameter. This file needs to be prepared in advance using standard editing tools or a spreadsheet that you can save in .csv format (for example, Microsoft® Excel®). Refer to the notes on the Web page about the format of bulk provision file.

To bulk provision reservationless conferences:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Bulk Provision Reservationless Conferences** in the navigation pane.
2. Select the file you want to process by entering the path and file name or click **Browse** to navigate to the file, and then click **Process File**.

After the file has been selected and processed, go to Downloading Reservationless Conferences to retrieve the resulting leader/participant access code pairs.

Note:
To inform users of their pre-assigned leader and participant access codes, you need to retrieve the complete list of all users' participant and leader access codes by selecting **Download Reservationless Conferences** on the MiCollab Audio, Web and Video Conferencing main page.

Note:
If Custom Access Codes have been enabled, the access codes for both the leader and participants are provided. If Custom Access Codes have not been enabled, the access code provided here is the "participant" access code. MiCollab Audio, Web and Video Conferencing automatically creates the "leader" access code. To inform users of their pre assigned leader and participant access codes, you need to retrieve the complete list of all users' participant and leader access codes.

25.12 Default User Settings

When initially provisioned, all users are given the same set of user settings and permissions. You can change these default user settings for all users on the system.

To view or edit the default user settings:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Default User Settings** in the navigation pane.
2. Set the following options:

- **Dial Out Allowed**: Indicates this user can dial out to others using the system (CO call). Default setting is enabled.
- **Deny Multiple Leaders**: Indicates this user may not have multiple callers as the conference leader. When selected, only the first person that enters the leader access code is the conference leader. Subsequent users that enter the leader access code will join the conference as a participant. The default setting is cleared.
- **Conference Settings**: Select from the following three options:
  - *Reservationless calls allowed, leader not required*: Users can make reservationless calls and a leader code is not required to access the call. This is the default setting.
  - *Reservationless calls allowed, leader required*: Users can make reservationless calls, but a leader code is required to access the call.
  - *Reservationless calls not allowed*: Users cannot make reservationless calls.

Note:
To preserve ports on the server for one-time and recurring conferences, Mitel recommends that you select **Reservationless Calls Not Allowed** when you select Enable Port Reservations. Ensure the **Allow user to schedule conference if conflict occurs** option is **not** selected under Port Reservations.

- **Maximum Length of Reservationless and Recurring Conferences**: Indicates this is the number of weeks in which these conference types can occur. The default setting is 26 weeks. The maximum length for reservationless and recurring conferences is 156 weeks.
- **Invitation Handler**: Select either of the following e-mail invitation types:
  - *Default Programs*: Use this setting for Microsoft Outlook users (or any other application that supports ICS files). Note that although other third-party clients may be compatible, only Microsoft Outlook is officially supported.
  - *Google*: Use this setting for calendar entries composed via Google Calendar and e-mail handled via Gmail.

Note:
This setting defaults to Default Programs and should be changed only for installations where the majority of users use Google Calendar and Gmail.

- **Invitation Length**: Select either of the following e-mail invitation length:
  - Generic Long: Use this setting for e-mail clients (for example, Microsoft® Outlook®) that allow for long form inserts (usually more than one line).
  - Generic Short: Use this setting for e-mail clients that only allow short form inserts (usually one line).

3. To restore the original defaults at any time, click **Restore Original Defaults**, then click **Ok** at the prompt. If the defaults are changed, users who were set up in the system before the change are not affected.

Note:
If the defaults are changed, users who were set up in the system before the change are not affected.

To restore all users to the new system defaults, click **Restore All Users to Defaults**. Any individual settings that differ from the defaults will need to be reapplied as described in Managing a User Profile.

4. Click **Save Changes**, and then click **Ok** at the prompt.

25.13 Broadcast Email

The Broadcast Email option sends an e-mail message to all the users and administrators with MiCollab Audio, Web and Video Conferencing accounts.

To Broadcast Email:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Broadcast Email** in the navigation pane.
2. Enter **Subject** and **Message**, and then click **Send Email**.

25.14 Billing Codes

The Billing Code feature allows an administrator to create billing codes and set the feature as required for a user to schedule a meeting. There are two areas on the page, Department Code and Project Code. The following options are available for both department and project codes and apply system wide for all users.

Note:
Billing codes are not supported for MiTeam and Ad-hoc meeting. Do not enable billing codes for creating MiTeam and Ad-hoc meeting.

- **Required**: When selected for Department Code or Project Code, then the user is required to choose a billing code from the list when scheduling a meeting. If cleared and billing codes exist, the user is given the option to select a billing code when scheduling a meeting.
- **Allow "None" Option**: When selected for Department Code or Project Code, then None appears at the top in the billing code list as a selectable option.

To add a billing code:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Billing Codes** in the navigation pane.
2. The Billings Codes page appears. This page has two areas, **Department Code** and **Project Code**, where you can create new billing codes for each. Type a department or project code, and then click **Add**.

To delete a billing code:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Billing Codes** in the navigation pane.

2. Select the department or project code (s) to delete, and then click **Delete**.
3. Click **Ok** at the prompt to confirm.

25.15 Active Calls

The system allows you to view information about conferences that are in progress. The call information page is updated according to the refresh rate that is selected at the top of the screen. The default refresh rate is every 30 seconds.

View active conference calls

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Active Calls** from the navigation pane. The page shows a conference call in progress and the participants.
2. While monitoring live conferences, you can perform the following operations:

   - **End Call**: Ends the conference without any warning or notice to conference participants.
   - **Drop Leg**: Drops this participant from the conference without any warning or notice to the participant.
   - **Collect Call Quality Data**: Collects call quality data for support purposes. The call must active for at least one minute or no data is collected.

     a. Click **Collect Call Quality Data** link for the conference that you want to collect call quality information. The call must be up for one minute or no data is collected.
     b. Click **DownloadDataCapture** option.
     c. At the prompt, click **Save**, and then choose a location to save the file.

Analyze call quality data

For Wireshark versions 1.0 and 1.1:

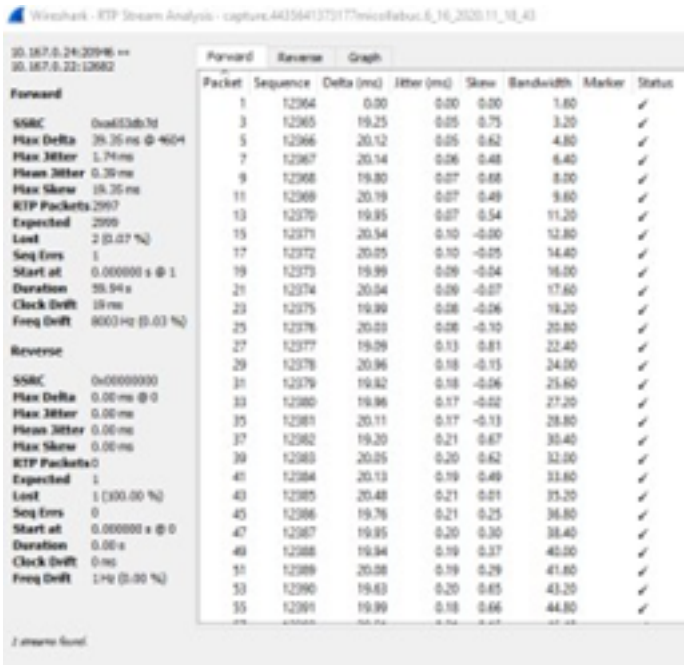
1. Unzip the downloaded call quality data file.
2. Two types (**info file** and a **monitor file**) of files are captured in thecall quality datafile. Open the **monitor file** in Wireshark.
3. Wireshark will show the trace as UDP. To convert UDP trace to RTP:

   a. Right-click a packet and select **Decode As**.
   b. Set to **RTP.**

   Perform the above procedure for the reverse stream also.

4. Once all packets are displayed as RTP, select **Telephony** > **RTP>Stream Analysis**.

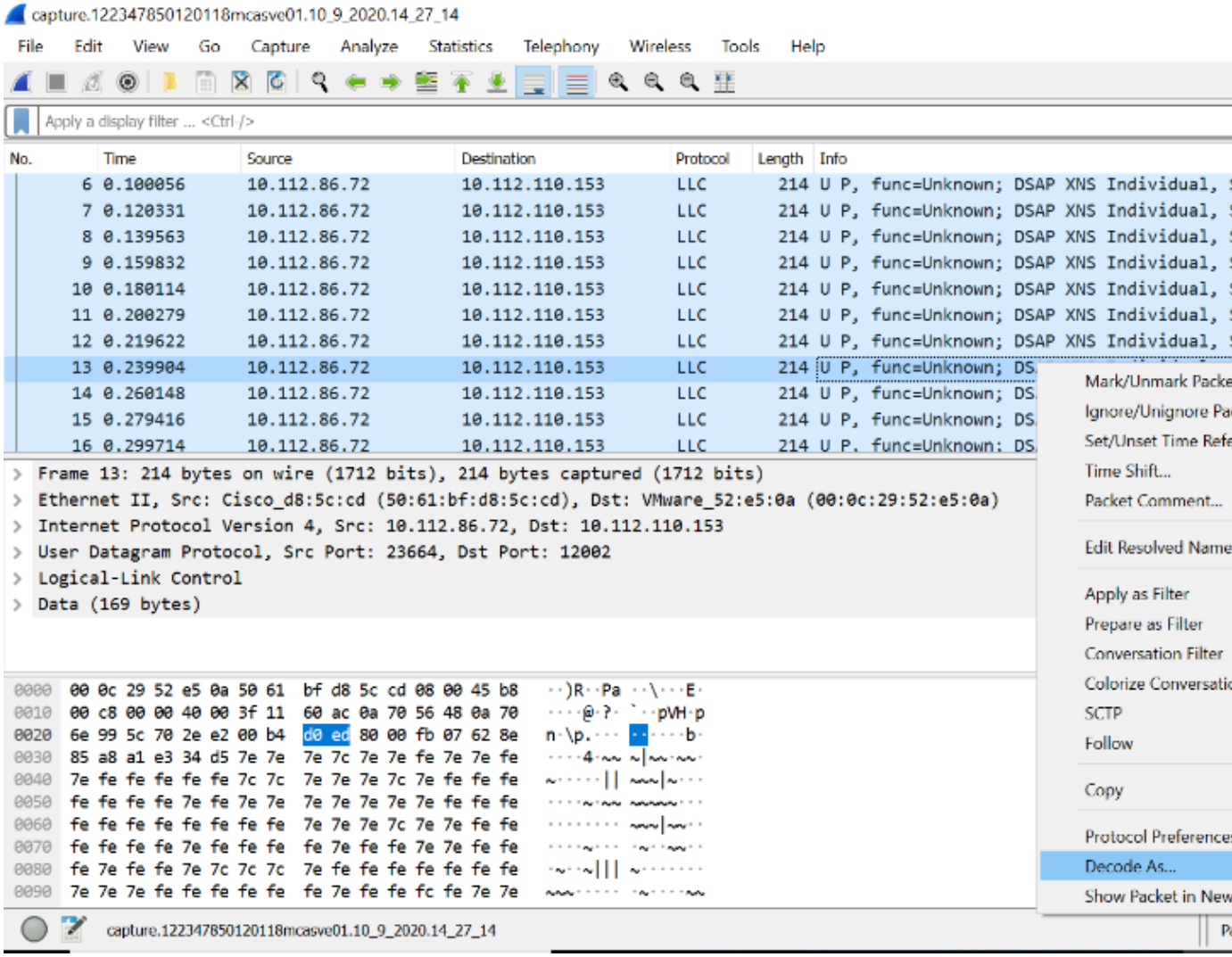
   VQ analysis with Jitter and bandwidth data is displayed.



For Wireshark version 3.2.2:

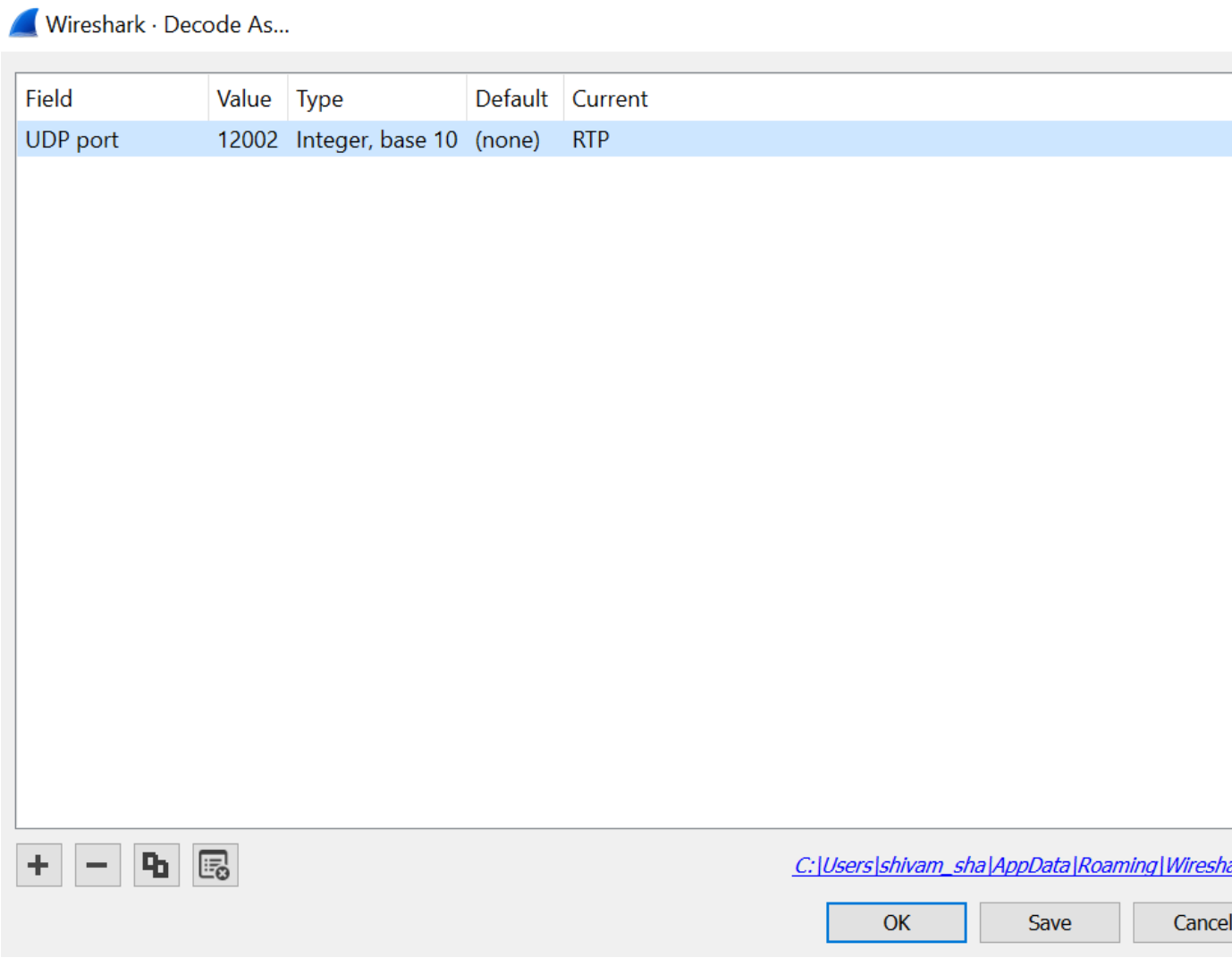
Use the following procedure to decode UDP packet into RTP.

1. Wireshark will show the trace as UDP. We need to convert this into RTP, right click on a packet and select decode as option.



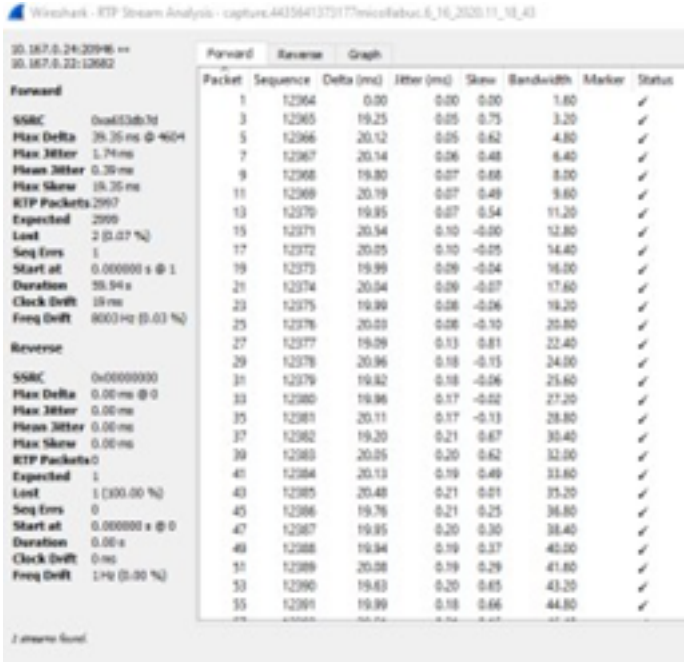
2. **Decode As** window prompt will open. Set the following options to decode the packet in RTP and select **OK**:

   - **Field**: UDP Port
   - **Value**: 12002 Port Number(DST Port)
   - **Type**: Integer, base 10
   - **Default**: none
   - **Current**: RTP



3. Once all packets are displayed as RTP select **Telephony** > **RTP>Stream Analysis**.

4. This will then open a VQ analysis which shows Jitter and bandwidth.



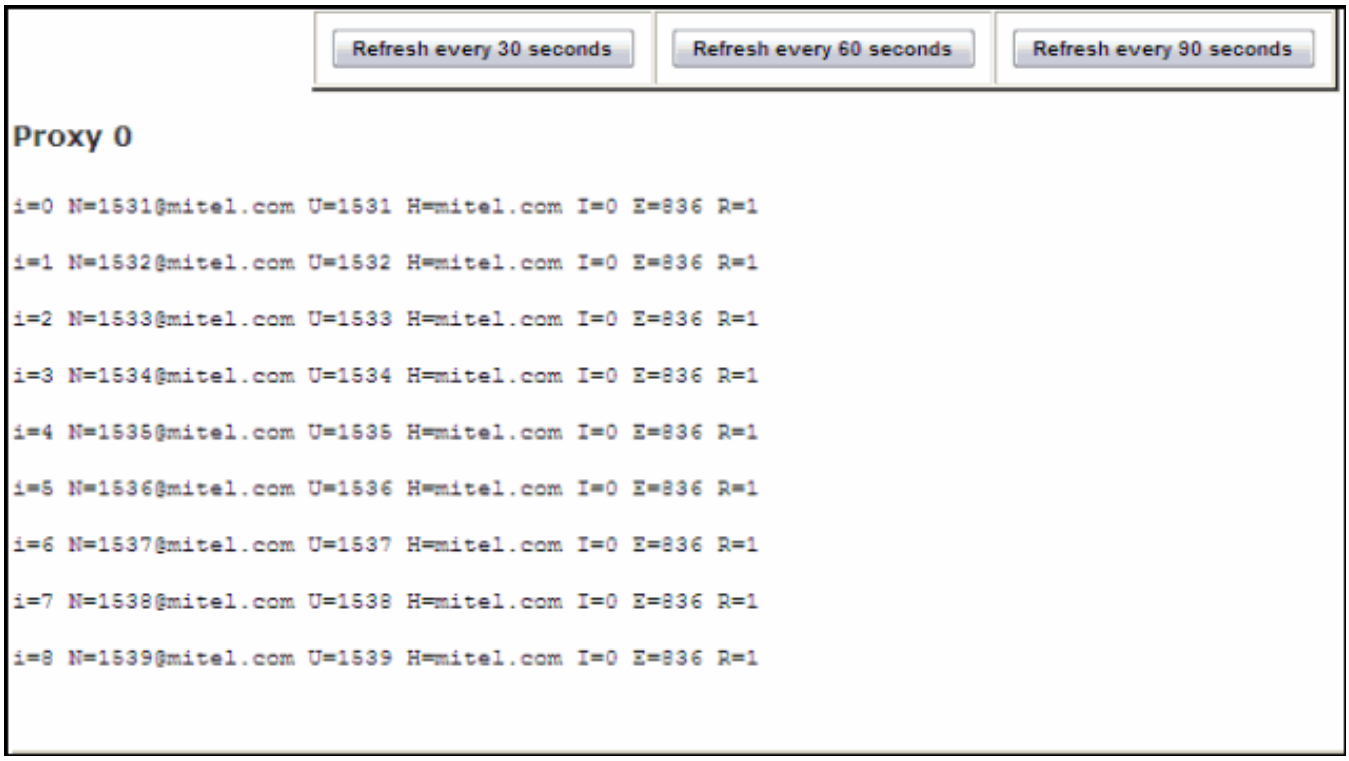
25.16 Proxy Extension Status

The Proxy Extension Status page provides connection status of the server registration process. The information on this page is updated according to the refresh rate that is selected at the top of the screen. The default refresh rate is every 30 seconds.

To view the proxy extension status:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Proxy Extension Status** in the navigation pane.
2. Depending on the platform you selected, do one of the following:

For a MiVoice Office 250:



Example results:

The columns display the following information:

- **i**: The proxy entry number (starts at 0 and increases)
- **N**: The extension entry number
- **U**: The username (in most cases this will be the extension number)
- **H**: The domain
- **I**: The in-use flag (1 for in use, 0 for not used)
- **E**: The expire time (when e becomes 0, the server will re-register)
- **R**: The registration status (when it is 1, the server has properly registered. 0 or -1 indicates the server has not properly registered)

For a Mitel 3300, MiCollab Audio, Web and Video Conferencing registers itself with the Mitel 3300 as a single device based on the settings in Configuring SIP Server. The Proxy Extension Status page displays the results of this registration process. Because this registration process happens often (about every 30 minutes), only the last attempt is displayed. An explanation of the Proxy Extension Status page results follows the example below.

Example.

```
Apr  2 15:55:35.756948 Sending to UDP_CH socket (10.0.0.198:5060):
REGISTER sip:icp3300.linktivity.lab SIP/2.0
Via: SIP/2.0/UDP 10.0.0.74:5064
Call-ID: 843296448@awc2
CSeq: 1 REGISTER
From: <sip:7002@icp3300.linktivity.lab>;tag=764313295
To: <sip:7002@icp3300.linktivity.lab>
Contact: <sip:10.0.0.74:5064>;methods="INVITE, SUBSCRIBE, BYE, CANCEL, ACK"
Expires: 3600
User-Agent: Mitel-AWC/3.5
Content-Length: 0

Apr  2 15:55:35.777764 Received UDP message from socket 7 (UDP_CH 10.0.0.198:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.0.0.74:5064 ;received=10.0.0.198:5060
Call-ID: 843296447@awc2
CSeq: 1 REGISTER
From: <sip:7001@icp3300.linktivity.lab>;tag=764313294
To: <sip:7001@icp3300.linktivity.lab>;tag=0_3939248944-60431496
Content-Length: 0

Apr  2 15:55:35.786984 Received UDP message from socket 7 (UDP_CH 10.0.0.198:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.0.0.74:5064 ;received=10.0.0.198:5060
Call-ID: 843296448@awc2
CSeq: 1 REGISTER
From: <sip:7002@icp3300.linktivity.lab>;tag=764313295
To: <sip:7002@icp3300.linktivity.lab>;tag=0_3939258944-60431497
Content-Length: 0

Apr  2 15:55:35.790258 Received UDP message from socket 7 (UDP_CH 10.0.0.198:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.0.0.74:5064 ;received=10.0.0.198:5060
Call-ID: 843296447@awc2
CSeq: 1 REGISTER
From: <sip:7001@icp3300.linktivity.lab>;tag=764313294
To: <sip:7001@icp3300.linktivity.lab>;tag=0_3939248944-60431496
Contact: sip:10.0.0.74:5064
User-Agent: Mitel-3300-ICP 8.0.9.18
Allow: INVITE,BYE,CANCEL,ACK,INFO,PRACK,OPTIONS,SUBSCRIBE,NOTIFY,REFER,REGIST
Date: Wed, 02 Apr 2008 15:55:42 GMT
Content-Length: 0

Apr  2 15:55:35.795739 Received UDP message from socket 7 (UDP_CH 10.0.0.198:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.0.0.74:5064 ;received=10.0.0.198:5060
Call-ID: 843296448@awc2
CSeq: 1 REGISTER
```

Example results:

- MiCollab Audio, Web and Video Conferencing sends a REGISTER message to icp3300 indicating that it would like to register itself as a particular endpoint, in this case7002@linktivity.lab:

  Apr 2 15:55:35.756948 Sending to UDP_CH socket (10.0.0.198:5060):

  REGISTER sip:icp3300.linktivity.lab SIP/2.0

  Via: SIP/2.0/UDP 10.0.0.74:5064

  Call-ID: 843296448@awc2

  CSeq: 1 REGISTER

  From: <sip:7002@icp3300.linktivity.lab>;tag=764313295

  To: <sip:7002@icp3300.linktivity.lab>

  Contact: <sip:10.0.0.74:5064>;methods="INVITE, SUBSCRIBE, BYE, CANCEL, ACK"

  Expires: 3600

  User-Agent: Mitel-AWC/3.5

  Content-Length: 0
- The Mitel 3300 receives this message and lets MiCollab Audio, Web and Video Conferencing know that it is now trying to authenticate the user:

  Apr 2 15:55:35.777764 Received UDP message from socket 7 (UDP_CH 10.0.0.198:5060):

  SIP/2.0 100 Trying

  Via: SIP/2.0/UDP 10.0.0.74:5064 ;received=10.0.0.198:5060

  Call-ID: 843296447@awc2

  CSeq: 1 REGISTER

  From: <sip:7001@icp3300.linktivity.lab>;tag=764313294

  To: <sip:7001@icp3300.linktivity.lab>;tag=0_3939248944-60431496

  Content-Length: 0

- The Mitel 3300 sends back a message letting MiCollab Audio, Web and Video Conferencing know that the registration was successful (“200 OK”):

  Apr 2 15:55:35.790258 Received UDP message from socket 7 (UDP_CH 10.0.0.198:5060):

  SIP/2.0 200 Ok

  Via: SIP/2.0/UDP 10.0.0.74:5064 ;received=10.0.0.198:5060

  Call-ID: 843296447@awc2

  CSeq: 1 REGISTER

  From: <sip:7001@icp3300.linktivity.lab>;tag=764313294

  To: <sip:7001@icp3300.linktivity.lab>;tag=0_3939248944-60431496

  Contact: sip:10.0.0.74:5064

  User-Agent: Mitel-3300-ICP 8.0.9.18

  Allow:
  INVITE,BYE,CANCEL,ACK,INFO,PRACK,OPTIONS,SUBSCRIBE,NOTIFY,REFER,REGISTER,UPDATE

  Date: Wed, 02 Apr 2008 15:55:42 GMT

  Content-Length: 0

25.17 Manage Published Data

When users create conferences, they have the option to publish them to their Published Area page. In this release, users are required to password protect their published conferences by default. However, in previous releases of the Audio, Web and Video Conferencing application, users could publish conferences without password protection. Without password protection in place, anyone can access the conferences, documents, and recordings that are placed in the Published Area page.

After an upgrade to this release, it is recommended that you "unpublish" all conferences that have been previously created without a password:

1. Under **Monitoring**, click **Manage Published Data**.
2. In the "Conferences Published without a Password" table, click **Unpublish All**. This action removes public access to the conferences, documents, and recordings.
3. To prevent unauthorized access to published conferences, ensure that the **Allow users to publish conference only with password** setting in the System Options page is enabled.

25.18 Manage Recordings

To Manage Recordings:

1. From the MiCollab Audio, Web and Video Conferencing main page, under **Monitoring**, click **Manage Recordings** from the navigation pane. The page shows a listing of Recordings.
2. From here, you can perform the following operations:

   - **Delete**: Manually delete a selected file.
   - **Mark them as permanent:** In this case the recording will never be auto deleted. The only way to delete recordings marked as permanent is for the administrator to select a record and manually delete it from the admin portal. Once a record is marked as permanent, it cannot be changed back to a time limit expiration.
   - **Backup:** This option will provide the admin an option to save files to an external drive.

Note:
You can sort the order of the table presented by clicking on the column header. All the columns are sortable. By default the columns are sorted by the recordings and date with the oldest recordings showing first.

Note:
At the system level, the date stamp against a recording uses the GMT time zone.

The following conditions and limitations apply to recordings:

- The amount of disk space available on the server for MiCollab Audio, Web and Video Conferencing storage, including recordings, is listed on the **System Options** page in the **Email Admin informing when the AWV disk space utilized reaches** field. Recordings are included in the limit (for example: 15.28 GB).
- There is no set time limit on recordings. As long as space is available on the hard drive, a recording can continue.
- The amount of disk space used for a recording depends upon what is being recorded (Share, Video, Chat, Audio and so forth). However, as a rough guideline approximately 100 MB is required for a 10 minute recording that includes Sharing, Audio, with one or two users participating in the video.

25.19 License Usage

To view License Usage:

- From the MiCollab Audio, Web and Video Conferencing main page, under **Monitoring**, click **License Usage** from the navigation pane. The page shows the maximum and current number of licenses in use.
- Options to modify the refresh rate can be set to every 30, 60, or 90 seconds.

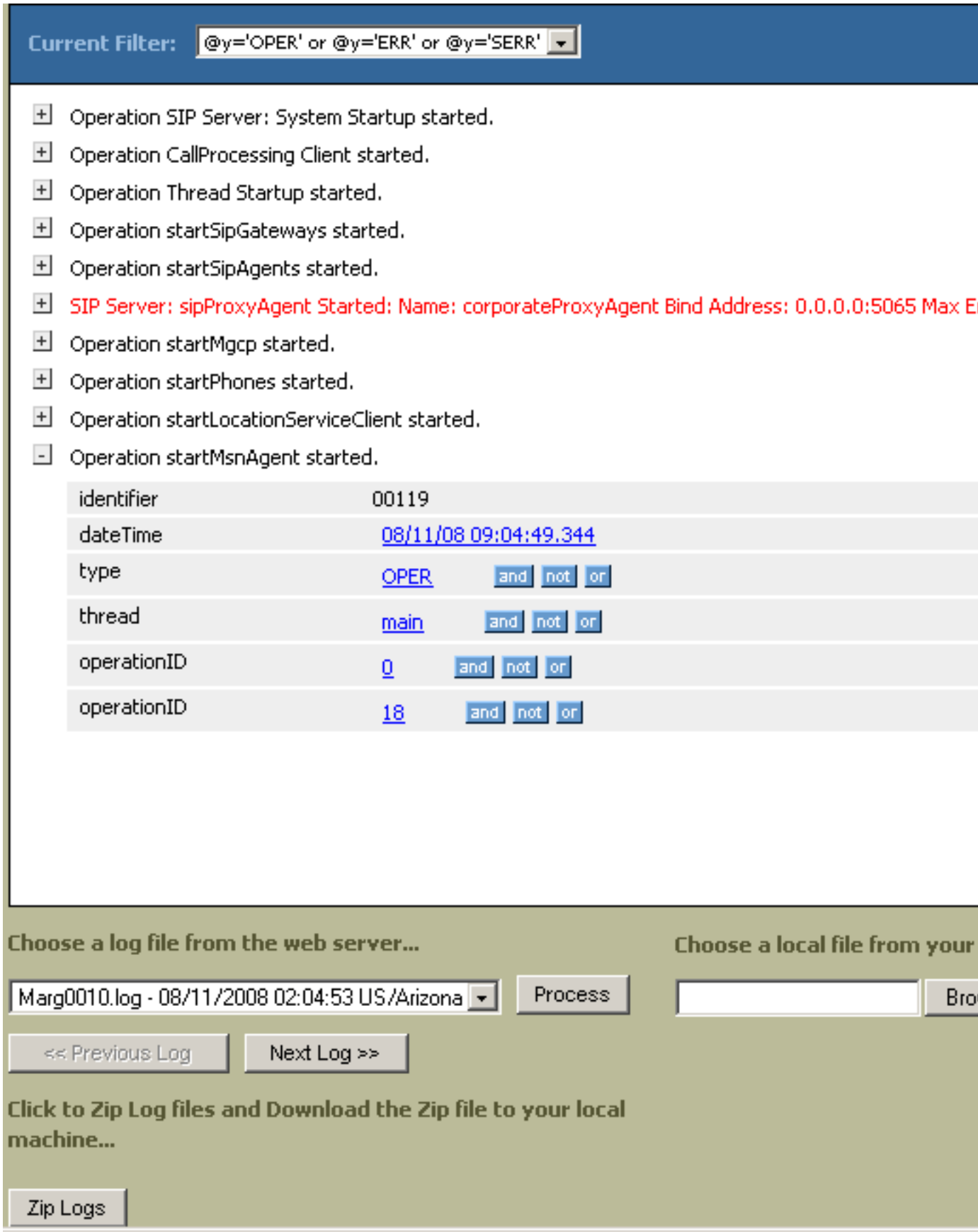
25.20 SIP Logs

Note:
The SIP Logs option appears in the navigation pane only when the MiVoice Office is selected as the platform in System Options. These log files are provided for Technical Support use and are not explained in detail in this section.

This viewer allows you to access SIP Server log information for the Mitel MiVoice Office 250 , and then save them to your computer in .zip file format. You can then use a text file reader (for example, Notepad®) to view the files.

To access SIP Server logs:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **SIP Logs** in the navigation pane. Click here to see an example of the diagnostics screen.


Current Filter:
@y='OPER' or @y='ERR' or @y='SERR'
Operation SIP Server: System Startup started.
Operation CallProcessing Client started.
Operation Thread Startup started.
Operation startSipGateways started.
Operation startSipAgents started.
SIP Server: sipProxyAgent Started: Name: corporateProxyAgent Bind Address: 0.0.0.0:5065 Max E
Operation startMgcp started.
Operation startPhones started.
Operation startLocationServiceClient started.
Operation startMsnAgent started.
identifier 00119
dateTime 08/11/08 09:04:49.344
type OPER and not or
thread main and not or
operationID 0 and not or
operationID 18 and not or
Choose a log file from the web server...
Choose a local file from your
Marg0010.log - 08/11/2008 02:04:53 US/Arizona
Process
<< Previous Log
Next Log >>
Click to Zip Log files and Download the Zip file to your local machine...
Zip Logs

2. Do one of the following:

   - *To view a log file*, select a file from the drop-down list, and then click **Process**. You can also click **Next Log >>** or **<< Previous Log** to select a log file.
   - *To view a log file on your computer,* click **Browse**, navigate to the log file location, and then double-click the file. Click **Process**.

   Note:
   Using this option may require you to change IE security settings when trying to view a file locally through the Web interface.

   - To zip the log files and download them, click Zip Logs. Click the blue Download Zip File link, and then save the file to your computer. The default file name is `ZipLogs.zip`. Trace logs are also included with the zipped files.

25.21 Call Activity Reports

From the Call Activity Reports page, you can view daily usage statistics to track server usage and system conferencing information.

To view activity reports:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Call Activity Reports** in the navigation pane. The Call Activity Report screen opens.
2. Do one of the following and determine a date range for the report you want to create.

   - Select a value from the **Date Range** list.
     - **Today**: Today's date
     - **Yesterday**: Yesterday's date
     - **This Week**: Sunday of the current week through today's date
     - **Last Week**: Sunday of last week through the Saturday of last week
     - **This Month**: First day of the month through today's date
     - **Last Month**: First day of last month through the last day of last month
     - **This Quarter**: First day of this quarter (1/1, 4/1, 7/1, or 10/1) through today's date
     - **Last Quarter**: First day of last quarter (1/1, 4/1, 7/1, or 10/1) through the last day of last quarter
   - Click one of the shortcut buttons: **Select Today**, **Select This Week**, or **Select This Month**. (The shortcut button selected is displayed in the Date Range box.)
   - Select a date range using the **Start Date/Time** and **End Date/Time** lists.
3. Type a project code or department code to view only system usage associated with the code entered.
4. Select a user or multiple users from the list to include in the report.
5. Select an item from the **Sort By** list to determine how you want the report to appear.

6. Select a format, either a **Web Report** (default) or a **CSV Report**, and then click **View**.

   - *If you select Web Report for the format*, the results are displayed on the screen.
   - *If you select CSV Report for the format*, click **Save** at the prompt to save the file to a location or click **Open** to display the results in your default text editor (for example, Microsoft® Excel).

25.22 VoIP Utilization Statistics

The VoIP utilization graph displays the VoIP port usage on MiCollab Audio, Web and Video Conferencing for the date and time range you select. A bar chart is displayed that provides both the number of ports and the number of port seconds for the time increment you select. This is useful for monitoring capacity utilization of the server over time.

To check VoIP utilization statistics:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **VoIP Utilization Statistics** in the navigation pane.
2. Select a **Start Date** and **End Date** from the list.
3. Select a **histogram interval** from the list.
4. Click **View** to display the information.

25.23 Scheduled Conferences

Scheduled conferences list calls that are scheduled for the date range specified. Detailed information is listed for each conference.

To view a list of scheduled conferences:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Scheduled Conferences** in the navigation pane.
2. Select a **Start Date** and **End Date** from the list.
3. Click **View** to display the report.

25.24 System Alerts Log

You can view a history of the e-mail notifications that the server has issued for a particular date period. This includes alarms and general notifications that are sent out by the server as a result of events on the system. Typically, the alerts shown in the log are general information and are also available from the View log file page on the MiCollab server.

To view the system alerts log:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **System Alerts Log** in the navigation pane.
2. Select a **Start Date** and **End Date** from the list.
3. Click **View** to display the report.

25.25 Install History Log

You can view a history of the server software installs that have been completed during the selected period.

To view the installation history log:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Install History Log** in the navigation pane.
2. Select a **Start Date** and **End Date** from the list.
3. Select the **Package Type** from the drop-down list or leave it as **All** (default) to view the entire list.
4. Click **View** to display the installation history log.

25.26 Port Reservations Report

The Port Reservations Report is available only if Port Reservations is selected. This report allows you to review past and future port usage for possible port conflicts.

To view Port Reservations:

1. From the MiCollab Audio, Web and Video Conferencing main page, click **Port Reservations** in the navigation pane.
2. Select a **Start Date** and **End Date** from the list.
3. (*optional*) Type a user name.
4. Click **View**. The report is displayed on the page.

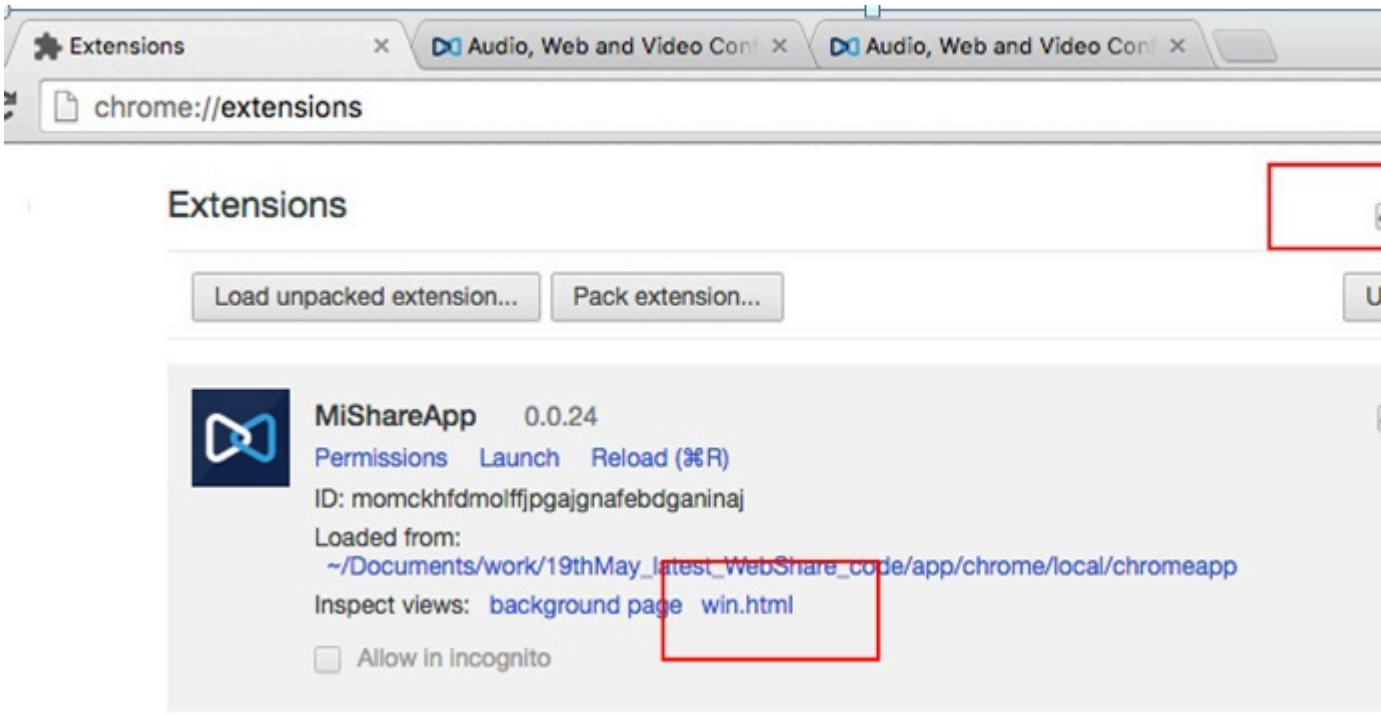
Note:
You can click a name from the report list to send an e-mail to that user. This feature allows you to notify a user when there is a potential port conflict for a scheduled conference.

25.27 Downloading Web Sharing Logs

The AWV Web sharing client collects logs within each user's Chrome browser. If a user is experiencing web sharing issues, you can send the logs to Mitel product support to help them troubleshoot.

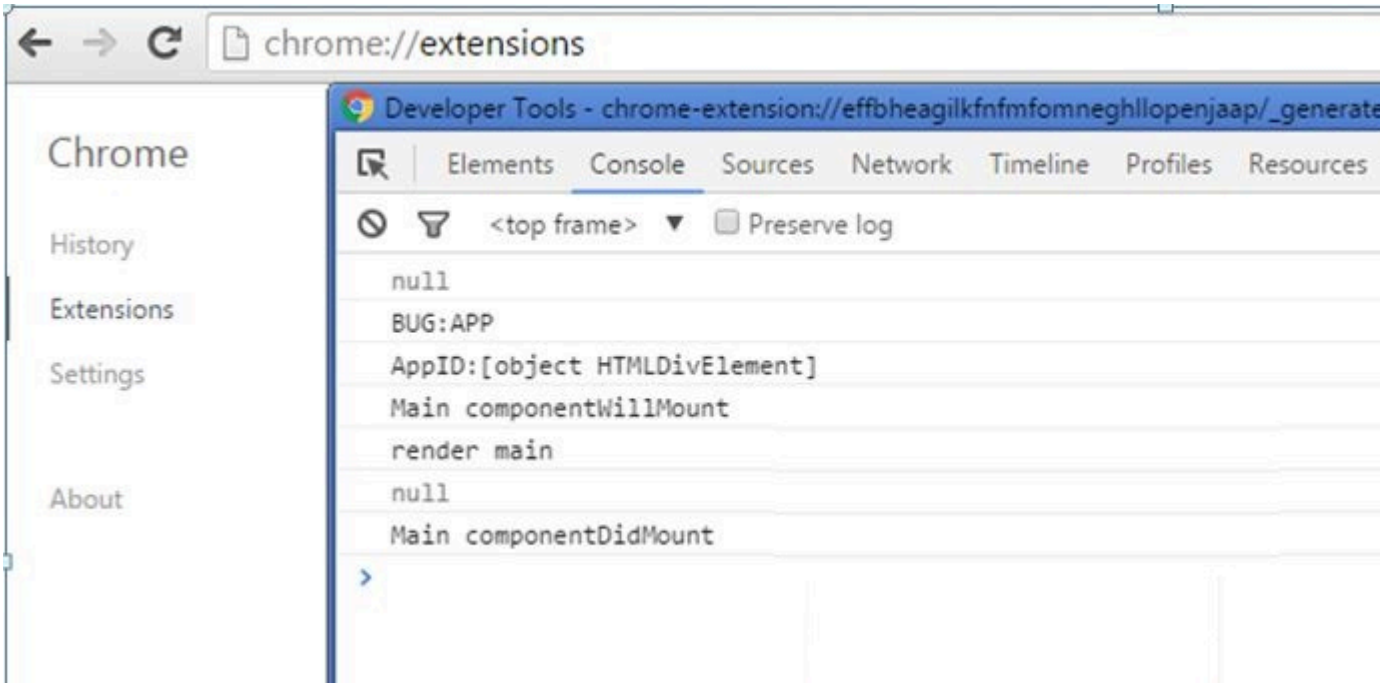
To collect the logs, a user performs the following steps. This procedure is also documented in the AWV end-user online help:

1. In your Google Chrome tool bar, click .
2. Click **Settings** and then click **Extensions**. The Extensions tab is displayed.
3. Check the **Developer Mode** box in the upper right area of the page.
4. Open the AWV web client in a new Chrome tab and click the **Share** button.
5. Return to the Extensions tab and scroll down to **MiShareApp**.



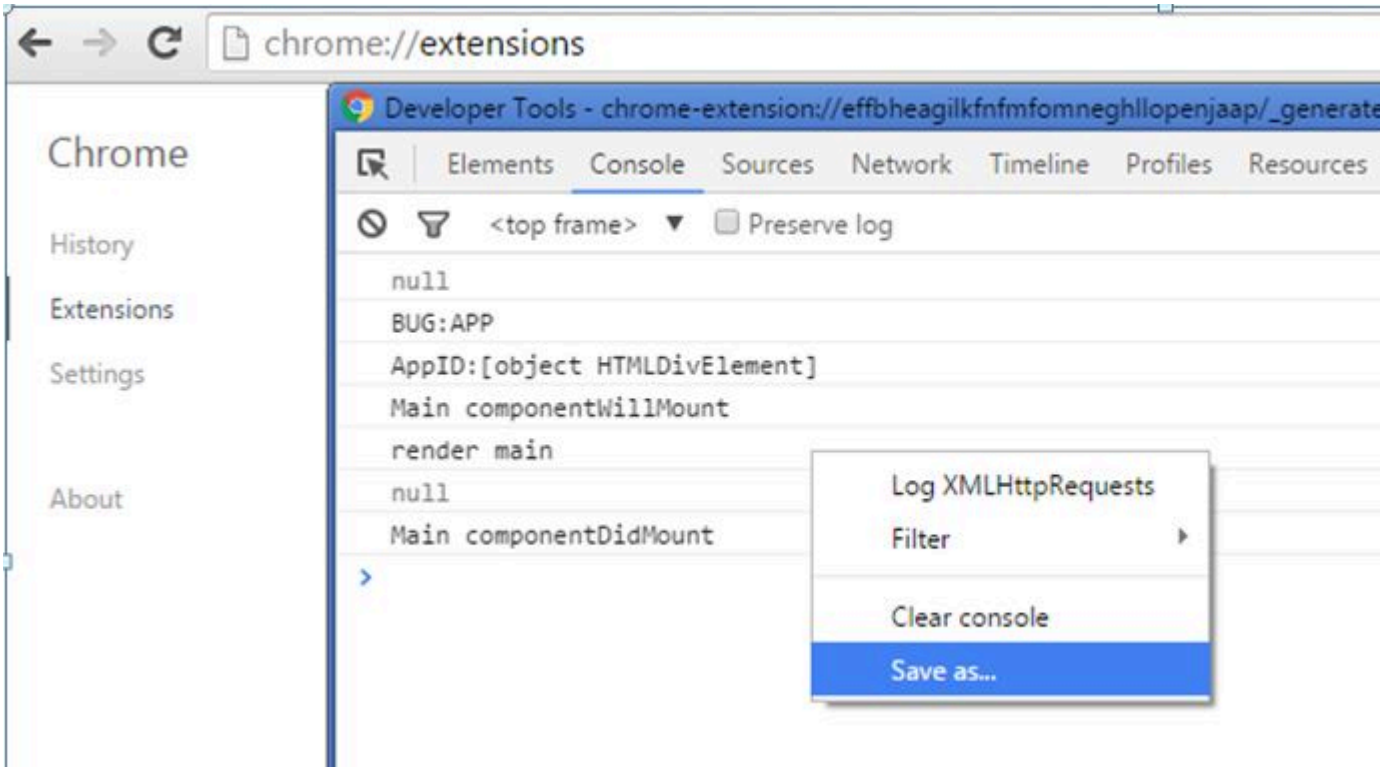
6. Click win.dita. The Developer Tools window opens.

Note:
The win.dita. link will only be available if you have started sharing from the AWV web client page.



7. Run the AWV web sharing scenario for which logs are required. Do not stop or cancel sharing during the log collection scenario. If you do, the developer tools window closes, the logs are deleted, and the win.dita link will not be present in the Extension tab.

8. After the AWV web sharing scenario is complete, return to the Developer Tools window, right-click in the window and select **Save as**.



9. Navigate to a folder on your PC.
10. Enter a filename for the log file in the following format: "MiShare_Logs_<date><your name>.txt" (for example: "MiShare_Logs_jan3_2016_steve.txt").
11. Leave “All Files” for the "Save as type" option.
12. Click **Save**.
13. Attach the log file to an email and send it your administrator.

After you receive the log file from the user, email it to Mitel product support with a description of the issue.

About NuPoint Unified Messaging (For on-premise deployments only) 26

This chapter contains the following sections:

- About the NuPoint UM Documentation Suite
- About this Help System
- Searching the Online Help
- What's New in This Release
- Accessing Documentation, Release Notes, Articles, and Downloads
- Searching the Online Help
- Documentation Conventions
- Contacting Technical Support
- Overview
- The Web Console
- The Text Console
- Console Capabilities
- Frequently Used Procedures
- Introduction
- About Configuration
- About Network Elements
- What is a Mailbox?
- Mailbox Configuration Summary
- Distribution List Configuration
- Record Company Greetings
- Managing Mailboxes
- Mailbox Parameters - Text Console
- Schedule Company Greetings
- Overview
- Overview
- Feature Bits by Category - Overview
- Feature Bits 001 to 049
- Other Classes of Service - Overview
- Group Class of Service - Overview
- Restriction Class of Service - Overview
- Managing TCOS
- Description - NuPoint Voice Application
- Default Configuration Settings
- Dial-by-Name
- Dial-Back
- NuPoint Voice Application Programming - Task List
- Configure a Dialing Plan
- Transfer to System Attendant
- Prevent Unaddressed Messages

- Enable the Dial by Name Function
- Configure Media Service (Packet Rate)
- Verify Configuration Parameters
- Define a Line Group
- Add Caller ID to Voice Mail Headers
- Description
- Testing Overview
- Configure External Applications
- Descriptions
- MiVoice Business ICP Programming for MiTAI MWI
- Introduction
- Worksheets Index
- Overview
- Hard Disk Utilities
- Change Text Console Password
- Set System Time and Date
- Lights Test
- Enable Alarm Management
- Perform System Shutdown and Startup
- Adjust Audio Stream
- Security - Overview
- List of Current Users
- List of Authorized Users
- Start or Stop an Audit Trail
- Functionally Partitioned System Administration
- Log In or Log Out of the Web Console
- Change a Password
- Change Text Console Password
- Display Administrator Privileges
- Overview
- Gathering Data
- Check Current Billing Rates
- Overview
- Overview - Statistics Reporting
- Overview - Billing Reports
- Overview
- Overview
- Installing an Optional Feature
- Direct Drop Overview
- About Call Detail Recorder
- Processing Each Call Type
- Hacker Detection
- Description
- Competitive TUI Emulation - Description
- Cut-Through Paging - Description

- Overview - Language Prompts
- Overview
- Overview
- Overview
- Introduction
- Description
- Introduction
- About NP Net TCP/IP
- Network Node Table - Introduction
- Configuring Network Addressing - Overview
- Configuring Network Mailboxes
- NP OnDemand - Description
- NP RapidDial - Description
- NP Receptionist - Description
- Dialing Plan Options
- Flow Options
- PBX Dial String Definitions
- What is a Treatment Type?
- About NP Receptionist Worksheets
- NP WakeUp - Description
- NP WakeUp - User Interface
- Call Records
- Overview of PMS Integrations
- EECO Troubleshooting Guide
- Description
- SMS Notification (UK Only) - Description
- About Current Users
- About Departments
- About Prompts
- About Dialing Policies
- About Miscellaneous Parameters
- Custom Pronunciations
- Troubleshooting SAA Name Recognition Problems
- Install Active Directory (AD) Snap-in
- Presence Overview
- SAA Backup and Restore
- Troubleshooting
- Speech to Text - Description
- Speech Navigation - Description
- Unified Messaging - Description
- Basic Unified Messaging Features
- Optional Unified Messaging Features
- Configure IMAP Server Settings for Exchange or Office 365
- Configure a Superuser Account for Office 365
- Create a Superuser Account for Microsoft Exchange 2016 or 2019

- Troubleshooting Notes for IMAP for Exchange or Office 365
- Configure IMAP Server Settings for Google Apps
- Configure Advanced UM Parameters
- Configure Text to Speech
- Configure Advanced UM Parameters
- Configure Text to Speech
- Force Manual License Update
- Enable Advanced UM for User Mailbox
- Troubleshooting Standard UM
- Visual Voice Mail Support
- VPIM - Description
- Web View - Description
- MiVoice Office 250 Integration Overview
- About Call Director
- About the NuPoint UM Documentation Suite
- What's New in This Release
- About the Call Flow Page
- About the Configuration Page
- Finding online Help Quickly
- Accessing Documentation, Release Notes, Articles, and Downloads
- Contacting Mitel
- Disclaimer, Trademarks, Copyright
- Personal Call Flow Example
- Corporate Call Flow Example - Main Auto Attendant
- System Templates
- Voicemail RADs
- Tutorials
- Override
- Schedule
- Message
- Menu
- Call Transfers
- Voicemail
- Dial-by-Name
- Internal/External Call Handling
- Caller ID Filter
- Daily Greeting
- Message Center
- Language Router
- Call Flow Authoring Procedures - Overview
- Starting with a template
- Adding an action
- Deleting an action
- Reusing an action
- Copying a call flow

- Deleting a call flow
- Inserting an action
- Setting action properties
- Setting the prompt language
- Recording and Importing Messages
- Viewing call flow paths
- Printing call flows
- Call Flow Authoring Procedures - Overview
- Starting with a template
- Adding an action
- Deleting an action
- Reusing an action
- Copying a call flow
- Deleting a call flow
- Inserting an action
- Setting action properties
- Setting the prompt language
- Recording and Importing Messages
- Viewing call flow paths
- Printing call flows
- About Call Director Reports
- About Call Flow Reports
- About MiCollab Client
- Enterprise Tab
- Synchronization Tab
- PBX Nodes Tab
- Accounts Tab
- Corporate Directory Tab
- Collaboration Tab
- Features Tab
- Peering Tab
- Federation Tab
- View Licensing Information

Note:
NuPoint Unified Messaging service is not supported for MiCollab on MiCloud Flex deployments.

Mitel® NuPoint Unified Messaging is a message processing system that provides voice and fax messaging capabilities and personal mailboxes. System administrators create and maintain software files for all mailboxes on the system (the server).

You perform the following functions:

- Create and modify mailboxes
- Delete and reassign mailboxes
- Perform routine maintenance of software files
- Change the system time and date
- Establish system security

Additional administrative responsibilities may include the following activities:

- Bill clients
- Run reports
- Build classes of service
- Establish programming for pagers
- Set up system-wide distribution lists
- Create messages, greetings, and tutorials

This Online Help system contains instructions for performing these functions. Although you can perform many procedures using the telephone, most administration is performed using a system maintenance console (either the Web Console or the Text console).

Note:
NuPoint UM is offered as a standalone product and as an application within MiCollab. For information concerning **NuPoint UM Standalone**, refer to this help system. For information concerning **MiCollab NuPoint UM** (including details concerning the unique features and functions supported in MiCollab), refer to the MiCollab documentation.

26.1 About the NuPoint UM Documentation Suite

To access the NuPoint Unified Messaging guides (in .PDF format) and the System Administration Help file, go to Mitel Document Center and log in. You must be a registered user to access Mitel Online.

The NuPoint UM documentation set includes the following components:

General Audience

- General Information Guide:

This guide includes general information on systems architecture, resiliency, feature descriptions, licensing, and geographic availability and provides an overview of administration and maintenance.

Installers

- Technician's Handbook:

This guide includes information on hardware and software requirements, platforms and configurations, installations, basic maintenance, upgrades, data migration, configuring MSL, and trouble shooting systems and features.

- Engineering Guidelines

This guide includes information on system capacities, system requirements, and network engineering.

Administrators

- **System Administration Help** (includes Call Director for the Administrator):

The help file incudes information on post-installation instructions, system administration and maintenance, configuring and managing NuPoint UM and optional features, and troubleshooting Advanced UM.

End Users

- Web View Help

This Help file includes information on the features that are available to users through the web client interface. It includes configuration information for end user settings and describes unified messaging features.

- Messaging User Guide

This guide includes information on setting up and using voice mailboxes, managing voice and email messages, using PCs to receive and manage messages, and the record-a-call, fax, and speech auto attendant features.

- Call Director Web Help

This help file includes information on configuring automated attendant call flows to handle your calls when you can't answer them personally.

- Mitel TUI Quick Reference Guide

This one-page document explains how to access voice mailboxes and identifies telephone user interface (TUI) main menu options.

Mitel Online

All Mitel product documentation is available at Mitel Document Center.

Accessing Documents and Help Files

1. a. Log in to Mitel OnLine.
   b. Point to **Support** and then click **Product Documentation**.
   c. In the right pane, select **Product Documentation**.
   d. Point to **Messaging** and click **NuPoint Unified Messaging**.
   e. A list of documents intended for System Administrators is displayed. Select a document from the list or select **Show End User Documents** or **Show Archived Documents** to access end user or archived documents.

26.2 About this Help System

This NuPoint Unified Messaging System Administration online help system is intended to help system administrators configure and maintain the NuPoint UM system and features.

Intended Audience

This guide is for system administrators who have completed the NuPoint UM System Administrator course. The Mitel OnLine version provides configuration procedures for both the Web Console and the Text console. The software version provides configuration procedures for the Web Console only.

Note:
In some cases, a procedure may be available only in Text console.

Finding Information

Each application or feature of NuPoint UM has its own section, arranged as follows:

- an **overview** or description of the application/feature and its components
- the **procedures** required to configure the application/feature using the Web console.
- the **procedures** required to configure the application/feature using the Text console

26.3 Searching the Online Help

The purpose of this topic is to help you understand how to optimize your searches so that you can find the information that you are looking for.

Finding Information

The Help system provides you with tabs to find information:

Contents tab	Groups the main topics of the Help system into books. To open a book, click the book. To view a topic, click the topic name.
Index tab	Lists index entries alphabetically. To see more index en tries, type a keyword in the box. Clicking a keyword in the list displays the related topic.
Search tab	Allows you to search the online Help using a particular word or phrase. The online Help system lists all topics that contain your word or phrase. Type the word or p hrase in the box and then press Enter. To view a topic, click the topic name. See Using Advanced Search Tech niques.
Glossary tab	Provides a definition for the terms used in this online Help.

Note:
The Search will not find the phrase "Do Not Disturb". "Not" is a Boolean operator that will initiate a search for the word "do" but not the word "disturb". Use "do disturb" or "DND" to find this term.

Using Advanced Search Techniques

When using the search feature in the online Help, the following techniques can help you narrow your searches for more precise results.

Search for	Example	Results
a single word	page	Topics that contain the word "page" and its grammatical variations, such as pager and paging.
a phrase	auto attendant	The query is equivalent to specifyin g "auto AND attendant," which will f ind topics containing both of the in dividual words.

Boolean operators

The AND, OR, NOT, and NEAR operators enable you to precisely define your search by creating a relationship between search terms. The following table shows how you can use each of these operators. If no operator is specified, AND is used. For example, the query "attendant console programming" (entered without the quotation marks) is equivalent to "attendant AND console AND programming."

Search for	Example	Results
Both terms in the same topic.	attendant AND console	Topics containing both the words "at tendant" and "console".
Either term in a topic	attendant OR console	Topics containing either the word "a ttendant" or the word "console" or b oth.
The first term without the second te rm.	attendant NOT console	Topics containing the word "attendan t" but not the word "console".

Note:
The |, &, and ! characters don't work as Boolean operators (you must use OR, AND, and NOT).

Finding words in a topic

After you have narrowed your word search to a list of topics, click a topic from the list. Each occurrence of the word will be highlighted in yellow in the topic text. Note that only exact matches are highlighted.

Note:
If a Help link is highlighted in yellow as a result of a search, the link may not function until you remove the highlighting by clearing the search results. To clear the search results, search on another word, or by exit the Help.

For large topics, you may find it easier to search for the word in the topic text. To search for a word in a topic:

1. Put your cursor at the top of the topic frame.
2. Type **Ctrl-f**.
3. Enter the word and click **Find Next**.

Linking back to the previously viewed topic

You can go back to the previously viewed topic by clicking the **Back** button in the menu bar or by pressing the **Alt** and **<-** keyboard keys at the same time.

26.4 What's New in This Release

For a list of new functionality, see the MiCollab What's New Guide on the Mitel Customer Documentation site.

26.5 Accessing Documentation, Release Notes, Articles, and Downloads

The following sections detail how to access specific NuPoint UM documents from Mitel Document Center.

Documents and Help Files

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Product Documentation**.
3. Click the **Product Documentation** link.
4. Point to **Messaging** and click **NuPoint Unified Messaging**.
5. A list of documents intended for System Administrators is displayed. Select a document from the list or select **Show End User Documents** or **Show Archived Documents** to access end user or archived documents.

The Qualified Hardware List

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Product Documentation**.
3. Click the **Product Documentation** link.
4. To search for a document, press **CTL + F**.
5. To access the Mitel Standard Linux Qualified Hardware list, type **MSL** in the **CTL + F** search box.

Product Release Notes

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Mitel Knowledge Base**.
3. Click **Mitel Knowledge Base**.
4. In the **Product** list, select **Mitel NuPoint UM IP** (Standard Edition).
5. Under **Article Type**, select **Release Notes** and click **Search**.

Knowledge Base Articles

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Mitel Knowledge Base**.
3. Click **Mitel Knowledge Base**.

4. In the **Product** list, select **Mitel NuPoint UM IP** (Standard Edition).
5. Under **Article Type**, select the type of article to be viewed.
6. Specify other search parameters to narrow your search and click **Search**.

Software Downloads

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Software Downloads**.
3. Select the appropriate Mitel NuPoint UM link.
4. Click the download link for your selected release and follow the instructions on the software download page.

26.6 Searching the Online Help

The purpose of this topic is to help you understand how to optimize your searches so that you can find the information that you are looking for.

Finding Information

The Help system provides you with tabs to find information:

Contents tab	Groups the main topics of the Help system into books. To open a book, click the book. To view a topic, click the topic name.
Index tab	Lists index entries alphabetically. To see more index en tries, type a keyword in the box. Clicking a keyword in the list displays the related topic.
Search tab	Allows you to search the online Help using a particular word or phrase. The online Help system lists all topics that contain your word or phrase. Type the word or p hrase in the box and then press Enter. To view a topic, click the topic name. See Using Advanced Search Tech niques.
Glossary tab	Provides a definition for the terms used in this online Help.

Note:
The Search will not find the phrase "Do Not Disturb". "Not" is a Boolean operator that will initiate a search for the word "do" but not the word "disturb". Use "do disturb" or "DND" to find this term.

Using Advanced Search Techniques

When using the search feature in the online Help, the following techniques can help you narrow your searches for more precise results.

Search for	Example	Results
a single word	page	Topics that contain the word "page" and its grammatical variations, such as pager and paging.
a phrase	auto attendant	The query is equivalent to specifyin g "auto AND attendant," which will f ind topics containing both of the in dividual words.

Boolean operators

The AND, OR, NOT, and NEAR operators enable you to precisely define your search by creating a relationship between search terms. The following table shows how you can use each of these operators. If no operator is specified, AND is used. For example, the query "attendant console programming" (entered without the quotation marks) is equivalent to "attendant AND console AND programming."

Search for	Example	Results
Both terms in the same topic.	attendant AND console	Topics containing both the words "at tendant" and "console".
Either term in a topic	attendant OR console	Topics containing either the word "a ttendant" or the word "console" or b oth.
The first term without the second te rm.	attendant NOT console	Topics containing the word "attendan t" but not the word "console".

Note:
The |, &, and ! characters don't work as Boolean operators (you must use OR, AND, and NOT).

Finding words in a topic

After you have narrowed your word search to a list of topics, click a topic from the list. Each occurrence of the word will be highlighted in yellow in the topic text. Note that only exact matches are highlighted.

Note:
If a Help link is highlighted in yellow as a result of a search, the link may not function until you remove the highlighting by clearing the search results. To clear the search results, search on another word, or by exit the Help.

For large topics, you may find it easier to search for the word in the topic text. To search for a word in a topic:

1. Put your cursor at the top of the topic frame.
2. Type **Ctrl-f**.
3. Enter the word and click **Find Next**.

Linking back to the previously viewed topic

You can go back to the previously viewed topic by clicking the **Back** button in the menu bar or by pressing the **Alt** and **<-** keyboard keys at the same time.

26.7 Documentation Conventions

Reader Advisories

The following reader advisories are used in this help system:

Note:
These symbols indicate text that contains additional information, especially useful in relation to a procedure.

CAUTION:
Information that helps you prevent equipment or software damage.

Warning:
Information that helps you prevent an interruption to telecommunications traffic.

26.8 Contacting Technical Support

Order Desk

To contact the Order Desk, call

- Mitel NA Order Desk 1-800-796-4835.
- Mitel UK Order Desk: +44 870 160 0471.
- Mitel EMEA Order Desk: +44 1291 426071.

Repair Department

You must obtain a Return of Merchandise Authorization (RMA) form from the Repairs Department before sending equipment back to Mitel.

- Mitel NA Repairs Department: 1-888-222-6483.
- Mitel EMEA Repairs Department: +44 1291 437666.

Technical Support

Please contact Mitel Technical Support if you require technical assistance. If you cannot resolve the problem with the Troubleshooting sections in the *NuPoint Unified Messaging Technician's Handbook*, please collect the required information listed in the Troubleshooting chapter before calling Mitel Technical Support.

- Mitel NA Technical Support: 1-800-561-0860 or 1-613-592-2122. (Please have your technical support ID ready.)
- Mitel EMEA Technical Support: +44 1291 436888. (Please have your dealer ID and password ready.)

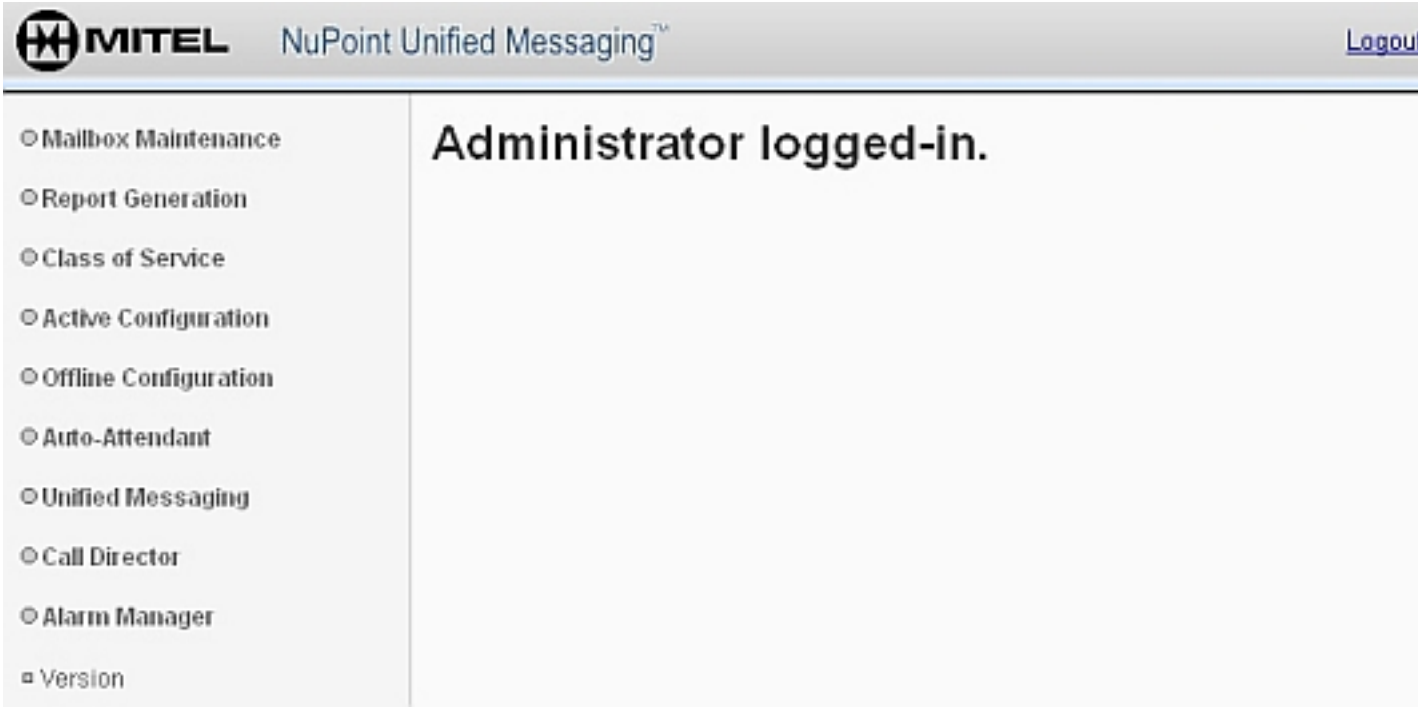
26.9 Overview

There are two administration consoles for NuPoint Unified Messaging: the Text Console and the Web console. You can use the Web console for most configuration and programming, however, there are some instances when you must use the Text Console. Where applicable, instructions are supplied for both.

The Web Console

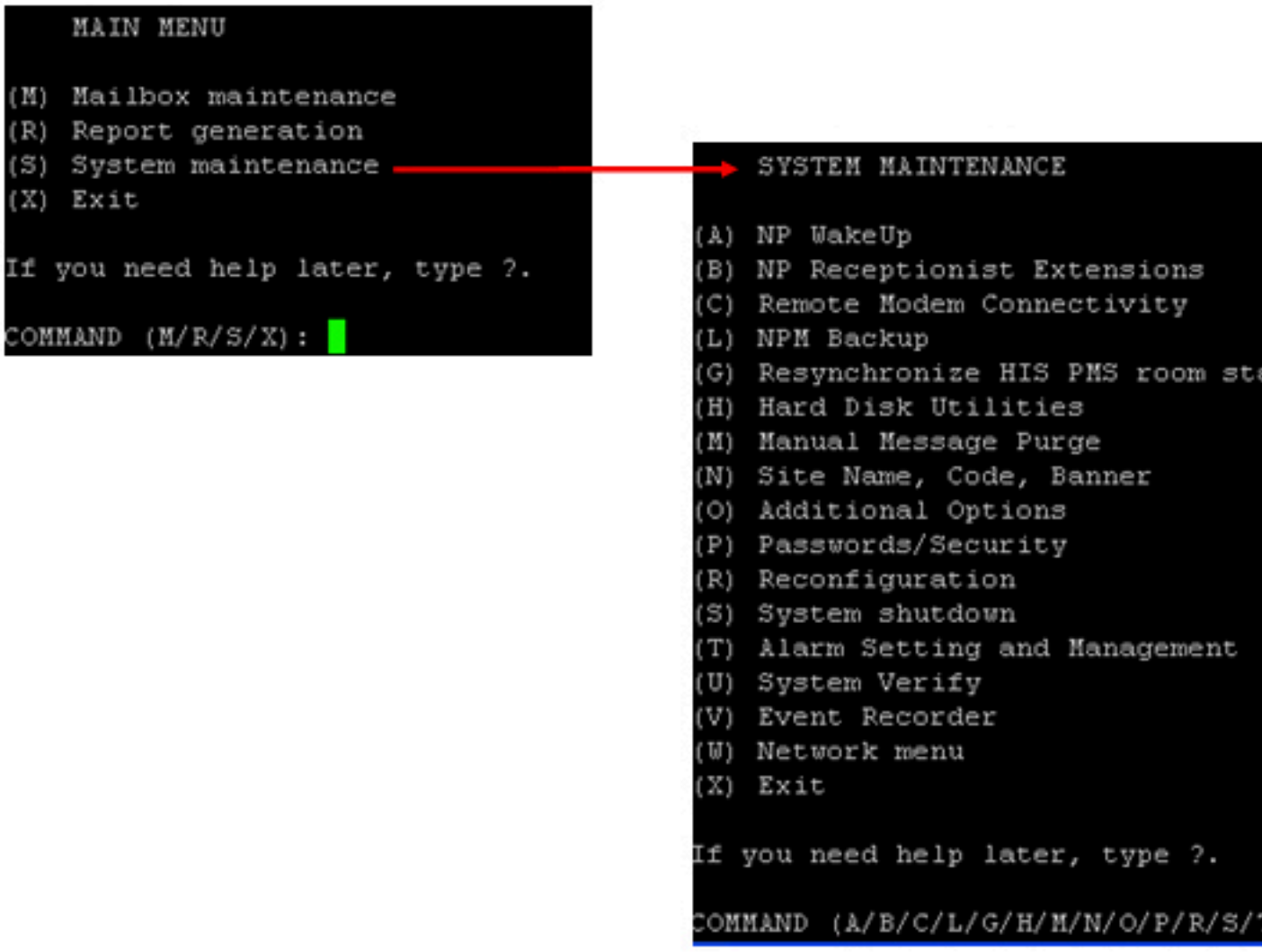
The Web Console provides a user-friendly graphical user interface (GUI) that enables you to perform most administration functions. It is strongly recommended that you begin using the Web Console instead of the Text Console when working with these features, so as to familiarize yourself with the Web interface as its capabilities become increasingly comprehensive. You must still use the Text Console for those configuration capabilities that are not supported on the Web Console.

Each Web Console window connects to one NuPoint Unified Messaging system. To administer a second NuPoint UM system, you can either open a Web Console session in another browser window or use the pass-through login capability in the Web Console to access other systems.



The Text Console

The Text Console is a menu-driven administration console that you can use for all software configuration, feature programming, and system administration on the NuPoint Unified Messaging server (except the Speech Auto Attendant feature). As shown below, you make menu selections to navigate through the console and to perform maintenance and administration tasks.



26.10 The Web Console

The Web Console provides a user-friendly graphical user interface (GUI) that enables you to perform most administration functions.

The Web Console supports two user types:

- **System superuser**: Two superusers ("admin" and "root") are created when the system is originally installed. They have access to all features and server resources.
- **FPSA user: Funtionally Partitioned System Administration (FPSA) users can access features and server resources based on which "permission categories" they have been assigned by the system superuser. For example, an FPSA user with permission category six is limited to accessing network and network-related features in the console**.

To log in to the NuPoint Unified Messaging Web Console:

1. Open a web browser and navigate to **http://< *IP address or Fully Qualified Domain Name* >/npm-admin**
2. Enter your user name and password, select the Server from the drop-down list, and then click Login.

Conditions

- Conditions for FPSA Users:

- Up to five different FPSA users can be logged in to Web Console simultaneously. If a sixth FPSA user attempts to log in, access will be denied.
- An FPSA user can only have one login session. If a user opens a second session on the same or another client PC, the first session will be terminated.
- A client PC can support only one login session. If a user opens a second session on the same client PC, the first session will be terminated.
- After five minutes of inactivity, an FPSA login session will expire automatically.
- After three unsuccessful login attempts, an FPSA user will be locked out and must contact the system superuser to have his or her password reset.
- Conditions for System Superusers:
- After 30 minutes of inactivity, a system superuser login session will expire automatically.
- After three unsuccessful login attempts, a system superuser will be locked out for 20 minutes. If more unsuccessful logins are attempted, the console will locks itself indefinitely and the administrator must use the UNIX shell to unlock it via SSH/PuTTY. See Unlocking the System Superuser Account, below, for details.
- The Web Console is supported on the following web browsers:
- Microsoft Edge
- Internet Explorer
- Google Chrome
- Mozilla Firefox

Unlocking the System Superuser Account

Once the Web Console is locked (temporarily or permanently), you can log in using SSH/PuTTY and invoke the following command:

```
%
/usr/vm/bin/unlocksona
```

The system prompts you for the password. After it is entered, the web console and SOAP interface are unlocked. The administrator can refresh (F5) the login page in the web browser and log in with the correct password.

Note: For more information about SSH/PuTTY access, see the *NuPoint Unified Messaging Technician's Handbook*.

Menus

Use the menu on the left-hand panel to navigate the Web Console. The menus are divided into the following main categories:

- Mailbox Maintenance

- Report Generation
- Audit Trail
- Class of Service
- Active Configuration
- Offline Configuration
- Auto Attendant
- Unified Messaging
- Call Director
- Alarm Manager
- FPSA Manager
- Utilities
- Activate Configuration
- Version

Click each top-level menu to expand the menus for that category. Click an expanded menu item to display the corresponding feature in the right-hand panel. High-level menu items have a circle next to them. With the exception of the Edit Offline Configuration menu, clicking the circle expands and contracts its submenus. Submenu items with a square beside them provide access to the features.

Users can reach console menus only if they have the proper FPSA permission category (or categories).

26.11 The Text Console

The NuPoint UM Text Console is a menu-driven configuration tool you can use to customize and administer NuPoint UM software. Console administration is a menu-driven procedure; the starting point is the console Main Menu. From this menu, you can choose one of three sub-menus that allow you to change mailbox data files, perform system maintenance, or run reports. Once you begin one of these tasks, the system prompts you for specific information. You may type a question mark (?) in response to prompts to receive embedded online help.

The Text Console supports two user types:

- **System superuser**: Two superusers ("admin" and "root") are created when the system is originally installed. They have access to all features and server resources.
- **FPSA user: Funtionally Partitioned System Administration (FPSA) users can access features and server resources based on which "permission categories" they have been assigned by the system superuser. For example, an FPSA user with permission category six is limited to accessing network and network-related features in the console .**

Multiple users can access Text Console simultaneously using any of the following methods:

- Onsite, by attaching a monitor and keyboard directly to the NuPoint UM server
- From a PC on the same network using an Ethernet connection
- From a remote PC using an SSH client like PuTTY

Text Console is supported through the main Linux interface (sign in as "root" to access the NuPoint UM Text Console, or as "admin" to access the MSL server console) and also through PuTTY.

Note:
For detailed Text Console instructions, refer to the NuPoint UM System Administration help file posted at Mitel OnLine.

To activate Text Console:

1. Enable the appropriate SSH settings in MSL.
2. Launch an SSH client such as PuTTY.
3. Enter the **Host Name (or IP Address)** of the NuPoint UM server.
4. Click **Open**. A command prompt displays.
5. Log in as "root" and enter the root password. (The root password may be the same as the administrator password.)
6. Type **console** and press **Enter**. The Text Console displays.

Each time you log in, the system displays the console Main Menu, previous login information, and the system status. The following output displays this information. (Your system may have additional options depending on its configuration.)

```
root@10.39.17.222's password:
Last login: Wed Jul  9 14:37:18 2014 from 10.35.19.89
[root@sanity2 ~]# console
--------------------------------------------------------------------------
Copyright (c) 1983-2009, Mitel Networks Corporation, All Rights Re
--------------------------------------------------------------------------
                        <System Status>
   HOST :       1
 STATUS :     ENA
 OS VSN :     2.6.32-431.5.1.el6.i686
 MEMORY :     188820/1938872
LOG DATA:      Y

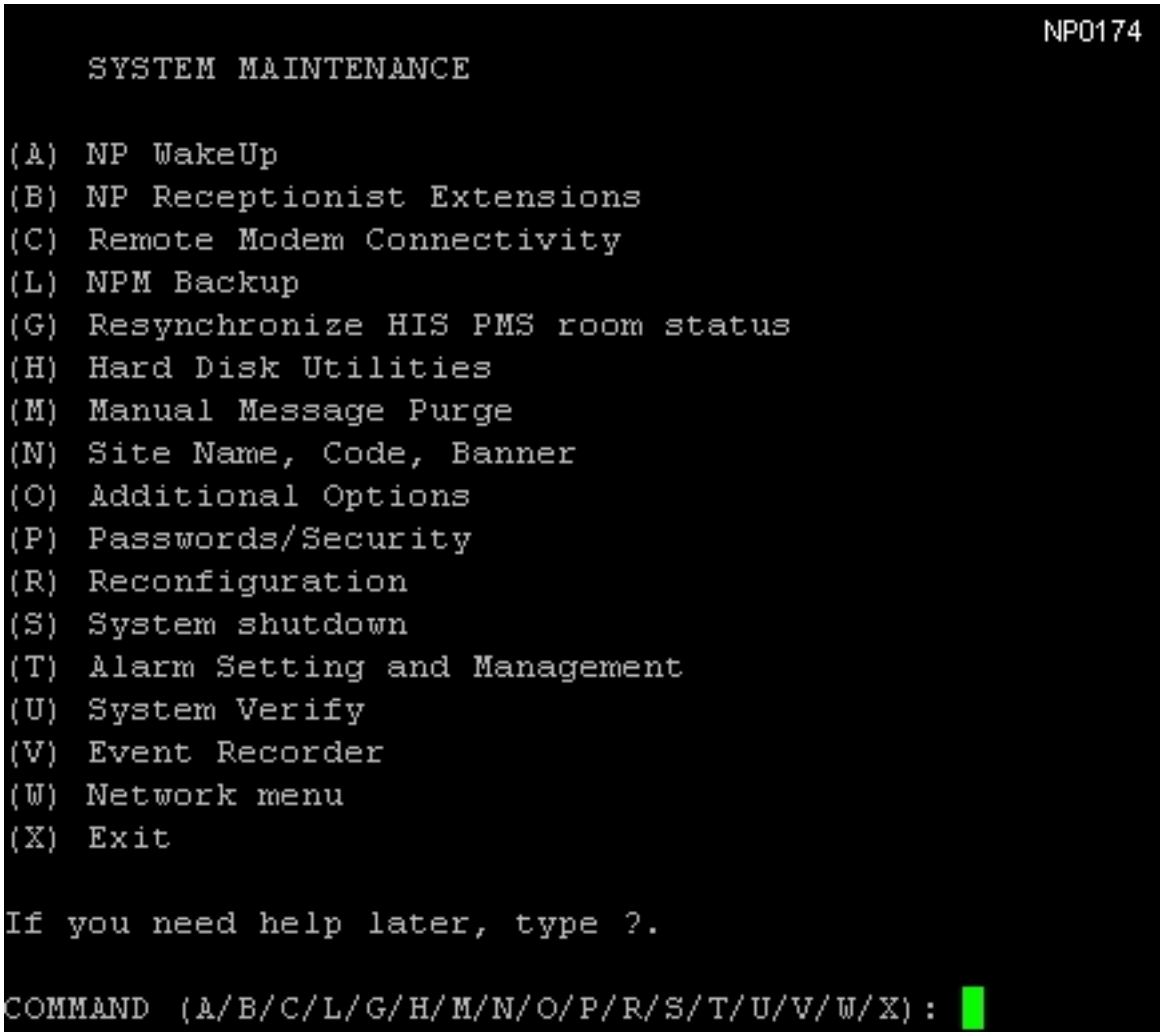

    MAIN MENU

(M) Mailbox maintenance
(R) Report generation
(S) System maintenance
(X) Exit

If you need help later, type ?.

COMMAND (M/R/S/X):
```

Configuration is performed by entering the letter that corresponds to the menu item to be accessed. For example, to see the System Maintenance menu, you type **s** (or **S**) at the prompt. The System Maintenance menu opens many more menu choices. Instructions in this guide include all menu entries required to access the options to be configured.



Viewing Menus

- When you finish entering a value for a parameter, the server displays an abbreviated form of the current menu, called the "short menu" (for example: COMMAND (A/E/F/G/H/X):). To view the complete current menu when a short menu is displayed, just press **Enter**.
- To return to the Main Menu from any NuPoint Voice configuration menu, press **X** (Exit), until the Main Menu appears.

Accepting Defaults

- To accept a default displayed in a *prompt*, just press **Enter**.
- To accept a default displayed in a *menu*, no action is necessary.

Avoiding Automatic Exit

CAUTION:
The NuPoint Unified Messaging server "times out" after 15 minutes. This means that if you do not enter anything at the console for 15 minutes, the server automatically exits from the current program. When this happens, all work that has not been saved on the disk is lost.

To avoid being timed out and losing your work, follow these steps:

1. When you need time to think, note the name of the current menu.
2. Exit to the (server) Main Menu.
3. When you want to continue your work, enter the appropriate menu options to regain your place.

If you find that the NuPoint Unified Messaging server has timed out, follow the steps below. If your screen is blank, press any key to reactivate the screen and then continue with these steps.

1. Press any key to start the login sequence.
2. Enter your user ID and password (if requested).
3. Starting from the Main Menu, enter menu options to proceed to the menu from which the server timed out.
4. Re-enter data as needed to regain lost work.

Quitting an Entry Session

At any point during entry of offline or online parameters, you can quit. Quitting discards all entries you have made and leaves the NuPoint Voice configuration the way it was before you started entering parameters.

To quit from the NuPoint Voice Configuration Offline or Online Menu:

Select:	(Q) Quit -- Forget Changes
Prompt:	Quit and forget changes? (y/n) =
Response:	Y to return to the NuPoint Voice Configuration Main Menu.

Shortcut Commands

You can use the CTRL (Control) key or the / (slash) key while simultaneously pressing another key to execute shortcut commands at a server console.

To do this...	Type...
Activate a timed-out console	any key
Exit from the offline or online menus, or FCOS, LCOS, GCOS menus, and save any entries.	X
Exit from the offline or online menus, or FCOS, LCOS, GCOS menus, without saving any entries.	Q + Y
Stop scrolling a displayed report.	CTRL-S

To do this...	Type...
Resume scrolling a displayed report.	CTRL-Q
Return to the NuPoint Unified Messaging application when a # prompt is displayed.	**CTRL-D** or type **exit**
Return to the Reports Menu if you paused the display	Q + return or Esc,Esc + return

Note:
If you see a display of nonsense characters when you activate the console, **press the space bar to reset.**

My System is Locked; How Do I Continue?

Occasionally, the system may appear to be "locked". When this happens, press **CTRL + Q** to continue console maintenance functions.

26.12 Console Capabilities

NuPoint UM configuration is in the process of being transferred to the Web Console. During this process, some items are only configurable using the Text Console. The following list details configuration capabilities:

Feature/Item	Text Console	Web Console
Basic Configuration: Line Groups Dial Plans Mailboxes Class of Service NuPoint Voice Application Pager/Outdial Application Message Waiting Application	YES with the **exception** of: - Network Elements	YES with the following **exceptions**: - scheduling of greetings - alternate greetings - copying greetings - enable cascade paging
System Administration		
Maintenance - purge, backup, alarm management	YES	YES with the following **exceptions**: - manual purge - system shutdown - data restore
Security -audit trails, Functionally Partitioned System Administration (FPSA)	YES	NO
Billing -Gather, set billing rates	YES	YES
Reports	YES	YES (subset of Text Console reports)

Feature/Item	Text Console	Web Console
Optional Features		
Call Detail Recorder	YES	NO (reporting only)
Call Director	NO (Configuration only)	YES (Configuration and interaction)
Competitive TUI Emulation	YES	YES
Cut-Through Paging	YES	YES
Language Prompts	YES	YES
NP Fax	YES	YES
NP Forms	YES	YES
NP Net	YES	NO (TCP/IP and NCOS configuration only)
NP OnDemand	YES	YES
NP RapidDial	YES	NO
NP Receptionist	YES	NO
NP WakeUp	YES	NO

Feature/Item	Text Console	Web Console
PMS Integration	NO (Serial and Serial-to-IP converter only)	YES (Rel 4.1 and later: Serial, Serial-to-IP, and IP.) (Except check-in/check-out behavior)
Record-A-Call	YES	YES
Softkeys	YES	NO (Extension mapping only)
SMS Notification	YES	YES
Speech Auto Attendant	NO	YES
Speech to Text	NO	YES
Unified Messaging	YES	YES
VPIM	YES	NO

26.13 Frequently Used Procedures

The following frequently-used procedures may be required when configuring many of the applications used with NuPoint Unified Messaging:

In the Web Console:

- Create a Line Group
- Customize an FCOS
- Assign an FCOS to a Mailbox
- Duplicate the Active Configuration
- Activate the Inactive Configuration
- View the Active Configuration

In the Text Console:

- Define a Line Group
- Customize an FCOS
- Assign an FCOS to a Mailbox
- Duplicate the Active Configuration
- Activate the Inactive Configuration
- Run a System Configuration Report

26.14 Introduction

The chapters in this section describe how to configure the base NuPoint Unified Messaging software after it has been installed on a server. The definitions on this page describe terms and concepts that are used in this guide:

Applications:

The following applications are provided with your basic NuPoint UM server. You can configure these applications to provide custom message-taking, outdialing, and Message Waiting Indication. Each application requires its own line group. (Note: NP Call Director and NP Receptionist are the exception - these two applications can share a line group with the NuPoint Voice application.)

- **NuPoint UM Voice Application** : the basic business application, used for message-taking and retrieval.
- **Pager Application** : used for paging, but also for a number of other functions that require outdialing.
- **Message Waiting Application** : used when an integration does not handle message waiting indicators itself.

Modifiers:

Modifiers are characteristics that are common to all applications. You control the behavior of the application by configuring its modifiers. The most common modifiers are listed here:

- Line Groups: A line group is a set of one or more incoming telephone lines, which come into line ports on the server hardware. Each application you use must be assigned its own line group (except for NuPoint Receptionist and Call Director, which can both work in the same line group as the NuPoint Voice application. Also, any operations involving outdialing can use the same line group assigned to the Pager application.) Most of the modifications you make to an application are made to its line group. See About Line Groups for more information.
- **Dialing Plan**: To configure each application, you must define its dialing plan, which is the structure of how the mailboxes are numbered. Related features include which key a user presses to speak to a system attendant, or to use call placement. See About Dialing Plans for more information.
- **Day/Night Hours**: This feature of the NuPoint Voice application lets you set the work schedule: both office hours and which days are handled as weekends. This also handles certain situations such as a user wishing to speak to a system attendant.
- **Mailboxes**: Every user of the server needs a mailbox, and all applications require mailboxes. The administrator's mailbox and attendant's mailbox are special mailboxes that interact with applications; along with other special mailboxes like tree, rotational, and broadcast, they are discussed in the Mailboxes section. Mailbox features, such as Distribution Lists, receipts, and greetings are also discussed in that section.

- **Class of Service**:

  - **Features Class of Service (FCOS):** a group of features applied to each mailbox that allow users to perform functions or control how the server can be used. See Features Class of Service.
  - **Limits Class of Service (LCOS)**: a group of limitations on each user, such as length and number of messages. LCOSs also affect how some optional features work. One LCOS is assigned to each mailbox. These are explained in Other Classes of Service.
  - **Group Class of Service (GCOS)**: determines which users can send messages or respond to messages from other users. There are two kinds of GCOSs, affinity and bit-mapped. One GCOS is assigned to each mailbox. These are explained in the Other Classes of Service.
  - **Network Class of Service (NCOS)**: controls users' network access and is a part of the NP Net Digital Network optional feature. More NCOS information is contained in the *NP Net chapter of the* Optional Features section.
  - **Restriction Class of Service (RCOS)**: is an element of NPA/NXX call screening that restricts mailbox outdials to certain area codes or to certain prefixes within an area code. One RCOS is assigned to each mailbox. These are explained in the Other Classes of Service.
  - **Tenant Class of Service (TCOS)**: used with the ESMDI "Multi-Tenant" application, to govern mailbox interaction between user communities. For more information about ESMDI integrations, see the *Optional Integrations Guide* available at Mitel OnLine.

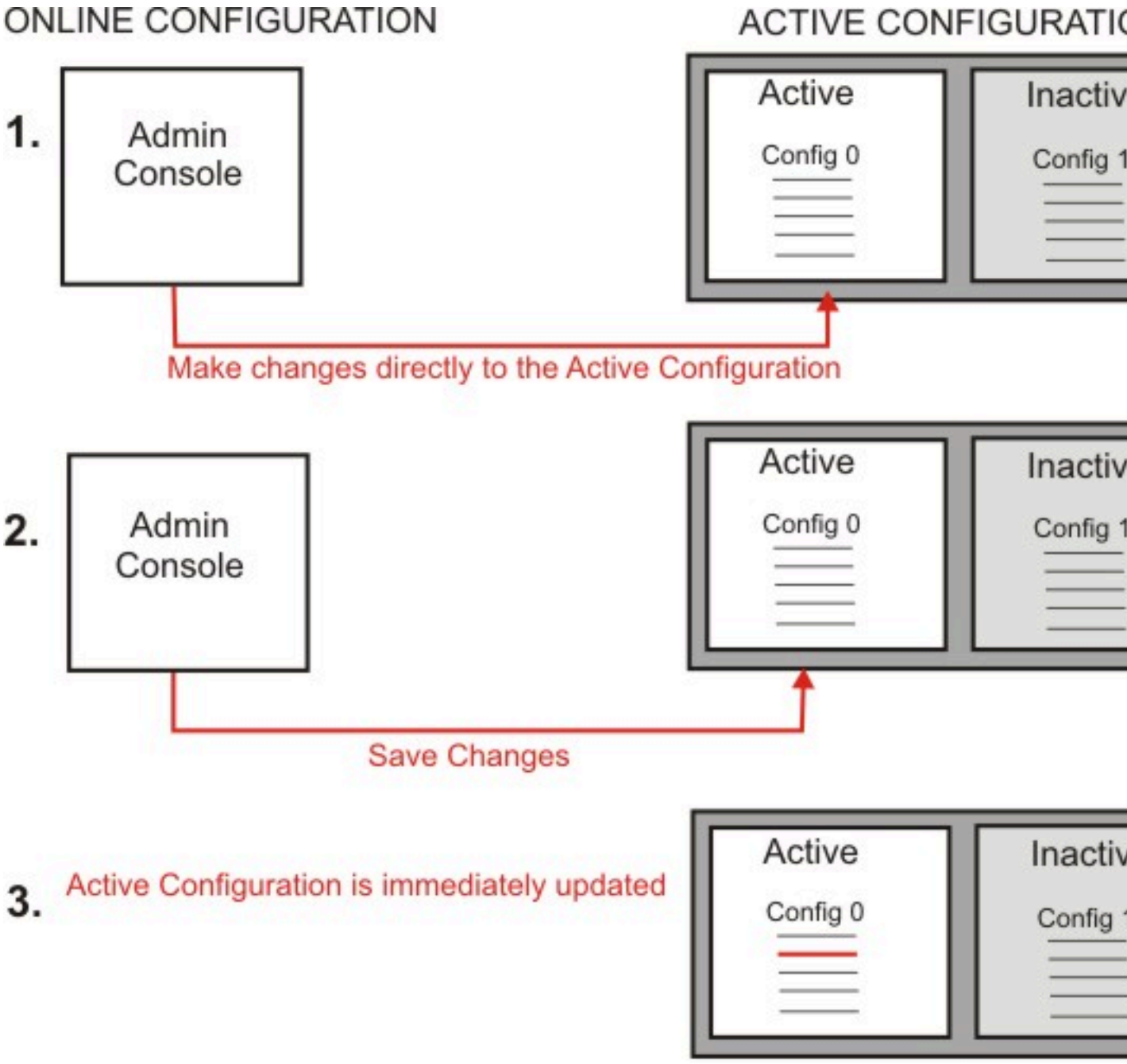
26.15 About Configuration

26.15.1 About Configuration

Configuration is the process of entering application and modifier data in the administrator Text console or the Web console. This data is stored in a configuration file on the hard disk, and controls call processing.

Online Configuration

Some configuration settings can be changed "on the fly", that is, without the need for activation. These changes are made directly to the active configuration and take effect immediately upon exiting the menu. These changes are referred to as **Online Configuration**.



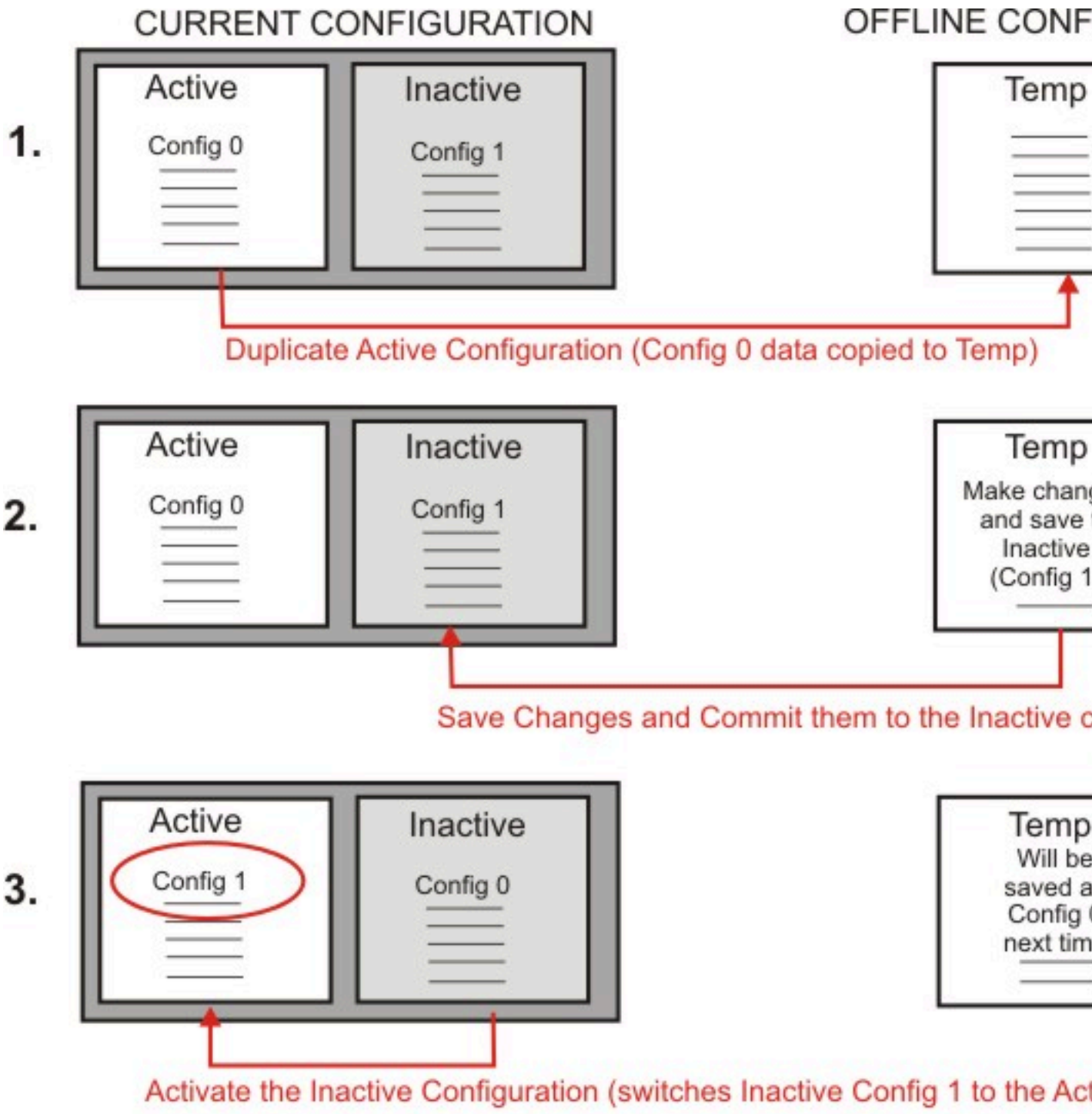
Offline Configuration

Other configuration settings **cannot** be changed "on the fly". The NuPoint UM service must be stopped while the configuration settings are updated. For these cases, (see diagram) you must:

Step 1: **Duplicate the Active Configuration**: copies the active configuration data (Config 0) to the Offline Configuration to provide a base for your changes.

Step 2: **Make your changes** to the Offline Configuration and save (commit) them. The Inactive Configuration is updated with your new configuration information.

Step 3: **Activate the Inactive Configuration**. Config 1 becomes the active configuration.



Note:
The **Offline** menu is used exclusively to make changes to the **Inactive** configuration.

Some applications and features require you to make changes to both Online and Offline configuration items. You can make these changes separately (make the online changes to the Active configuration before you duplicate it) OR after Step 2, you can make the necessary Online configuration changes to the INACTIVE version and then, when you activate, all changes will be included.

26.15.2 View Active Configuration

1. In the navigation tree, select **Active Configuration > View Active Configuration**.
2. To view the configuration of a particular line group, select the **number** from the list, or select **all** to view all groups.
3. Click **View** to see the report on screen, or click **Download** to save the report as a text file.

26.15.3 Duplicate the Active Configuration

For configuration parameters that must be modified offline, the Web Console prompts you to duplicate the active configuration.

1. In the navigation tree, click **Offline Configuration** and then **Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**. A confirmation message appears.
3. Make the required changes to the duplicate (offline) configuration.
4. When you are finished, click **Commit Changes and Exit** to commit the changes to the duplicate (offline) configuration.
5. When you are finished modifying the duplicate, and you are ready to implement the new configuration, you must Activate theInactive Configuration.

26.15.4 Activate the Inactive Configuration

To activate the inactive configuration:

1. In the navigation tree, select **Offline Configuration > Activate Offline Configuration**. An onscreen message indicates if the Offline Configuration has changed since the last activation.
2. You can delay the activation until **MWI queue** and **Pager queue** are empty by selecting the appropriate check boxes.
3. Click **Activate**. The currently active configuration is replaced with your edited offline version.

Note:

- NuPoint services are temporarily unavailable while the configuration is activated.
- When you activate the new configuration, the old configuration is stored offline as the "inactive" configuration. If you experience problems with the new configuration, you can restore the old configuration by repeating the preceding steps, provided no changes have been made to the configuration in the interim.

26.15.5 Duplicate the Active Configuration

For configuration parameters that must be modified offline, the Web Console prompts you to duplicate the active configuration.

1. In the navigation tree, click **Offline Configuration** and then **Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**. A confirmation message appears.
3. Make the required changes to the duplicate (offline) configuration.
4. When you are finished, click **Commit Changes and Exit** to commit the changes to the duplicate (offline) configuration.
5. When you are finished modifying the duplicate, and you are ready to implement the new configuration, you must Activate theInactive Configuration.

26.15.6 Activate the Inactive Configuration

To activate the inactive configuration:

1. In the navigation tree, select **Offline Configuration > Activate Offline Configuration**. An onscreen message indicates if the Offline Configuration has changed since the last activation.
2. You can delay the activation until **MWI queue** and **Pager queue** are empty by selecting the appropriate check boxes.
3. Click **Activate**. The currently active configuration is replaced with your edited offline version.

Note:

- NuPoint services are temporarily unavailable while the configuration is activated.
- When you activate the new configuration, the old configuration is stored offline as the "inactive" configuration. If you experience problems with the new configuration, you can restore the old configuration by repeating the preceding steps, provided no changes have been made to the configuration in the interim.

26.15.7 About Line Groups

A line group is a quantity of telephone lines (server ports) that are grouped together and assigned to a single application. Any programming that is done for the application applies to every port in the line group. For example, you may have a NuPoint Voice line group, and/or a Paging line group. The number of ports assigned to each line group is dependent upon the traffic that you expect to experience for that particular application.

At the PBX or CO level, all telephone lines connected to the ports of an individual line group are typically assigned to a hunt group, ACD group, UCD group, etc. to ensure that incoming calls are answered by the first port that is available for the particular application.

Note:
For MiCollab deployments of NuPoint UM, you must use the MiCollab Users and Services Provisioning application to set up one or more Network Elements before configuring Line Groups.

Line Group Number

Each line group is represented by a discrete number. Valid line group numbers are 1 through 24. The preset default for the NuPoint Voice application is 1.

Group Name

The group name identifies the line group's purpose. For example, a line group could be called "Message Center." There is no default group name.

Line(s) in Group

You identify each line (or port) in a group with three identifiers that indicate a module, a slot, and a port. This set of three identifiers is called a *triplet*.

- **Module** refers to a CPU, the server's main processor. Since all NuPoint UM implementations have a single-module server, you can omit the module identifier and simply refer to the slot and port numbers.

Note:

Support for multiple-module servers (e.g. NuPoint UM 640) was discontinued with NuPoint Release 6.0. As a result, you do not need to specify a module number for Release 6.0 and later.

- Slot is a reference to line card technology that doesn't apply to current model servers. For this reason, slot is always 0 for mail ports or 5 for fax ports.
- Port refers to the actual port number, starting at 0 and ending at the upper limit of your port licensing.

For each module, slot, and port, there are valid values. The following table describes them:

Module/Host	Slot	Port (virtual)
NuPoint UM 60 ports = 1 (or blank) NuPoint UM 120 ports = 1 (or blank)	Always 0 for mail ports. Always 5 for fax ports.	0 - licensed port limit, no duplicates allowed OR * for all ports

All of these formats are valid:

Example	*Specifies*
1: *	All lines on module 1
1:0:0-1:0:59	All lines from 0 to 59 on module 1
1:0:*	All lines on module 1
1:0:0-2:0:4	All lines on module 1, slot 0, through module 2, slot 0, port 4
1:*,2:*	All lines on modules 1 and 2

If you are adding multiple lines to a group, you can separate the line numbers by commas as you enter them. For example, to add lines 0,1 and 5, enter 1:0:0,1:0:1,1:0:5.

If you are entering a range of lines, you must use the full triplet on both sides of the range. For example, to add 60 lines on module 1 to a line group, enter 1:0:0-1:0:59 (for single-module systems, you can omit the module number; for example, 0:0-0:59.)

Note:
For more information about adding line groups for specific applications, see the help topic for that application.

26.15.8 About Dialing Plans

Dialing Plans for Mailboxes

The dialing plan is a string of nine elements. The elements in the string define, by position, the number of digits in valid mailbox numbers. The first element shows the number of digits allowed for mailboxes that begin with 1. The next element shows the number of digits allowed for mailboxes that begin with 2, and so on up to mailboxes that begin with 9. Each element is separated by commas.

If you change any element, you must re-enter the entire mailbox dialing plan.

Valid mailbox numbers can be up to 11 digits long, so valid numeric elements can be 0 (zero) through 11. When an element is zero, no mailboxes beginning with that digit are allowed.

Example 1: if your dialing plan is *0, 3, 3, 7, 3, 3, 3, 3, 10,* the NuPoint Voice application interprets the string as follows:

Digit	Element	Interpretation
1	**0**	**No mailboxes start with 1. Mailbox numbers 1, 11, 111, etc. are all invalid.**
2	**3**	**Mailboxes starting with 2 are three digits long. Valid mailbox example: 211**
3	**3**	**Mailboxes starting with 3 are three digits long. Valid mailbox example: 347**
4	**7**	**Mailboxes starting with 4 are seven digits long. Valid mailbox example: 434-1234.**
5 6 7 8	**3 3 3 3**	**Mailboxes starting with 5, 6, 7, and 8 are three digits long. Valid examples are: 523, 617, 727, 855.**
9	**10**	**Mailbox numbers starting with 9 are ten digits long. Valid mailbox example: 912-456-7778.**

The default dialing plan is *3,3,3,3,3,3,3,3,3,3* meaning all mailboxes have 3 digits that may start with any digit from 1-9.

You can also substitute a dial plan **type** for length of extension as follows:

Dialing Plans for Server Features

Other entries allowed in the dialing plan allow other NuPoint Unified Messaging server features. The following table lists these entries for your reference.

Element	Explanation
0-11	**Length of the mailbox. Zero means none may start with this number.**
V	**Variable number (1 through 11) of digits; server uses timeout to determine end of mailbox number**
M	**Analog networking (AMIS) mailboxes leading digit**
A	**Dial-by-Name (ASCII) leading digit**
T	**Call placement leading digit**
N(n)	**Networked mailboxes, (n) = mailbox number length. NV (variable number length) is also acceptable**
P(n)	**Network mailbox with prefix used, (n) = mailbox length including prefix digit**

If the extension numbers at your site use too many starting digits to implement all these capabilities in your dialing plan, you can use the optional star prefix dialing plan, described below.

Optional Star Prefix Dialing Plan

The standard dialing plan tells the NuPoint application how to handle DTMF digits 1 through 9. If you have a conflict (for example, if you have extensions starting with digit 3 and you have also assigned Dial by Name to digit 3), you can implement the optional Star Prefix dialing plan. This allows multiple features using the same digit entry with the star (*) key.

You can implement several features with the optional dialing plan, as shown in the table below.

Optional Dialing Plan Choices	Counterpart in Regular Dialing Plan
Dial-by-Name	**A**
Analog Networking	**M**
Networking without prefix	**N**
Networking with prefix	**P**
Call Placement	**T**

For example, your regular Dial-by-Name dialing plan might look like this: 0,0,3,3,3,3,A,3,3 which would trigger the prompt, "Please enter a mailbox number or press **7** to dial by name." If you also have extension numbers that start with 7, they can never be directly reached. To avoid this conflict, use the Text Console to program a star prefix digit into the dialing plan. When properly configured, the star prefix dialing plan for this example triggers the prompt, " Please enter a mailbox number or press ***7** to dial by name."

PBX Dialing Plans

A PBX only allows a certain range of extension numbers. Ideally, employees' mailbox numbers should match their extension numbers. This makes it easier for callers to remember the proper mailbox number. If the numbers do not match, and the optional NP Receptionist program is installed, you can program certain conversion factors to allow the NuPoint Voice application to match the extension with the correct mailbox number.

If the company has employees in the field who do not have regular PBX extension numbers, you can give them mailbox numbers that do not fall in the range of allowable PBX extensions, even if there are enough mailbox numbers in this range. You can reserve these extra mailboxes for future expansion of in-house staff. For example, if the PBX allows extensions 200 to 399, you can keep the dialing plan at the default setting of *3,3,3,3,3,3,3,3,3*, and assign all field personnel mailboxes 600 through 799.

Example 2: if your dial string is 0,4,3,3,3,3,A,V,10, it is interpreted as follows:

Digit	Element	Interpretation
1	**0**	**No Directory Numbers (DNs) start with 1.**
2	**4**	**DNs starting with 2 are four digits long. For example, 2123 is valid. 212 is not.**

Digit	Element	Interpretation
3 4 5 6	3 3 3 3	DNs starting with 3, 4, 5 and 6 are three digits long.
7	A	DNs starting with 7 are Dial-by-Name.
8	V	DNs starting with 8 can be any length (variable).
9	10	Mailbox numbers starting with 9 are ten digits long. Valid mailbox example: 1-916-456-7777

26.15.9 About Mailboxes

Think of a system mailbox as a post office box where voice messages, instead of written memos, are collected. Company employees become "system users" when they are assigned personal mailboxes.

To "open" their mailboxes, users call the system number, log in (press the star (*) key plus the mailbox number on the telephone keypad), and enter personal passcodes. From NuPoint Receptionist, users press the star key (*) plus the mailbox number, again press the star key (*), and enter their passcodes. In an integrated system, users are taken directly to the passcode prompt.

A range of software tools are available to customize your system.

- After login, the functions that users can choose depend on the classes of service assigned to the mailbox when it was created:

  - Feature bits, grouped into a Feature Class of Service (FCOS), allow users to perform functions or control how the server can be used. One FCOS is assigned to each mailbox.
  - Limits Class of Service (LCOS) control features such as the number and length of messages stored in a mailbox. One LCOS is assigned to each mailbox.
  - Group Class of Service (GCOS) is the group management resource that keeps track of large systems with many groups. GCOS determines which users can send messages or respond to messages from other users. One GCOS is assigned to each mailbox.
  - Network Class of Service (NCOS) controls users' network access; it is part of the NuPoint Net Digital Network optional feature.
  - Restriction Class of Service (RCOS) is an element of NPA/NXX call screening that restricts mailbox outdials to certain area codes or prefixes within an area code. One RCOS is assigned to each mailbox.
  - Tenant Class of Service (TCOS) is used with the ESMDI "Multi-Tenant" application to govern mailbox interaction between user communities. (See "Creating or Modifying a Tenant COS" in the*NuPoint Unified Optional Integrations Guide*.)
- Message Waiting Types specify how users are notified of unplayed messages in mailboxes.
- Attendant Extension Numbers are called when assistance is requested by a caller leaving a message in a mailbox or when outside callers request assistance through NuPoint Receptionist. (SeeRequired and Optional Mailbox Information.)
- NuPoint Receptionist processes calls according to individual users' requests.

  - Treatment Types assigned to mailboxes contain most instructions. (See Treatment Types.)
  - Mailbox Extension Numbers are checked when callers input an extension number; this is the actual number that the system dials; it can be programmed when the "extension" is outside the PBX network (see Programming NuPoint Receptionist to Dial an Outside "Mailbox's Extension.)

Note:
You can configure and manage mailboxes, using either the Text Console or the Web Console.

Outside Callers versus System Users

- An "outside caller" dials the system number, enters a mailbox number, listens to the mailbox greeting (or to the prompt, "Please leave a message for <name>"), and then leaves a message.
- A "system user" logs in to his or her own mailbox and uses the make, give, or answer command to leave a message.

Variable Length Mailbox Numbers

The variable length mailbox number capability allows the server administrator greater flexibility when assigning mailbox numbers. You can configure a dialing plan to allow variable length mailbox numbers. Code a V in the desired digit position in the dialing plan, as described in the NuPoint Voice Application section under "Mailbox Dialing Plan."

Without this capability, all mailboxes in the same line group that begin with the same digit must be the same length. If, for example, you specify "3" as the mailbox number length for mailboxes beginning with 1,

then all 1-series mailboxes must be three digits long: 100, 101, 102-199, etc. This means you have only 100 mailboxes available beginning with 1.

When you specify that mailboxes beginning with a certain digit can be variable length, those mailboxes can be as short as one digit (9), or as long as 11 (99999999999). This allows you over 11 billion different mailboxes beginning with 9! (You cannot, of course, configure 11 billion mailboxes, since that would exceed the storage capacity of the disk.)

Hotel installations can make good use of variable length mailboxes. It is convenient for a guest's mailbox number, telephone number, and room number to be the same, but this is impossible to achieve with fixed length mailbox numbers and a single line group. To understand why, realize that most hotel dialing plans assign three-digit numbers to rooms on floors one through nine, and four-digit numbers to rooms on floor 10 and above. If the mailbox for room 111 matched the phone number, the mailbox for room 1111 could not.

Variable length mailboxes allow you to keep all mailboxes in a single line group and still assign mailboxes that match room and telephone numbers.

Configuration Considerations

If you configure variable length mailboxes, mailbox owners must modify their interactions in these ways:

- When addressing a message to multiple recipients, they must enter a pound sign (#) after each mailbox number that is variable length, or wait for the server to prompt for the next recipient's mailbox number.

Note:
If mailbox owners enter a pound sign after a mailbox number that is not variable length, the server interprets it to mean that message addressing is complete. This can be confusing to mailbox owners, who find that pressing a pound sign at "the same time" elicits differing prompts. To avoid this confusion, it is recommended that you make either all mailboxes variable length, or none.

After entering the final mailbox number and pound sign, they must do one of the following:

- Enter an additional pound sign to get the "Begin recording . . ." prompt.
- Wait for the "Begin recording . . ." prompt.

The System Time/Date Stamp for Messages

The system adds the time/date stamp to every message to tell the recipient when the message was recorded.

- If the user plays the message on the same day that it arrives, only the time is given

  (for example: 2:00 p.m.).
- If the user plays the message on a later day within the same week, the day of the week and the time are given (for example: Monday, 2:00 p.m.).

- If the user plays a message more than a week after it was received, the day of the week, the date, and the time are given (for example: Monday, May 22, 2:00 p.m.).

26.15.10 About Class of Service (COS)

Class of Service (COS) determines the characteristics that a mailbox will have. Some COS values determine what features will apply (such as x, or x). Other COS values determine what limits will apply (such as x and x). The NuPoint UM system is equipped with a set of default COS values which you can apply to the mailboxes you create. You can also copy and modify the default values to create your own custom COS values.

Types of COS

- A **Feature Class of Service** (FCOS) is a collection of mailbox features, options, and abilities, identified by feature bits. For example, a mailbox that has a COS containing feature bit 043 allows that mailbox to receive the message of the day (an announcement from the attendant's mailbox). each mailbox must be assigned an FCOS. If one is not specifically assigned, then the default FCOS 1 is applied.
- A **Limits Class of Service** (LCOS) is a group of mailbox limits used to control time and storage parameters within mailboxes, such as the number of messages the mailbox can store. The LCOS also determines the mailbox prompts language.
- A **Group Class of Service** (GCOS) manages communication between mailboxes for a particular set of users (for example, when some users need to exchange messages with each other but not with the majority of other mailbox owners).
- A **Restriction Class of Service** (RCOS) controls outdial applications, such as Call Placement, message delivery, and pages, and limits these telephone calls by either area code or prefix.

Two remaining classes of service are described in detail in other guides:

- A **Network Class of Service** (NCOS) controls network access for users; see the NuPoint Net application section.
- A **Tenant Class of Service** (TCOS) manages mailbox interaction between user communities; see "ESMDI Integration" in the *NuPoint Unified Messaging Optional Integrations Guide* for more information.

26.15.11 Media Service

Overview

By default, Mitel devices compress 20 milliseconds of sampled speech input into output frames, that is, a default "packet rate" of 20 ms. Different endpoints (for example, SIP devices) may require different packet rates for successful audio streaming. NuPoint UM interworking with MiVoice Business Release 4.0 (3300 ICP Release 10.0) or later, allows you to configure a variable packet rate for these devices.

Limitations

- Variable packet rate is not supported for SIP connectivity with the MiVoice Office 250 or DMG (formerly PIMG/TIMG) deployments. These deployment options will maintain the fixed rate of 20 ms. even when the Variable Packet rate option is selected.
- Variable packet rate is not supported on MiVoice Business software prior to Release 4.0 (3300 ICP Release 10)

26.16 About Network Elements

IMPORTANT: **Do not use this screen for MiCollab deployments using the Mitel MiVoice Business ICP. You must configure Network Elements in the MiCollab Users and Services application. You must also configure Network Elements before you configure line groups.**

Network Elements configuration must be done using the **Web Console**.

For standalone NuPoint UM, and for MiCollab deployments of NuPoint UM with the MiVoice Office 250 , you can use the Network Elements page of the NuPoint UM Web Console (only) to configure and manage various elements including multiple NuPoint servers, ICPs, and Digital Media Gateways (formerly PIMG/TIMG).

The local NuPoint UM server is automatically added to the Network Elements table and is identified by a padlock icon. The properties of the local server are configured at installation in the MSL server console so they are not configurable from the Network Elements page.

26.16.1 Add a Network Element

To add a network element:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click Network Elements. The Network Elements table is displayed.
4. Click Add. The Add Network Elements form is displayed.
5. Configure the fields on the Network Elements form as described below.
6. Click Save.
7. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

Network Elements Fields Description

Fields	Description/Values
Type	*Required field. Select one of the following types: NPM, MN3300, PIMG, TIMG, HD PIMG, SIP GATEWAY, Other **Note**: The **SIP GATEWAY** option will appear only if the NuPoint Unified Messaging software is installed with a MiCollab license. If this is the case, then the MN3300 option will not appear in the list. The SIP GATEWAY option is used to integrate NuPoint Unified Messaging with the MiVoice Office 250 , MiVoice 5000 , or MiVoice MX-ONE. For more information about product integration, consult the following resources: • MiVoice Office 250 with NuPoint UM standalone— MiVoice Office 250 Integration and *Mitel MiVoice Office 250 and NuPoint UM Integration Guide* • MiVoice 5000 with MiCollab NuPoint UM — *MiCollab Platform Integration Guide* • MiVoice MX-ONE with NuPoint UM standalone — *NuPoint UM Technician's Handbook*
Name	(Optional Field.) Enter a name for the new element. This is the display name of the element.

Fields	Description/Values
Domain Name	*Required field. This is the display name of the element, unless a name has been entered in the Name field. If the element type is "NPM", you must enter in this field the fully qualified domain name of the server. For example: www.mitel.com. If the element type is anything other than "NPM", you can enter any name here, but it is strongly recommended that you enter the fully qualified domain name.
IP Address	* Required field. The IP address of the system. For example: 127.0.0.1
Number of Ports	Specifies the number of ports available. The maximum number of ports varies based on the configuration. **Note**: This field will not be visible when the element is configured as NPM or MN3300.
Username	The user ID of the administrator account that is used to access the system. Maximum length is 20 alphanumeric characters. **Note**: This field is only visible when the element is configured as NPM or MN3300.

Fields	Description/Values
Password	The password of the administrator account that used to access the system. Maximum length is 20 alphanumeric characters. **Note**: This field is only visible when the element is configured as NPM or MN3300.
URL	Specifies the path to launch the admin Console of the remote machine. Some characters such as ”space” must be encoded as per the W3C specification (http://www.w3.org/Addressing/URL/url-spec.dita). **Note**: This field is only visible when the element is configured as "Other".

26.16.2 Modify a Network Element

You can modify the properties of any element except for the local element. To modify local element properties, you must use the Mitel Standard Linux (MSL) server manager console. For more information, see the *NuPoint UM Technician's Handbook*. You can modify the properties of one element at a time.

To modify an element:

1. In the navigation tree, click Offline Configuration**> Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click Network Elements. The Network Elements table is displayed.
4. Select an element in the table, and then click Edit.
5. Edit the required network element fields.
6. Click Save.

7. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.16.3 Delete a Network Element

You can delete an element or multiple elements. You cannot delete the local element.

Note:
If lines have been mapped to an element, you must remove them before the element can be deleted.

To delete an element:

1. In the navigation tree, click Offline Configuration**> Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click **Network Elements**. The Network Element table is displayed.
4. Select an element (or multiple elements) in the table, and then click Delete. Confirm the deletion.
5. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.16.4 Log In to a Remote Network Element

You can log in to a remote network element (that is, an element that is not the local element), through the Network Element table OR through the Web Console login page.

Log in from the Network Elements Table

1. In the navigation tree, click Offline Configuration**> Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **No**.
3. Click **Network Elements**. The Network Elements table is displayed.
4. Click the Login button beside the element to which you want to log in. If a userID and password have been supplied for the element when it was added to the Network Elements table, then you will be automatically logged in. If not, then the link redirects you to the login page for that node.

Log in from the Web Console Login Page

1. Open a Web browser and navigate to **http://** ***<IP Address or FQDN of the NuPoint UM server>*** **/ npm-admin**.
2. Enter the User Name and Password for the remote server, then select the server from the **Server** list.
3. Click Login.

26.17 What is a Mailbox?

Think of a system mailbox as a post office box where voice messages, instead of written memos, are collected. Company employees become "system users" when they are assigned personal mailboxes.

To "open" mailboxes, users call the system number, log in (press the star (*) key plus the mailbox number on the telephone keypad, and enter personal passcodes. From NuPoint Receptionist, users press the star (*) key plus the mailbox number, again press the star (*) key, and enter their passcodes. In an integrated system, users are taken directly to the passcode prompt.

A range of software tools are available to customize your system. Once logged in, the functions users can choose depend on the class of service assigned to the mailbox when you create it:

- Class of Service
    - Feature bits, grouped into **Feature Class of Service** (FCOS), allow users to perform functions or control how the server can be used. One FCOS is assigned to each mailbox. (See FCOS.)
    - **Limits Class of Service** (LCOS) controls features such as the number and length of messages stored in a mailbox. One LCOS is assigned to each mailbox. (See LCOS.)
    - **Group Class of Service** (GCOS) is the group management resource that determines which users can send messages or respond to messages from other users. One GCOS is assigned to each mailbox. (See GCOS.)
    - **Restriction Class of Service** (RCOS) is an element of NPA/NXX call screening that restricts mailbox outdials to certain area codes or prefixes within an area code. One RCOS is assigned to each mailbox. (See Restriction Class of Service.)
    - **Network Class of Service** (NCOS) controls users' network access; it is part of the NuPoint Net Digital Network optional feature. (See Network Class of Service.)
    - **Tenant Class of Service** (TCOS) is used with the ESMDI "Multi-Tenant" application to govern mailbox interaction between user communities. (See "ESMDI Integration" in the *NuPoint Unified Messaging Optional Integrations Guide* for more information.)
- **Message Waiting Types** specify how users are notified of unplayed messages in mailboxes. (See Message Waiting Types.)
- **Attendant Extension Numbers** are called when assistance is requested by a caller leaving a message in a mailbox or when outside callers request assistance through NuPoint Receptionist. (See Required Mailbox Information)
- NuPoint Receptionist processes calls according to individual users' requests.
    - **Treatment Types** assigned to mailboxes contain most instructions. (See NuPoint Receptionist Treatment Types.)
    - **Mailbox Extension Numbers** are checked when callers input an extension number; this is the actual number that the system dials; it can be programmed when the "extension" is outside the PBX network (see Programming NuPoint Receptionist to Dial an Outside "Mailbox's Extension.)

Outside Callers versus System Users

- An "outside caller" dials the system number, enters a mailbox number, listens to the mailbox greeting (or to the prompt, "Please leave a message for <name>"), and then leaves a message.
- A "system user" logs in to his or her own mailbox and uses the make, give, or answer command to leave a message.

The System Time/Date Stamp for Messages

The system adds the time/date stamp to every message to tell the recipient when the message was recorded.

- If the user plays the message on the same day that it arrives, only the time is given

  (for example: 2:00 p.m.).
- If the user plays the message on a later day within the same week, the day of the week and the time are given (for example: Monday, 2:00 p.m.).
- If the user plays a message more than a week after it was received, the day of the week, the date, and the time are given (for example: Monday, May 22, 2:00 p.m.).

26.17.1 Types of Mailboxes in a Typical Installation

Besides standard mailboxes, a server typically has an administrator's mailbox, up to five attendant's mailboxes, and other special mailboxes. Special mailboxes have all the characteristics of standard mailboxes, plus special privileges and capabilities.

Standard Mailboxes

A standard mailbox is a collection point for voice messages. It also has greetings and prompts associated with it and can be configured to provide an array of capabilities related to voice messaging. You use different classes of service to configure mailboxes to provide the required capabilities.

Special Mailboxes

The following special mailboxes are described in detail below:

- Administrator's mailbox
- Attendant's mailbox
- Broadcast
- Chain
- Check-In and check-out mailboxes
- Greeting-Only mailboxes
- Guest mailboxes
- NP OnDemand templates
- Rotational mailboxes
- Template mailboxes (NP Forms)
- Tree (bulletin board) mailboxes (including Shared Extension mailboxes)

Administrator's Mailbox

The initial software installation contains an administrator's mailbox that has these special privileges:

- Contains the company greetings
- Can create or edit master distribution lists that can be used by any mailbox owner in the server (with an appropriate FCOS)
- Can add mailboxes, delete mailboxes, and change mailbox configuration, by phone

For more information about the administrator's mailbox, see NuPoint Voice Application - Customize Administrator Mailbox.

Attendant's Mailbox

The initial software installation also contains an attendant's mailbox. This mailbox supplies these functions:

- Its greeting is the message of the day, which is stored only in the attendant's mailbox.
- A customized site tutorial (a form of greeting) can be recorded from the attendant's mailbox.
- When outside callers access the message center, they are prompted to enter a mailbox number or wait. Callers who wait are then prompted to leave a name and a message. These unaddressed messages are stored in the attendant's mailbox.

For more information about the attendant's mailbox, see NuPoint Voice Application - Customize Attendant Mailbox.

Broadcast Mailboxes

With a broadcast mailbox, any caller can send a single message to multiple mailboxes. In addition, mailbox owners can send names and greetings to other mailbox owners. This capability is particularly useful for disaster recovery or overflow mailboxes. Broadcast mailboxes other than broadcast message mailboxes can also send a message waiting status to multiple mailboxes.

To illustrate use of a broadcast message mailbox, suppose the manager of a company health club wants club members to know about an upcoming tournament. The manager logs in to his or her mailbox and makes a message for the broadcast message mailbox. The broadcast message mailbox, in turn, sends the message to all members' mailboxes (this is sometimes called the "bulletin board feature").

In this example, the server administrator assigns a Broadcast FCOS to one mailbox. The server administrator then creates distribution list 01 for that mailbox, including the mailbox numbers of all the club members, to a maximum of 65,535.

This is a useful feature if you have mailboxes accessed in different calling areas. You can update the greeting for all the mailboxes, and then callers can reach the local mailbox to get the information they need. Or, you could use it to broadcast to remote mailboxes through NP Net (an optional feature).

Broadcast Message Mailbox

A broadcast message mailbox must contain a distribution list 01. If you want the broadcast message mailbox to be able to keep messages that have been broadcast, it must first be able to receive messages. Add any of the "receive" feature bits to the broadcast message mailbox. Feature bit 043 (Receive message of the day) is needed only if the broadcast message mailbox is also the user's *only* mailbox. In the LCOS assigned to this mailbox, you should set a shorter message length so the mailbox will not fill up too quickly.

Broadcast Greeting, Name, or Passcode Mailbox

Broadcast greeting is a method of propagating a newly recorded or modified greeting to a list of mailboxes, similar to the method used for propagating messages with broadcast messages mailboxes. Broadcast name is identical in concept to broadcast greeting, except that newly recorded and modified names will be propagated to the broadcast list. Broadcast passcode is similar, except that it propagates a new mailbox passcode to the list.

You can create the broadcast list for a broadcast greeting, name or passcode mailbox like any distribution list, either from the User Options menu or from the List Maintenance Menu at the server maintenance console. All three of these mailbox types use distribution list 09. By assigning the appropriate feature bits to a mailbox, one, two, or all three of these capabilities can be performed by one mailbox.

Greeting

A broadcast greeting mailbox requires feature bit 174 (Define broadcast greeting) in its FCOS. All types of greetings and all names created or modified on these broadcast mailboxes will be broadcast, including:

- Day/night company greetings for the administrator's mailbox
- Message of the day
- Site tutorial for attendant mailboxes
- Multiple mailbox greetings

Name

You can record a name in the broadcast name mailbox and have it announced. The mailbox is defined by the presence of feature bit 178 (Define broadcast name mailbox) in the FCOS. Since the name in the mailbox should be the name of the recipient group, such as "Sales Bulletin Board," users must remember to state their names at the beginning of their messages. This name override capability is enabled through feature bit 123 (Announce broadcast mailbox name) in the mailbox FCOS. With this feature, if you do not record a name in the broadcast mailbox, the mailbox number is announced. In addition, answers to the messages are also broadcast. Without this feature, the server announces the name of the broadcast message originator, if that person is a server user. In this case, answers to a message go to the sender only. Outside callers must remember to announce their names if they want recipients to know who sent the message.

Passcode

You can change the passcode in the broadcast passcode mailbox and have it transmitted to all mailboxes in the distribution. This feature is enabled through feature bit 231 (Passcode Broadcast Mailbox) in the mailbox FCOS.

Multiple Mailbox Greetings

Mailboxes with multiple mailbox greetings defined broadcast each individual greeting as it is created or modified, and a recipient mailbox is checked to see if its FCOS has feature bit 175 (Receive broadcast greeting) or feature bit 179 (Receive broadcast name), or feature bit 232 (Allow receipt of passcode broadcasts). Mailboxes generating broadcast greetings that also have multiple mailbox greetings enabled can only send messages to recipient mailboxes that also have multiple mailbox greetings enabled.

Broadcast Message Waiting Status

The server also has the ability to automatically send the message waiting status of a mailbox to a distribution list of mailboxes without sending the actual message. This is useful in a business where any one of a number of people can respond to a message, but only one person needs to. A single response eliminates redundant answers to a message, thereby raising staff productivity and satisfying the sender of the message.

Example of Use

In a brokerage firm, any of six account executives can respond to potential clients' requests for information. If the request results in a sale, the account executive who answered the request receives credit for that sale.

Broadcasting the message waiting status of a mailbox gives this firm an easy and efficient way to pass these potential sales on to its brokers. The brokerage first routes all prospects to a main mailbox in which they can leave requests. When callers leave requests, the server automatically turns on the message waiting lights on brokers' phones. The first available broker then logs into the main mailbox and responds to the request.

Configuration Requirements

The broadcast message waiting status capability uses a server feature plus distribution list 01 of a mailbox:

- You must include feature bit 134 (Broadcast message waiting only) in the FCOS assigned to a mailbox before it can send its message waiting status to a distribution list.
- You must also set up distribution list 01 of a mailbox to include all the destination mailboxes to which to send the message waiting status of the main mailbox.

Multiple Mailboxes per User

Each mailbox in distribution list 01 always reflects the message waiting status of the main mailbox, regardless of how many messages are in that destination mailbox. Therefore, you may want to assign a separate mailbox to users for their messages and reserve the destination mailbox simply to notify them a message is in the main mailbox.

Incompatibility With Broadcast Message Feature

A mailbox can either send its messages or its message waiting status to the mailbox in its distribution list 01, but not both. This means the FCOS assigned to a mailbox cannot have both of these feature bits:

- 122 (Define broadcast mailbox)
- 134 (Broadcast message waiting only)

Combining Broadcast Mailbox Types

In addition to being a standard mailbox, a broadcast greeting, name, or passcode mailbox can also be a tree mailbox. A broadcast greeting, name or passcode mailbox can itself be a broadcast message mailbox that contains different broadcast lists for messages and greetings. To have both messages and greetings broadcast to the same list of recipients, it is necessary to make distribution lists 01 and 09 identical. List 01 controls the messages broadcast to recipients, and list 09 controls the greeting, name, or passcode broadcast to recipients.

Limits

Standard server limits on greeting and name length also restrict the broadcast greeting or name lengths for the sending mailbox; limits for recipient mailboxes are ignored.

Greetings will not be broadcast when modified through the console Greeting Copy/Delete Menu at the server maintenance console.

Statistical or billing information is not available for broadcast greeting activity.

Non-Delivery Receipts

Non-delivery receipts are deposited in the broadcast mailbox under any of the following conditions:

- The recipient mailbox does not have the appropriate bit in its FCOS to receive a broadcast greeting or name.
- A remote recipient mailbox could not be reached because of network blockage.
- A greeting could not be copied or recorded for a mailbox (local or remote) for miscellaneous reasons.

Chain Mailbox

Chain mailboxes play a greeting, then route calls to the mailbox selected by the caller. The chain mailbox itself cannot accept messages from users or callers. Chain mailboxes are useful for routing incoming callers. For example, a chain mailbox greeting could say, “Welcome to the Acme Company Credit Department. If you are calling about new home mortgages, enter 100 on your pushbutton phone. If you want to refinance your existing mortgage, enter 110. For car and truck loans, enter 120. If there is a problem with your credit report, enter 130. If you wish to speak to an operator, or have a rotary phone, please wait.” The caller can then dial the appropriate mailbox number and be transferred to it.

A mailbox owner can log into a chain mailbox and change the mailbox name, greeting, and passcode, but cannot make messages, or create or use distribution lists.

Check-In/Check-Out Mailboxes

These mailboxes are used by hotels.

A check-in mailbox is a special mailbox that manipulates other mailboxes. When a check-in mailbox is accessed, the server prompts for the mailbox number to be checked in, then prompts the caller (usually a hotel or motel attendant) to record a name and enter a passcode for the mailbox. More than one desk clerk can call into a single check-in mailbox at one time, so it is unnecessary to create more than one check-in mailbox for your server.

A check-out mailbox is the counterpart of the check-in mailbox. When the attendant calls a check-out mailbox, the server prompts for the mailbox number to be checked out. It then gives the attendant the choice of either keeping or discarding any messages left in the mailbox. Finally, the server purges the guest’s name, greeting and passcode, and follows the attendant’s command about messages. The mailbox is then ready to be checked in for the next guest.

A check-out mailbox must also be created to use the hotel check-in/check-out feature of the server.

Greeting-Only Mailboxes

When a caller reaches a Greeting-Only mailbox, the server plays the greeting and then hangs up. Greeting-Only mailboxes are established by assigning FCOS 6 (Greeting Only) or a similar FCOS to them.

To illustrate a use of a Greeting-Only mailbox, imagine that a theater manager wants callers to hear an announcement of show times. The manager would create a mailbox with this FCOS, call the mailbox, log in, then record a greeting.

The mailbox user can change the mailbox name, greeting, and passcode but cannot create or use distribution lists. No one can make messages for or give messages to a Greeting-Only mailbox.

A Greeting-Only mailbox must have a greeting; otherwise the server considers the mailbox invalid. To log in to a Greeting-Only mailbox that does not have a greeting, press the star (*) key on the phone key pad; then enter the mailbox number. You may choose to remove feature bit **066** (Login during greeting in Greeting-Only mailbox) after you record a greeting for the mailbox.

Guest Mailboxes

A guest mailbox is one that is assigned to each guest, typically in a hotel or motel. You establish a guest mailbox by assigning an FCOS, such as the Lodging FCOS described in the Feature Classes of Service section, to it. These mailboxes are particularly appreciated by users who might be unfamiliar with voice messaging systems, and their uninitiated callers.

The guest does not need to do any kind of mailbox set-up, such as recording a name and passcode, before using the mailbox.

The server can usually be integrated with the hotel/motel telephone system to allow the user to log in simply by pressing a button on the telephone and entering a passcode, when prompted by the server. Immediately after the guest logs in, the server will play the first message automatically. The guest is given the options of keeping or discarding the message; when the choice is made, the next message, if any, is played without any input from the guest.

Prompts for a guest mailbox are in the form, “Press P, the 7 key, to play your message....” in order to be most helpful to the uninitiated user.

Callers also hear these expanded prompts, “Press R, the 7 key, to review your message...”

As a variation, a hotel or motel may wish to assign the full-feature guest mailbox. This is a mailbox with FCOS 2 (Full Guest) or its equivalent in the mailbox configuration. The desk clerk would still check in this mailbox; however, the guest would be able to change the name and passcode, and would also be able to record a personal greeting, make messages for other guest’s mailboxes, and so on.

NP OnDemand Template Mailboxes

NP OnDemand is an optional feature where the NuPoint Unified Messaging system creates mailboxes only when they are needed. A NP OnDemand template mailbox is used as a model for the temporary mailboxes that this application creates. Typically, temporary mailboxes have their LCOS limits set to very small numbers (such as a day or two).

Rotational Mailbox

A rotational mailbox allows callers to hear greetings that change. Greetings change either by time and date (in a “period” rotational mailbox) or with every call (in an index type rotational mailbox).

A rotational mailbox of either the period type or the index type plays its greeting, then plays the greeting of a child mailbox. Distribution list 01 in the rotational mailbox controls the rotating (or cycling) of callers through the child mailboxes. Rotational mailboxes do not require greetings, which can be useful in some applications.

You make a standard mailbox rotational by assigning FCOS 17 (Rotational) to it. You make a standard mailbox a child mailbox by including it in the distribution list of the rotational mailbox.

Callers cannot leave messages in the rotational mailbox itself, but they can leave messages in one of the child mailboxes, if the child mailbox is assigned an FCOS that allows callers to leave messages. You may have up to 190 child mailboxes in the rotational mailbox's distribution list 01.

Note: You must use the **Text Console** to configure period- or index-type rotational mailboxes.

Period-Type Rotational Mailboxes

To illustrate a use of a period-type rotational mailbox, suppose that a restaurant owner wants all callers to hear the special of the day. Tuesday callers, for example, would hear the restaurant greeting and the special for Tuesday; Wednesday callers would hear the restaurant greeting and the special for Wednesday, and so on. Figure 5-7 illustrates this example.

In this example, the restaurant owner would assign FCOS 17 (Rotational Mailboxes) to one mailbox (mailbox 100) and record a restaurant greeting for this mailbox. For this mailbox, the owner would also create distribution list 01 containing seven child mailboxes (mailboxes 101-107). To each of the seven child mailboxes the owner would assign FCOS 6 (Greeting Only); for each the owner would also record the daily special. The owner would then set the start date and start time for the rotation and the length of time before the server rotates to the next mailbox (24 hours in this example).

Index-Type Rotational Mailboxes

The server assigns a sequential index to each member of the rotational mailbox's distribution list. If a sorted list is created, mailboxes are indexed starting with the lowest-numbered mailbox. If an unsorted list is created, mailboxes are indexed starting with the first mailbox entered in the list. The first caller reaches the first indexed mailbox; the second caller reaches the second indexed mailbox, and so on. When the last-indexed mailbox is reached, the cycle starts over at the first indexed mailbox.

As an example of an index-type rotational mailbox, imagine that a veterinarian wants pet owners to hear three pet-care messages over an unspecified period of time. Each tie pet owners call the veterinarian's number, they (are likely to) hear a different one of the three messages.

In this example (Figure 5-8) the veterinarian assigns FCOS 17 (Rotational Mailboxes) to one mailbox (mailbox 781) and records a standard veterinary-practice greeting for this mailbox. For this mailbox the veterinarian also creates distribution list 01 containing three mailboxes (mailboxes 711-713). To each of the three mailboxes, the veterinarian assigns FCOS 6 (Greeting Only); for each, the veterinarian also records a different pet-care message.

Messages

Callers cannot leave messages in the rotational mailbox itself, but they can leave messages in one of the child mailboxes, if the child mailbox is assigned an FCOS that allows callers to leave messages. You may have up to 190 child mailboxes in the rotational mailbox's distribution list 01.

Greetings

If you want the server to hang up after it plays the child mailbox greeting, assign a Greeting-Only FCOS to these child mailboxes, including feature bit 062 (Hang up immediately after greeting).

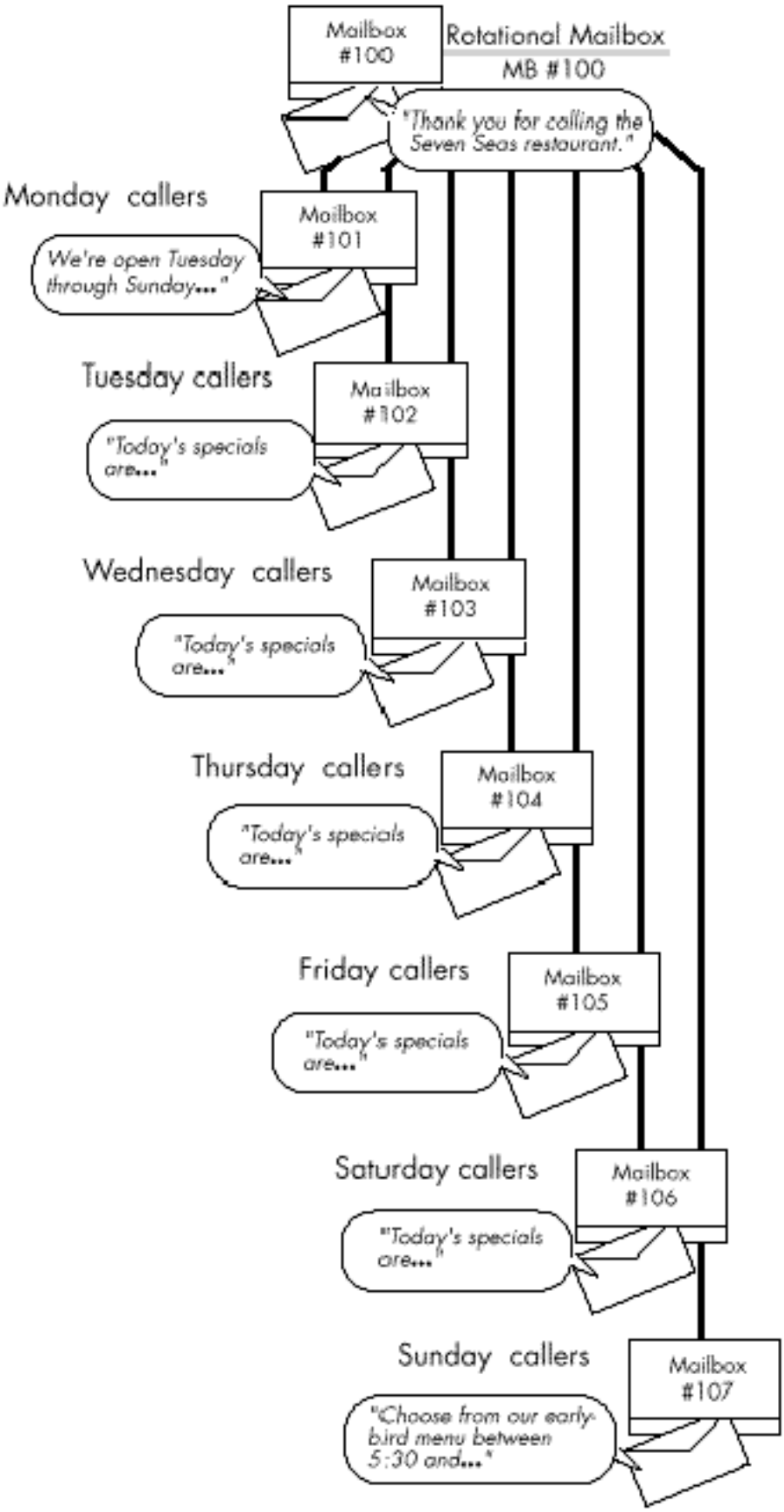
If you want each mailbox to provide an introductory announcement before connecting the caller with an employee, give the child mailboxes an FCOS that includes feature bit 063 (Call mailbox attendant after greeting) or feature bit 064 (Call mailbox's extension number after greeting). Do *not* include feature bit 062 (Hang up after greeting). Be sure to include the attendant's or extension number in the appropriate field when creating the mailbox.

Rotational mailboxes can also be used with NP Forms applications (see FCOS 16).

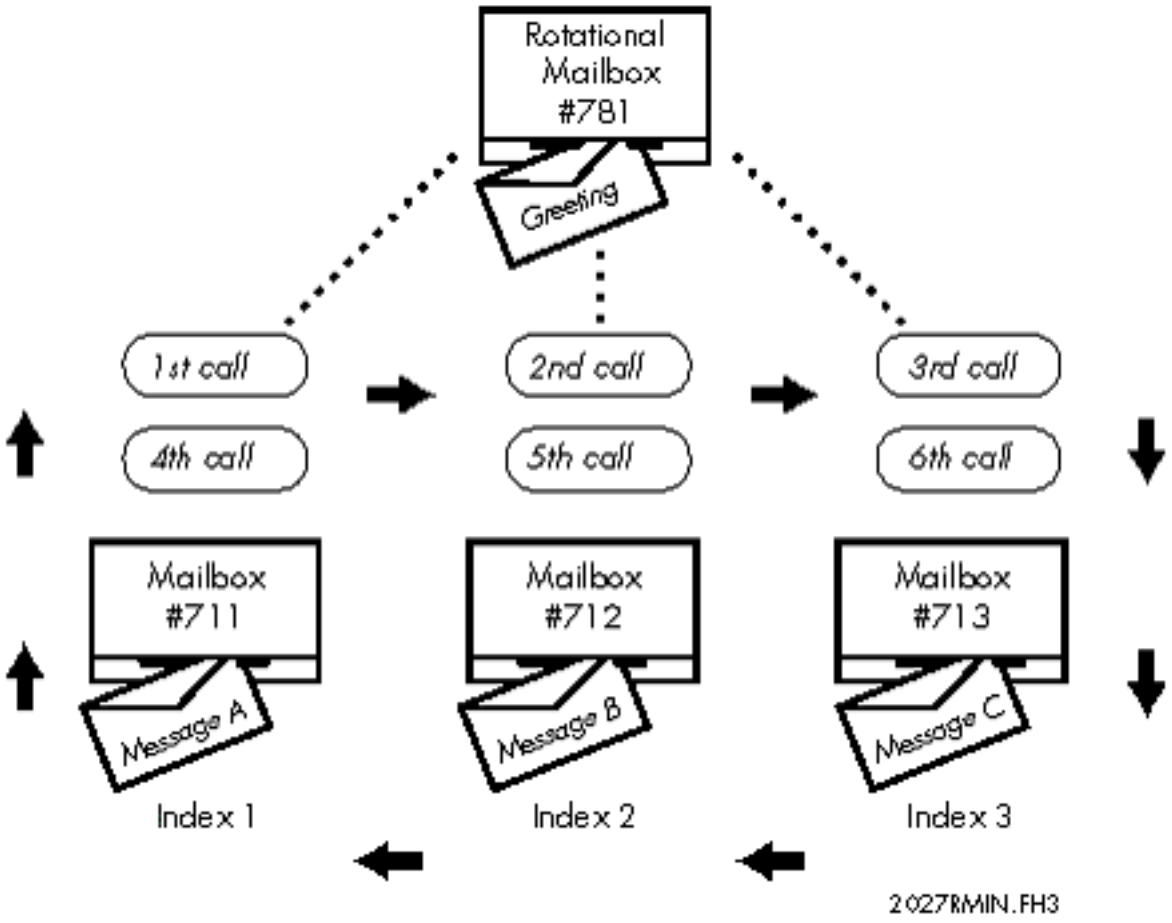
Mailbox Status

You can obtain information on existing rotational mailbox parameters, such as whether the mailbox is the period or index type, by using the Mailbox Dump option in the Mailbox Maintenance menu.

Sample Period-Type Rotational Mailbox


Mailbox #100
Rotational Mailbox
MB #100
"Thank you for calling the Seven Seas restaurant."
Monday callers
Mailbox #101
We're open Tuesday through Sunday..."
Tuesday callers
Mailbox #102
"Today's specials are..."
Wednesday callers
Mailbox #103
"Today's specials are..."
Thursday callers
Mailbox #104
"Today's specials are..."
Friday callers
Mailbox #105
"Today's specials are..."
Saturday callers
Mailbox #106
"Today's specials are..."
Sunday callers
Mailbox #107
"Choose from our early-bird menu between 5:30 and..."

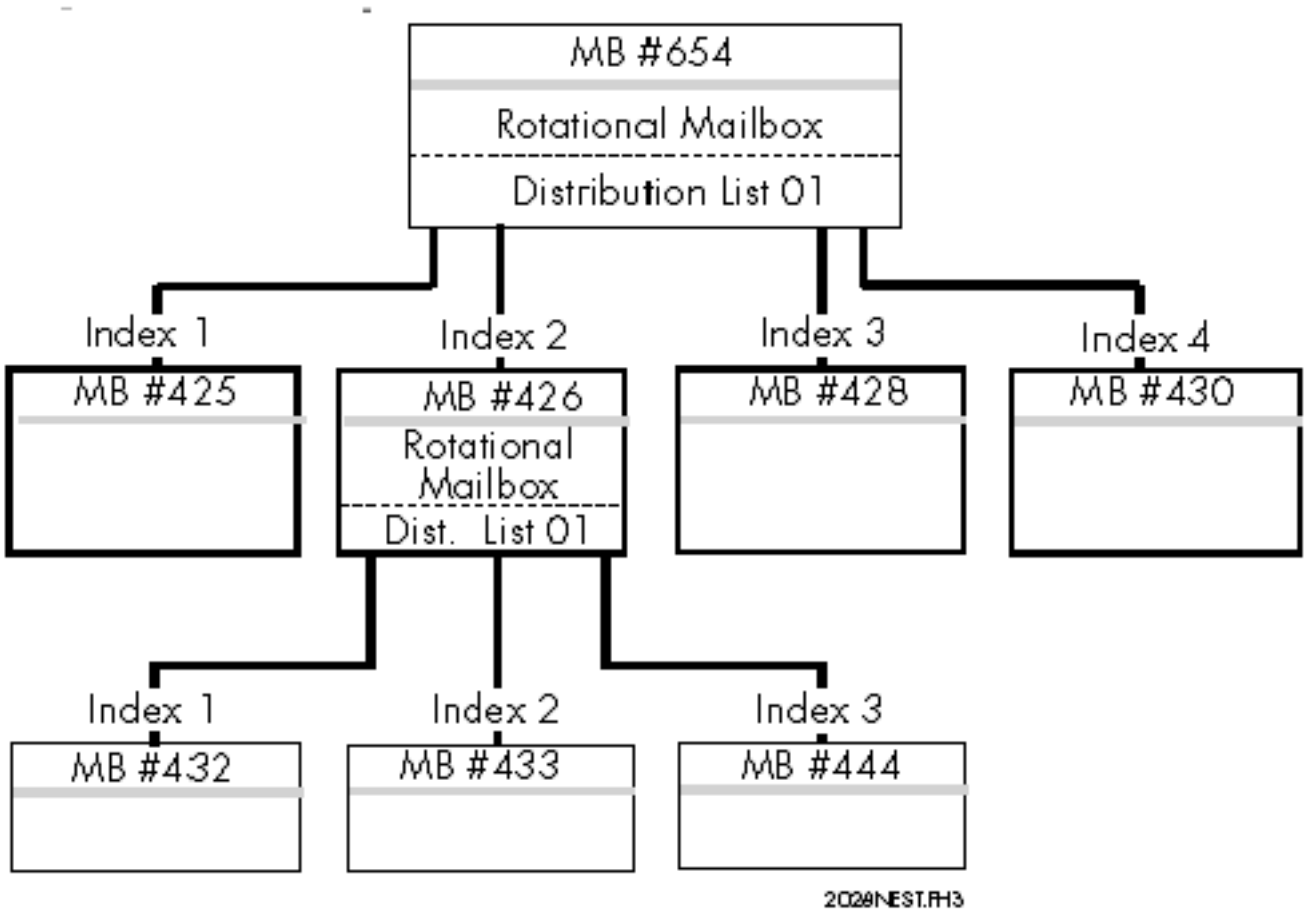
Sample Index-Type Rotational Mailbox



Nested Rotational Mailboxes

You can build nested rotational mailbox arrangements by making a child mailbox itself a rotational mailbox. The figure below shows an arrangement in which the rotational mailbox has three child mailboxes. One of the child mailboxes (mailbox 426) is itself a rotational mailbox, with three other child mailboxes (mailboxes 432, 433, and 444).

Sample Nested Rotational Mailboxes



Rotational Mailbox Diagram

Before configuring a rotational mailbox, complete a Mailbox Worksheet and a Rotational Mailbox Diagram. Each diagram entry is explained in the following paragraphs. Pre-programmed (default) values for entries are given, where applicable. If you want to use a default value, indicate that fact on the diagram. Then you will not need to select or enter any information for that parameter during re-configuration. The diagram below shows a sample Rotational Mailbox diagram. Blank worksheets and diagrams are here.

Mailbox No.

Enter the number of the rotational mailbox in the topmost box on the worksheet. Enter the numbers of all mailboxes that are members of the rotational mailbox's distribution list 01 (child mailboxes) in the remaining boxes. For every mailbox number you identify in the Rotational Mailbox Diagram, you should complete a corresponding Mailbox Worksheet. Blank worksheets are located in this manual.

FCOS

The FCOS assigned to a child mailbox determines its relationship to the rotational mailbox and also determines how it is used. For example, FCOS 17 or a customized equivalent enables a rotational mailbox; FCOS 6 or a customized equivalent enables the mailbox to give the caller information then hang up. Use either one of the defaults described in the Feature Class of Service section or customize an FCOS that includes all the applicable feature bits.

Index

If you want rotation to start at the first child mailbox in the rotational mailbox's distribution list 01, just enter a check mark; otherwise, enter the index number of the mailbox you want the rotation to start at. Rotation starts with the lowest-numbered index.

Period

If you want the rotation to cycle on a time-and-date basis, enter the number of hours in the period. This is the length of time before the server rotates to the next child mailbox. All callers reach the same mailbox in the distribution list during the stated period. (No index is necessary.)

Start date

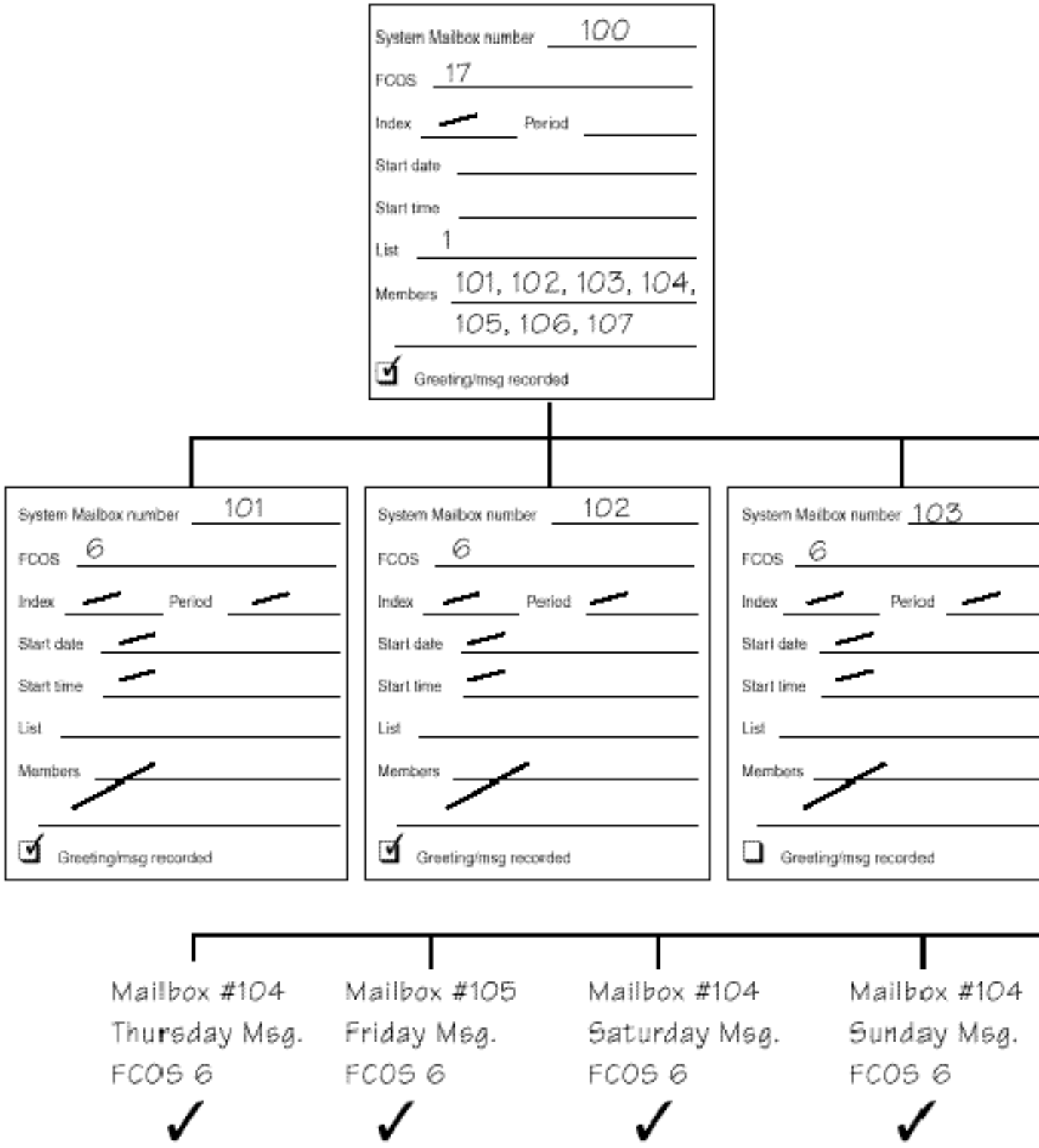
For the period type of rotation, enter the date on which the rotation cycle is to start.

Start time

For the period type of rotation, enter the time at which the rotation cycle is to start.

Sample Rotational Mailbox Diagram

Rotational Mailbox Worksheet



List

A rotational mailbox must have distribution list 01, whose members are the mailboxes that are rotated to. If the list is sorted when it is created, the rotation cycle begins with the lowest-numbered mailbox. If the list is unsorted when it is created, the rotation cycle begins with the first mailbox entered in the list. Distribution lists are allowed in child mailboxes (for example, to create a nested arrangement) but they are not needed for the rotational arrangement to work.

Members

Identify all child mailboxes as members of distribution list 01 in the rotational mailbox.

Template (NP Forms) Mailboxes

NP Forms is an optional feature, and provides an information template function (voice forms) for a server.

An NP Forms mailbox plays the greetings stored in its child mailboxes, sequentially, and records a message after each greeting. A typical application must have a rotational mailbox, with several child NP Forms mailboxes, all pointing to the same list of Greeting-Only mailboxes.

Tree Mailboxes

A tree mailbox provides a call routing capability. It plays a greeting then prompts the caller to enter a single digit to obtain more information. After entering the desired digit, the caller is routed to a child mailbox. A tree mailbox is sometimes called a “bulletin board” mailbox.

A mailbox owner can set up a tree mailbox by creating distribution list 01, then adding the numbers of the child mailboxes into this list. The lowest-numbered mailbox number can be reached by pressing 1 after the greeting, the next lowest-numbered mailbox number can be reached by pressing 2, etc. Up to 190 child mailboxes can be added. A greeting that directs a caller to enter an appropriate number must be recorded.

As an example of a tree mailbox, suppose that a major hotel chain wants to route callers to a particular reservations desk. The tree mailbox greeting could be: “Welcome to Globe Hotels’ world-wide reservation service. Press 1 for hotels in Canada and the US; press 2 for hotels in Mexico and South America; press 3 for hotels in Europe.” Figure 5-11 illustrates this arrangement.

To implement this arrangement, you would first plan for two series of numbers to be processed in the same order:

- The mailbox numbers for the three reservations desks
- The single-digit numbers callers press on the key pad to reach these mailboxes

The chart below gives an example.

Department	Mailbox #	Digit callers press to reach mailbox
Canada/US.	104	1
Mexico/S. America	106	2
Europe	107	3

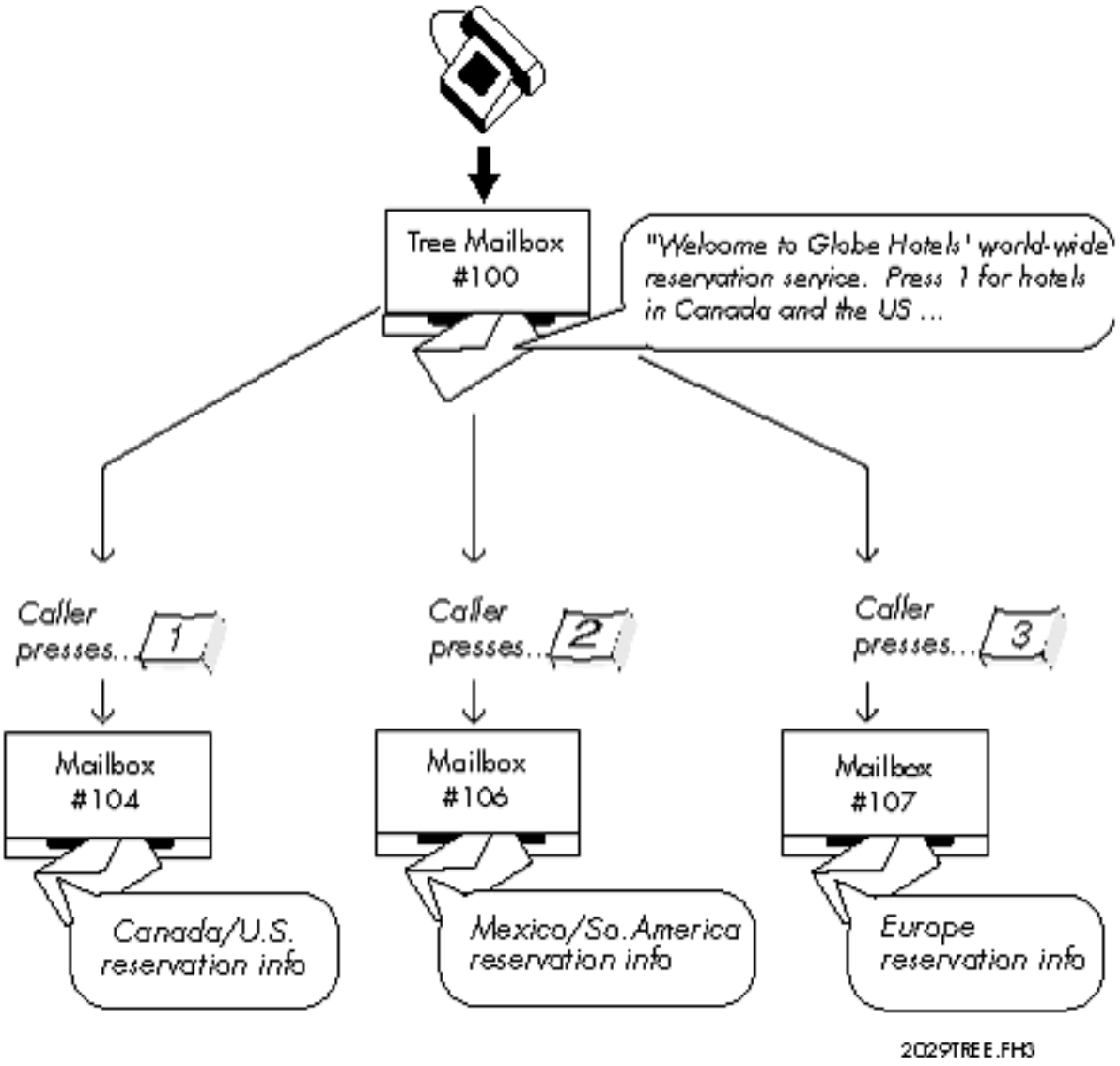
Second, you would assign the Tree FCOS to a standard mailbox that acts as the tree mailbox. You would then create standard mailboxes for each reservation desk to act as child mailboxes. Next, you would add

the child mailbox numbers to distribution list 01 of the tree mailbox. Finally, you would record a greeting, similar to the one mentioned earlier, for the tree mailbox.

Types of Child Mailboxes

Child mailboxes in the distribution list of a tree mailbox can themselves be trees or any other types of mailboxes. For example, by assigning an FCOS such as Unlimited or Restricted to a child mailbox, callers can leave messages.

Sample Tree Mailbox Arrangement



Server Assigns Caller Input Digits

The server assigns the digits 1, 2, and 3 to the mailboxes in distribution list 01: digit 1 to the first mailbox in the list, digit 2 to the second mailbox in the list, and so on. If the list is sorted, digit 1 is assigned to the lowest numbered mailbox, digit 2 to the next lowest numbered mailbox , and so on. If you assign additional mailboxes to the list, then you should change the tree mailbox's greeting to reflect the new

choices available. For sorted distribution lists, if you delete a mailbox from the list, or if new numbers are assigned to mailboxes, you must change the greeting to reflect the new order. These changes would not affect unsorted distribution lists.

More Than Nine Child Mailboxes

If you have more than nine child mailboxes, the server pauses briefly after single-digit entries to allow for more digits. To speed up processing, the greeting should tell users they can enter 2# instead of 2 for the second branch.

Routing of Calls

If callers do not enter a digit after listening to the greeting in a tree mailbox, they are routed to the attendant's mailbox.

- If feature bit 120 (Default to first child mailbox of tree mailbox) is included in the FCOS, callers are routed to the first mailbox in the list. The server then processes the call according to the FCOS assigned to the first child mailbox.
- Feature bit 186 (Default to last child mailbox of tree mailbox) works similarly, defaulting to the last mailbox in the list. The server then processes the call according to the FCOS assigned to the last child mailbox.

Shared Extension Mailbox

To configure a tree mailbox where several people share one telephone extension, you can use the suggested additional FCOS for Shared Extension Mailbox (see Features Class of Service).

Assign the following feature bits to the Tree mailbox:

- 229 Play names of list 1 children
- 234 Check message wait status of children

You will also need to consider the routing of calls. If callers do not enter a digit after listening to the greeting in a tree mailbox, they are routed to the attendant's mailbox. For this type of mailbox, you do not want this to happen. To avoid this situation, you can assign either of the following feature bits:

- 120 Default to first child mailbox of tree mailbox
- 186 Default to last child mailbox of tree mailbox

You could have a last mailbox that has a greeting only and then hangs up ("Nothing recorded, Good Bye."). In this case, distribution list 01 would contain the shared users and the last "good bye" mailbox, which can be shared throughout your extension mailbox applications.

The shared extension mailbox must contain distribution list 01 with all child mailboxes as members. You can record a greeting for the mailbox; the server automatically prompts the user with the child mailboxes' names.

Each child mailbox must have an FCOS that contains feature bit 134 (Broadcast message waiting only), and distribution list 01 with the parent mailbox as the only member. Each child mailbox can have a name recorded so the shared extension mailbox plays its greeting with user names. If you don't record a name, the mailbox number is played instead.

Here is an example of what a caller would hear: “You have reached Ivy Dormitory, room 18” (a custom greeting). Then follows a standard greeting: “To leave a message for Cindy Jones, press 1. To leave a message for Laura Smith, press 2.” If a user does not record a name, the prompt would be: “To leave a message for mailbox 203, press 3.”

A user of a shared extension mailbox would be prompted to enter the same digits when logging in, for example, “Hello Ivy Dormitory, room 18. To retrieve messages for Cindy Jones press 1, to retrieve messages for Laura Smith, press 2.” Then the user would be prompted with a name confirmation, and asked for the child mailbox’s passcode.

If a user moves to another room or telephone station, you can transfer the child mailbox to another shared mailbox extension without losing any messages.

Check both the current room mailbox and the moving to room mailbox distribution lists 01 for the following items:

- Are the members in the lists sorted or unsorted?
- When you make the change, which option will the move to room mailbox provide to the callers?

Note: When you are moving from one room to another, it is strongly recommended that the new member be at the end of the current members (just before the Good Bye mailbox number). You might have to write down the members sequence, and then delete all and re-input them in the needed sequence.

To do this, you would remove the child mailbox from distribution list 01, and add it to another shared mailbox extension’s distribution list. Then you would change the child mailbox’s distribution list to point to the new parent mailbox. All settings for the child mailbox, such as messages, greetings, name, etc. will remain intact.

NP Receptionist Considerations

Feature bit 121 (Define tree mailbox) lets a child mailbox also be a tree mailbox. Feature bit 141 (Define chain mailbox in NP Receptionist) allows a child mailbox to act as a chain mailbox. In addition, with these feature bits included in the mailbox’s FCOS, NP Receptionist can route a call from a chain mailbox to a tree mailbox and vice-versa.

Callers can bypass the single-digit tree options if they want to enter an extension number instead. In the greeting of the tree mailbox, tell callers they can press # to bypass the single-digit tree options. Be sure to tell callers that they can press # only while the greeting is playing; at any other time during the call, if callers press #, they will be disconnected. The greeting should also state that callers can reach an attendant by pressing 0.

Tree Mailbox Diagram

Before configuring a tree mailbox, complete a Mailbox Worksheet and a Tree Mailbox Diagram. Each diagram entry is explained in the following paragraphs. Pre-programmed (default) values for entries are given, where applicable. If you want to use a default value, indicate that fact on the diagram. Then you will not need to select or enter any information for that parameter during re-configuration. The diagram below shows a sample Tree Mailbox diagram. Blank Mailbox Group Worksheets are here.

Mailbox No.

Enter the number of the tree mailbox in the topmost box on the worksheet. Enter the number of all mailboxes that are members of the tree mailbox’s distribution list 01 (child mailboxes) in the remaining

boxes. For every mailbox number identified in the Tree Mailbox Diagram, there should be a corresponding Mailbox Worksheet completed (see “Mailbox Worksheets” later in this section).

Sample Tree Mailbox

FCOS

A The FCOS assigned to a child mailbox determines its relationship to the tree mailbox and also determines how it is used. For example, FCOS 15 (Tree) or a customized equivalent enables a tree mailbox; FCOS 17 (Rotational Mailboxes) or a customized equivalent enables branching to another mailbox; FCOS 6 (Greeting Only) or a customized equivalent enables the mailbox to give the caller information then hang up; FCOS 1 (Unlimited) allows the mailbox to play a greeting then allows a caller to leave a message. Use either one of the defaults described in the Feature Class of Service section or customize an FCOS to include all the applicable feature bits.

List

A tree mailbox must have distribution list 01, whose members are the mailboxes that are branched to when a caller presses the associated digit.

Members

Identify all child mailboxes as members of distribution list 01 in the tree mailbox.

Greeting recorded

You must record a greeting in the tree mailbox, to tell callers which digit to press for the desired mailbox. You should also record appropriate greetings or messages in the child mailboxes.

26.17.2 About Distribution Lists

This topic covers:

- How distribution lists are used in the server software
- Interactions between distribution lists and various class of service settings
- Distribution list administration

Overview

A distribution list allows a mailbox owner to send the same message to a number of recipients by entering the distribution list number instead of entering each mailbox number. Mailbox owners can create distribution lists by phone, or a server administrator can create them at the server maintenance console.

There are two types of distribution lists: mailbox owner distribution lists (sometimes called “user distribution lists”), which are only accessible by the mailbox owner, and master distribution lists (sometimes called “system distribution lists”), which are accessible by all users of a line group.

In addition to addressing messages, distribution lists control the actions of several special mailbox features. The distribution lists in tree mailboxes and rotational mailboxes identify child mailboxes, and the distribution lists in broadcast mailboxes identify the recipients of broadcast messages, greetings, and so forth.

Distribution list administration involves many parts of server administration:

- FCOS settings allow mailbox owners to send to and receive from distribution lists.
- LCOS settings control the maximum number of list per mailbox, up to 99, and the maximum number of recipients per list, up to 65,535.
- GCOS settings identify which mailboxes can exchange messages.
- Mailbox settings control the ability of mailbox owners to review and/or modify distribution lists.

Once you have configured mailboxes appropriately, you can create distribution lists – including master distribution lists – and maintain them from a telephone. In addition, you can create distribution lists from the server console using the List Maintenance Menu.

Mailbox Owner Distribution Lists

Mailbox owners can create up to 99 distribution lists for groups of people that they communicate with frequently. Mailbox owner distribution lists are only accessible by the mailbox owner. Although a server administrator can create distribution lists for any mailbox, it is usually easier to let the mailbox owners create and maintain their own lists.

When mailbox owners are given the capability to create and use their own distribution lists, the server plays the appropriate prompts and options in the User Options Menu. Besides adding and deleting members, mailbox owners can review the members of a list and record a spoken name for it to serve as a confirmation when addressing messages to the list.

A server administrator can control whether or not a mailbox owner can review or modify distribution lists. Turning off both capabilities can be useful for broadcast mailboxes, while turning off the modify capability can be useful in service bureau environments in which the service bureau maintains the lists for the customers.

Mailbox owners address messages to their distribution lists by pressing a 0 (zero) before the list number, for example “015” to address a message to distribution list 15. If feature bit 036 is enabled, the sender receives a receipt listing which recipients have and have not listened to the message.

Master Lists

Master lists are useful when more than one person must send messages to the same group of people. A master list is a line group-specific distribution list that you can define in the administrator’s mailbox for that line group. There can be up to 99 master lists. All mailbox owners who call in on that particular line group can use a master list by pressing “00” before the list number; for example, “009” to address a message to master distribution list 9, or “0025” for master list 25.

A master list defined for one line group is not necessarily a distribution list for another line group. They can share master lists if they share the same administrator’s mailbox.

Although you can create master distribution lists over the phone, it is usually easier to use the server maintenance console due to the size of some lists. It is often necessary to add newly-created mailboxes to one or more master list. You must use the phone to log in to the administrator’ mailbox and record spoken names for master distribution lists. For more information see Master Distribution Lists.

Distribution Lists and Special Mailboxes

Several types of special-function mailboxes use distribution lists to accomplish their purposes. These include:

- Tree and rotational mailboxes
- Broadcast message mailboxes
- Broadcast password mailboxes
- Broadcast greeting mailboxes
- Broadcast name mailboxes

Tree, rotational, and broadcast message mailboxes all use distribution list 1 to define child or recipient mailboxes. For tree and rotational mailboxes, the order of child mailboxes in the distribution list can affect what callers hear.

Broadcast greeting, name and passcode mailboxes use distribution list 9 to identify the recipients of the broadcasts. Using list 9 for these features allows these mailboxes to also perform other special functions, such as broadcast messages, which use distribution list 1. The mailbox owner can define the remaining distribution lists.

Nesting Distribution Lists

“Nesting” refers to the ability to make one distribution list a member of another list. This allows you to create a distribution list for each department, and then create a company-wide distribution list that only contains the department lists. Any changes to the department lists are automatically picked up by the company-wide list.

The server allows unlimited distribution list nesting by default, except in a broadcast mailbox. Nesting operates as shown in the figure.

Distribution List Nesting

Once the lists are set up, mailbox 301 can make a message to list 2, and the following mailboxes receive the message: 224 through 227, 101 through 104, and 401 through 403. Mailbox 104 only receives one copy of the message, even though it appears in both lists 3 and 4.

Feature bit 222 prevents mailbox owners from nesting distribution lists.

If you are creating the distribution list from the server console, identify a nested distribution list by including “D” before the list number (for example, D03). This is not needed when creating a list from the telephone; just enter the list number (for example, 03). For complete information refer to the Mailbox task list in this manual.

Note:

If you send a message to a nested list that contains many mailboxes, a mailbox owner can receive a message twice. This can happen if a mailbox appears in two lists and the mailbox owner receives the message while the server is still processing the rest of the list. If the mailbox owner discards the message, the server can send another copy when it reaches to the second occurrence of the mailbox. This is only an issue with very large nested distribution lists.

For more information see Nest a Distribution List.

Distribution List Interaction With FCOS

You can use the mailbox FCOS to control the ability to send messages to distribution lists, receive messages sent to other lists, or create or modify distribution lists. As described above, a feature bit prevents distribution list nesting. Additional feature bits control whether mailbox owners can use master distribution lists.

The feature bits listed here affect distribution list use.

Feature Bits that Control Distribution Lists	
Feature Bit	**Description**
032	**Make (messages) to user distribution list**
033	**Give (messages) to user distribution list**
034	**Make to master distribution list**
035	**Give to master distribution list**
036	**Auto-receipt for user distribution list messages**
044	**Receive user distribution list messages**
045	**Receive master distribution list messages**
074	**Create or modify user distribution list**
134	**Broadcast message waiting status**
222	**Deny nesting of distribution lists**

In addition, these limits affect distribution lists:

- Maximum number of distribution lists (maximum 99)
- Maximum recipients count (maximum 65,535)

For more information about Class of Service, see Features Class of Service.

Distribution List Interaction With LCOS

You can use LCOS settings to control the number of distribution lists per mailbox, the number of members per list, and the maximum number of recipients for any message. The specific limits that apply to distribution lists are:

- Maximum members per distribution list (maximum 65,535)
- Maximum number of distribution lists (maximum 99)
- Maximum recipients count (maximum 65,535)

You can use the “Maximum recipients count” limit to control the impact of nested distribution lists. The server does not deliver the message to more recipients than this limit allows, even if the total recipients in the nested distribution lists is greater.

Note:

The maximum for a distribution list in a tree or rotational mailbox is 190 members.

For more information about LCOS, see Other Classes of Service.

Distribution List Interaction With GCOS

Distribution lists are affected by the GCOS settings that control the ability of any mailbox owner to send messages to other mailbox owners. You must ensure that all members of a master distribution list have GCOS settings that allow them to exchange messages. Mailbox owners cannot add recipients who do not share GCOS settings to their distribution lists.

For more information about GCOS, see the Other Classes of Service section.

Mailbox Settings for Distribution Lists

Each mailbox has two parameters that are specific to distribution lists:

- Lists with review rights
- Lists with change rights

These parameters control which lists a mailbox owner can review or change. Review rights allow the owner to play the names and numbers of all mailboxes in a list. Denying review rights can keep the contents of a list confidential. Change rights allow the owner to add or delete mailboxes in a list. Denying change rights prevents the user from altering a distribution list, which is helpful for certain applications, such as networking, that require distribution lists.

List Maintenance

The List Maintenance Menu allows you to create, modify, delete and view distribution lists in any mailbox. You can also locate all lists that contain a specific mailbox, and delete that mailbox from all lists.

By using Administration by Phone you can create, modify, delete and review master distribution lists in an administrator's mailbox, and you can record names for those lists. From an administrator's mailbox you can create and modify master lists from 1 to 99, just like a mailbox owner's personal lists. Administrators' mailboxes do not have user (mailbox owner) distribution lists, only master lists.

26.17.3 About Names and Greetings

A mailbox owner can record a name for the mailbox. If the owner does not record a name, the server uses the mailbox number instead. For example, if you have mailbox 5731 and record "Kevin Lee" as your name, other users hear "Kevin Lee" when they make messages for your mailbox. If you do not record a name, users hear "Mailbox fifty-seven thirty-one." Users also hear mailbox names when they play messages from other users. If you get a message from an outside caller, no name is used.

Greetings are played when callers or users reach your mailbox, either by entering your mailbox number or by dialing your extension (if you have an integration that supports this feature). Mailbox owners can choose various types of greetings, depending on their FCOS. In many of the integrations that a server supports, owners can choose greetings that respond to the condition under which a call has been received by the server: Ring No Answer, Busy, or Forward. Personal greetings for these three possible conditions are called *conditional greetings*. To have the same greeting played under all conditions, a user would enable the *primary greetings*.

The general greeting option allows a user to select whether to use personal or server greetings. If conditional greetings are also enabled, the user can select conditional server greetings that play in response to line conditions as shown in the following table.

Greetings Supplied by the Server	
Condition	**Greeting**
Ring No Answer	**"I'm sorry, [name] does not answer. Please leave your message at the tone."**
Busy	**"I'm sorry, [name] is on another call. Please leave your message at the tone."**
Call Forward	**"I'm sorry, [name] is not available. Please leave your message at the tone."**

You can copy a mailbox greeting to a mailbox name and copy a mailbox name to a greeting.

26.17.4 Unplayed Messages and Message Receipts

NuPoint UM offers message processing flexibility in the related areas of:

- Defining what happens to unplayed messages
- Controlling when the server sends message receipts

Unplayed Messages

Feature bit **145** (Message stays in original queue) determines how the server classifies a message if a mailbox owner does not explicitly keep a message (by pressing K) or discard it (by pressing D).

Message Receipts

Feature bit **147** (Send receipt after full play) controls whether the server waits for a mailbox owner to explicitly keep a message (by pressing K) or discard it (by pressing D) before sending a receipt to the sender of that message. The server makes this decision only after a mailbox owner plays the entire message.

The presence of this feature bit works on a partially played message exactly as it does on a completely played message. Otherwise, it would be possible for the server to put a partially played message into a mailbox owner's saved queue but not send a receipt.

Feature bit 147 has an effect only when it is in the same FCOS as feature bit 145. Refer to Feature BitDescriptions for more information about how these two feature bits interact.

26.18 Mailbox Configuration Summary

When you create a mailbox, you are actually building a data file on the hard disk. As a minimum, the following five elements must be entered:

- Mailbox number (default is 1).
- FCOS (default is 1).
- LCOS (default is 1).
- GCOS (default is 1).
- Message waiting type #1.

This procedure summarizes the steps involved in configuring, maintaining, and searching for mailboxes.

Configure Mailboxes

1. Complete Mailbox Worksheets. An index of blank Mailbox Worksheets is located here

   .
2. Configure each **standard mailbox** in accordance with completed Mailbox Worksheets.
3. Configure **administrator's mailboxes**. One administrator's mailbox can be configured for each line group.

4. *Configure**attendant's mailboxes**. Up to five attendant's mailboxes per line group can be configured.*
5. Configure tree mailboxes, if needed.
6. Configure rotational mailboxes, if needed.
7. Configure broadcast mailboxes, if needed.

26.18.1 Mailbox Names with Accented Characters

NuPoint UM Releases 4.0 and later support the entry of accented names. The Speech Auto Attendant feature requires that you enter the accented character for proper recognition of the spoken name.

Note: If you have upgraded from a pre-4.0 release, your database may contain names that should contain accents. Please use the Web Console to modify these mailboxes to include the accented characters.

In Windows, you can use a combination of the ALT key and the numeric key pad to insert these accented characters:

Capital Letters			Lower Case Letters	
To type:	Press ALT +		To type:	Press ALT +
À	0192		à	0224
Â	0194		â	0226
Ä	0196		ä	0228
È	0200		è	0232
É	0201		é	0233
Ê	0202		ê	0234
Ë	0203		ë	0235
Î	0206		î	0238
Ï	0207		ï	0239
Ô	0212		ô	0244
Œ	0140		œ	0156
Ù	0217		ù	0249
Û	0219		û	0251
Ü	0220		ü	0252
Ÿ	0159		ÿ	0255
Ç	0199		ç	0231
Ö	0214		ö	0246
Æ	0198		æ	0230
Ø	0216		ø	0248
Å	0197		å	0229
Š	0138		š	0154
Ž	0142		ž	0158
ß	0223			

26.18.2 Configure an Overflow Mailbox

You can use an overflow mailbox to accept messages when a primary mailbox is full.

To configure an overflow mailbox:

1. Customize an FCOS to include feature bit 189 (Rotate on Full Mailbox).
2. Create a standard mailbox that will be the overflow mailbox, or use an existing standard mailbox and assign the customized FCOS.
3. Create Distribution List 1 for the primary mailbox, and add the overflow mailbox as the member. You can add more than one mailbox to the list and the server uses each one as an overflow mailbox when the previous overflow mailbox fills up.

When a new message is received by a full mailbox, it is routed to the first available mailbox in the full mailbox's Distribution List 1 (the overflow mailbox).

26.18.3 Configure a Broadcast Mailbox

This procedure describes how to configure these types of broadcast mailboxes:

- Broadcast **message** mailbox
- Broadcast **name** mailbox
- Broadcast **greeting** mailbox (including automatic transfer to an attendant or a mailbox extension)
- Broadcast **passcode** mailbox
- Broadcast **message waiting** mailbox

It also describes how to broadcast messages, names, and greetings to the same recipients.

To configure a broadcast mailbox:

1. Complete a Mailbox Worksheet. Blank Mailbox Worksheets are here.
2. Enter the requested information, as described in the following sections, from your completed worksheet.

Broadcast Message Mailbox

1. Customize an FCOS to include the following feature bits:
   - **40** (receive messages from other users)
   - **44** (receive user distribution list messages)
   - **122** (define broadcast mailbox)
2. Configure a broadcast message mailbox (same as a standard mailbox) and assign the new FCOS.
3. Create Distribution List 1 for the broadcast message mailbox just configured, adding as members all the mailboxes that are to receive messages made for the broadcast mailbox.

Broadcast Name Mailbox

1. Customize an FCOS to include feature bit **178** (define broadcast name mailbox).
2. Configure a broadcast message mailbox (same as a standard mailbox) and assign the new FCOS.
3. To every receiving mailbox, assign an FCOS that includes feature bit **179** (receive broadcast name).
4. Create Distribution List 9 for the broadcast name mailbox, adding as members all the mailboxes that are to receive names sent on from the broadcast mailbox.

Broadcast Greeting Mailbox

1. Customize an FCOS to include feature bit **174** (define broadcast greeting mailbox).
2. Configure a broadcast message mailbox (same as a standard mailbox) and assign the new FCOS.
3. To every receiving mailbox, assign an FCOS that includes feature bits:

   - **161** (enable mailbox's conditional greetings)
   - **162** (enable mailbox's general greetings)
   - **175** (receive broadcast greeting)
4. Create Distribution List 9 for the broadcast greeting mailbox, adding as members all the mailboxes that are to receive greetings sent on from the broadcast mailbox.

Broadcast Greeting Then Transfer to an Attendant

1. Customize an FCOS to include the following feature bits:

   - **63** (call mailbox attendant after greeting)
   - **174** (define broadcast greeting mailbox)
2. Configure a broadcast greeting mailbox as described above and assign the new FCOS.
3. For the **Attendant extension number** parameter, enter the number of the attendant's extension that the caller is to be automatically transferred to after playing the greeting.

Broadcast Greeting Then Transfer to a Mailbox Extension

1. Customize an FCOS to include the following feature bits:

   - **64** (Call mailbox user extension after greeting)
   - **174** (define broadcast greeting mailbox)
2. Configure a broadcast greeting mailbox as described above and assign the new FCOS.
3. For the **Mailbox's extension number** parameter, enter the number of the mailbox's extension that the caller is to be automatically transferred to after playing the greeting.

Broadcast Passcode Mailbox

1. Customize an FCOS to include feature bit **231** (Passcode broadcast mailbox).
2. Configure a broadcast greeting mailbox as described above and assign the new FCOS.

3. To every receiving mailbox, assign an FCOS that includes feature bits:

   - **125** (Clear user passcode)
   - **232** (Allow receipt of passcode broadcasts)
4. Create Distribution List 9 for the broadcast passcode mailbox, adding as members all the mailboxes that are to receive the broadcast passcode.

Broadcast Message Waiting Mailbox

1. Customize an FCOS to include feature bit **134** (Broadcast message waiting only).
2. Configure a broadcast greeting mailbox as described above and assign the new FCOS.
3. Create Distribution List 1 for the broadcast message waiting mailbox, adding as members all the mailboxes that are to receive the message-waiting status.

Same Recipients for Messages, Names, and Greetings

1. Create Distribution Lists 1 and 9 for the broadcast message mailbox. Make the two lists identical.
2. *Use Distribution List 1 for broadcasting messages.*
3. Use Distribution List 9 for broadcasting names and greetings from the broadcast message mailbox.

26.18.4 Configure a Shared Extension Mailbox

This capability allows multiple users who share a telephone extension to each have their own private mailbox.

To configure the shared-extension capability in a tree mailbox:

1. Configure a tree mailbox and assign a customized FCOS that includes the following feature bits:

   - All the feature bits typically required for a tree mailbox, as in FCOS 15 (Tree)

   - **229** (Play names of list 1 children)
   - **234** (Check message wait status of children)
2. Add the same GCOS to the tree mailbox that is assigned to its child mailboxes (the mailboxes that share the extension).
3. For each child mailbox:

   - Assign an FCOS that includes feature bit **134** (Broadcast message waiting status).

   - Assign the same GCOS that you assigned to the tree mailbox.
4. Create Distribution List 1 for the tree mailbox just configured, adding all the child mailboxes.
5. Create Distribution List 1 for each child mailbox. Make the tree mailbox the only member.
6. Record a greeting for the tree mailbox. For example, "Thank you for calling Redwood Realty." The server automatically supplements this greeting with directions for the caller to press a different number for each person sharing the tree mailbox (extension). For example, "To leave a message for John McSales, press 1, for Jane VanBroker, press 2, for Lee Smith, press 3."

7. Direct mailbox owners of the child mailboxes to record their own names and greetings in their respective mailboxes, if wanted.

26.18.5 Configure a Chain Mailbox

To configure a chain mailbox:

1. Complete a Mailbox Worksheet. Blank worksheets are here.
2. Create a new mailbox (or modify an existing mailbox) and assign **FCOS 8** (the default Chain FCOS) or another FCOS that contains all feature bits applicable for chain mailboxes.
3. Record a mailbox owner's greeting for the chain mailbox.

26.18.6 Implement a Tree Mailbox

A tree mailbox plays a greeting and ends with a prompt to enter a single digit to obtain more information. When the caller presses a digit, the call is transferred to another (child) mailbox or to the operator. A tree mailbox is sometimes called a "bulletin board" mailbox. FCOS 15 is the default Tree FCOS.

Tree Mailbox Worksheet/Diagram

Before configuring a tree mailbox, complete a Mailbox Individual Worksheet and a Tree Mailbox Worksheet. (Blank worksheets are available here.) Include the following information:

- **Mailbox number:** Enter the number of all mailboxes that are members of the tree mailbox's distribution list 01 (child mailboxes) in the remaining boxes.
- **FCOS:** The FCOS assigned to a child mailbox determines its relationship to the tree mailbox and also determines how it is used.
- • Use one of the default FCOS or a customized FCOS that includes all applicable feature bits. (See Step 2. Create 'Root' Mailbox with FCOS 15, below.)
- **List:** A tree mailbox must have distribution list 01, whose members are the mailboxes branched to when a caller presses the associated digit.
- **Members:** Identify all child mailboxes as members of distribution list 01 in the tree mailbox.
- **Greeting recorded:** You must record a greeting in the tree mailbox to tell callers which digit to press for the desired mailbox.
- • Also record appropriate greetings or messages in the child mailboxes.

To Configure a Simple Tree Mailbox

Use the following steps to configure a simple tree mailbox:

1. Complete a Mailbox Individual Worksheet and a Tree Mailbox Worksheet.
2. If required, customize an FCOS based on the default FCOS 15 to add the following optional feature bits:

1. • To route callers who do not enter a digit promptly after the Tree mailbox greeting to the **first** child mailbox, add feature bit **120** (default to first child of mailbox).
   • To route these callers to the **last** child mailbox, include **feature bit 186** (default to last child of tree mailbox)

1. Create a "Root" mailbox and assign the default or customized Tree FCOS.
2. In the child mailboxes, disable the Tutorial.
3. Create Distribution List 01 for the Tree mailbox just configured.
4. Add the numbers of all child mailboxes to this list:

1. • To reach the lowest mailbox number, press 1 after the greeting.
   • To reach the next mailbox number, press 2, and so on.
   • Up to 190 child mailboxes can be added.

1. Record an appropriate greeting in the tree mailbox and all child mailboxes to direct callers to enter the appropriate numbers.

1. • If you delete a mailbox from the list or if you assign new numbers to mailboxes, you must change the greeting to reflect the new order. In other words, you must re-assign list entries because the system assigns caller input digits.
   • If the appropriate FCOS bits are set (FCOS bits 120 or 186, see Step 2) and callers do not enter a digit after listening to the greeting in a tree mailbox, callers are routed to the attendant's mailbox or to the first or last child mailbox.

To Configure a Nested Tree Mailbox

1. Select the child mailbox that you want to set up as a Tree mailbox.
2. Configure the mailbox as described under To Configure a Simple Tree Mailbox, above.
3. Create Distribution List 1 for the newly-configured nested tree mailbox by adding all child mailboxes (related to the nested tree mailbox) as members.
4. Record a greeting in the nested tree mailbox.

Notes on Tree Mailboxes

- Child mailboxes in the distribution list of a tree mailbox can be tree (or any other type of) mailboxes.
- • Using NP Receptionist, feature bit **121** (Define tree mailbox) allows a child mailbox to also be a tree mailbox.

  • Feature bit **141** (Define chain in mailbox in NP Receptionist) allows a child mailbox to act as a chain mailbox.

  • With these feature bits included in the mailbox's FCOS, NP Receptionist can route a call from a chain mailbox to a tree mailbox and vice-versa.

  • Callers can bypass the single-digit tree options if they want to enter an extension number instead. *For example:* By assigning an FCOS such as Unlimited or Restricted to a child mailbox, callers can leave messages.
- The system processes the call according to the FCOS assigned to the selected child mailbox.
- • If feature bit **120** (Default to first child mailbox of tree mailbox) is included in the FCOS, callers are routed to the first mailbox in the list.

  • Feature bit **186** (default to last child mailbox of tree mailbox) works similarly by defaulting to the last mailbox in the list.

When the tree mailbox is built in the administrator's mailbox, the tree mailbox greeting should:

1. • Instruct callers to press the # key (pound) to bypass the single-digit tree options.
   • State that callers can reach an attendant by pressing 0 (zero).

Note: Be sure to tell callers to press the # key (pound) only while the greeting is playing; at any other time during the call, if callers press #, they are disconnected.

EXAMPLE: SIMPLE TREE MAILBOX

A major hotel chain wants to route callers to a particular reservations desk. The tree mailbox greeting says, "Welcome to Globe Hotels' world-wide reservation service. Press 1 for hotels in Canada and the US; press 2 for hotels in Mexico and South America; press 3 for hotels in Europe."

To Implement this Arrangement:

1. Plan for two series of numbers to be processed in the same order:
   - Mailbox numbers for the three reservations desks.
   - Single-digit numbers callers press on the telephone keypad to reach these mailboxes. The following table illustrates the example.

Department	Mailbox #	Digit callers press to reach mailbox
Canada/US	104	1
Mexico/South America	106	2
Europe	107	3

2. Assign the Tree FCOS to a standard mailbox that acts as the tree mailbox.
3. Create standard mailboxes for each reservation desk to act as child mailboxes.
4. Add the child mailbox number to distribution list 01 of the tree mailbox.
5. Record a greeting (similar to the one mentioned in this example) for the tree mailbox.

26.18.7 Implement a Rotational Mailbox System

A rotational mailbox plays its greeting, and then plays the greeting of a child (distribution list) mailbox. The child mailbox greeting is selected by "rotating" through the mailboxes in distribution list 01 of the rotational mailbox. Mailbox rotation can be triggered by one of two methods: **index** or **period**.

Note:
Setting **index** and **period** can not be performed in the Web Console. Use the Text console to configure.

Index Method

When you create distribution list 01 in the rotational mailbox:

- Index number 1 is automatically assigned to the lowest mailbox number in the list; index number 2 to the next highest number, and so on.
- Every time the rotational mailbox is called, the system plays the rotational mailbox greeting and plays the greeting of the mailbox that matches the current index.
    - After this greeting plays, the counter increments by one.
- The next time that the rotational mailbox is accessed, the system plays its greeting and the greeting of the mailbox that matches the new index.
- When the greeting of the last mailbox in distribution list 01 plays, the system rotates back to the first mailbox on the list, resets the index to 1, and begins the cycle again.
    - Default index is 1 (that is, the cycle begins with the lowest mailbox on the list). You may set the index to a higher number if you want the cycle to begin with a different mailbox.

Period Method

The greeting of the first mailbox in distribution list 01 plays for the specified period, and then the second mailbox greeting plays for the specified period.

A start date and start time for the cycle must be set. After all mailboxes in the distribution list are accessed for the specified period, the system resets the start date and time to the date and time of the last call. Then the cycle begins again, with the greeting of the first mailbox in the list.

Prepare the Mailboxes

In this application you are working with a rotational mailbox and a child (distribution list) mailbox. The following table summarizes the steps to prepare these mailboxes.

Rotational Mailbox	Child Mailbox
1. Customize a rotational mailbox FCOS.	1. Create the mailboxes
2. Create a mailbox with this FCOS.	2. Log in to the mailboxes, and record suitable greetings.
3. Set the index or period.	
4. Set up the distribution list. (This step must be done aft er distribution list mailboxes are created).	
5. Log in to the mailbox and record a greeting	

Note:
In practice, combine some of these steps for efficiency.

To Configure a Rotational Mailbox System

Steps 1 through 4 outline a general plan for setting up a rotational mailbox and its child mailboxes.

Step 1: Create Mailboxes

1. Create one mailbox with the rotational mailbox FCOS that you configured.
2. Create as many child mailboxes as you need. Choose an FCOS that suits the application.

EXAMPLES:

- If you want the system to hang up after it plays the child mailbox greeting, assign a Greeting-only FCOS to the mailboxes.
- If you want each mailbox to provide an introductory announcement before connecting the caller with an employee, give the child mailboxes an FCOS that includes feature bit **063** (Call mailbox attendant after greeting) or feature bit **064** (Call mailbox's extension number after greeting). Be sure to include the attendant's extension number in the appropriate field when creating the mailbox.

Note:
The rotational mailbox and all child mailboxes must be in the same GCOS.

Step 2: Set the Index or Period for the Rotational Mailbox

The index tells the system which mailbox in the distribution list should begin the cycle. The system automatically rotates to the next mailbox in the list on each subsequent call.

The period defines how long to play the current child mailbox greeting before rotating to the next greeting. If you specify a period, it will override the index.

This procedure is only available in the **Text console**. See Configure a Rotational Mailbox .

Step 3: Prepare the Rotational Mailbox

1. Call the system and log in to the rotational mailbox.
2. Press **U** (the 8 key) for User Options.
3. Press **L** (the 5 key) to change a distribution list. You are prompted for a distribution list number.
4. Enter **01**.
5. Press **A** (the 2 key) then enter the number of a child mailbox.
6. Repeat Step 5 until all child mailboxes have been added to the list. Press **X** (the 9 key) to save the changes.
7. Press **U** (the 8 key) for User Options.
8. Press **G** (the 4 key), then record a Greeting.

9. Press **X** (the 9 key) to save the changes. Press **X** *twice in quick succession* to exit the mailbox and recycle to the system greeting.

Step 4: Prepare the Child Mailboxes

1. Log in to the **first** child mailbox.
2. Press **U** (the 8 key) for User Options.
3. Press **G** (the 4 key) and record a greeting.
4. Press **X** (the 9 key) to save the changes. Press **X** *twice in quick succession* to exit the mailbox and recycle to the system greeting.
5. Log in to the **next** child mailbox.
6. Repeat steps 2 through 5 until all mailboxes have suitable greetings.

26.18.8 Passcode Expiry

Overview

In the interest of increased security, you can configure an expiry period for mailbox passcodes from 1 to 365 days. To disable the passcode expiry feature, ensure that it is set to the default value of "0".

Enforcement of the passcode expiry is performed through the TUI interface. Users who log in to the TUI of an expired mailbox are prompted to enter a new passcode.

UM users who do not use the TUI are unaffected by passcode expiry behavior. UM email messages continue to be synchronized and delivered after passcode expiry. Web View users can continue to log in.

Conditions and Limitations

- This feature is not supported for MiCollab deployments of NuPoint Unified Messaging and must be left at the default setting of "0" expiry.
- By default, the TUI plays back the new passcode to the user. To change this operation to a prompt to "Re-enter new passcode", TUI users must have FCOS feature bit 300 - Enable Secure Tutorial assigned.
- New passcodes are valid only if:
  - they meet existing NP-UM passcode restrictions
  - they differ from the most recent passcode
  - they are successfully confirmed by the TUI (when feature bit 300 - Enable Secure Tutorial is assigned)

26.18.9 Assign Alternate Extensions to a Single Mailbox

The Alternate Extension feature is used to assign multiple extension numbers to a single mailbox. You can add four more extension fields to the mailbox record for a total of five phone numbers that can be associated with one mailbox. The first extension is the primary extension; the other four are alternate extensions.

Call Behavior

Call behavior depends on the call scenario. The Receptionist feature and FCOS bit 64 use the primary extension to transfer calls as before. All the extension fields are used by this new feature to match against incoming calling IDs.

The following describes a few call scenarios:

1. Calling from any of the mapped extensions to voice mail is greeted by the login prompt of the mailbox that has the mappings.
2. A call to a teleworker phone that then forwards to voice mail is greeted by the desk phone's mailbox's greeting.
3. A call to a cell phone that then forwards to a DID number on the switch that ends up at the desk phone will get ring back while the desk phone is ringing. If the call is not picked up, the desk phone forwards to voice mail and the caller hears the desk phone's mailbox's greeting.
4. When an MWI action is instigated, only the set on the switch whose extension matches the mailbox number is affected. This extension may or may not be one of the 5 mapped to the mailbox.

In general, alternative extensions are used for non-desktop telephone numbers (for example, cell phones or teleworker phones). However, the system does not prevent you from associating desktop telephone extensions with the primary mailbox.

Configuration

Depending on the integration and call scenarios, configuration for this feature can be quite different. However, there are always three common aspects:

- Set configuration
- Switch configuration
- NuPoint Unified Messaging configuration

Example:

MiVoice Business ICP Integration – desk phone and teleworker phone

In this scenario, a MiVoice Business ICP user has a desk phone and a teleworker phone. This user would like these two phones to have the same mailbox and get the same voice mail integration with each of the two phones.

Set configuration:

- Configure the teleworker set to forward to the voice mail hunt group. This should be the same as forward configuration for the user's desk phone.

Switch configuration:

- Same as set configuration.

NuPoint configuration:

1. Create a mailbox matching the extension of the user's desk phone.
2. Set the primary extension to the extension of the user's desk phone (i.e. use the default value).
3. Set the alternate extension #2 to the extension of the user's teleworker phone.

   Assuming that the extensions are of the same length, the extension dial plan of the line group for incoming calls does not have to change. (Otherwise, the flexible 'r;v' dial plan would have to be used.)
4. Configure the mailbox extensions.

26.18.10 Unplayed Messages and Message Receipts

NuPoint UM offers message processing flexibility in the related areas of:

- Defining what happens to unplayed messages
- Controlling when the server sends message receipts

Unplayed Messages

Feature bit **145** (Message stays in original queue) determines how the server classifies a message if a mailbox owner does not explicitly keep a message (by pressing K) or discard it (by pressing D).

Message Receipts

Feature bit **147** (Send receipt after full play) controls whether the server waits for a mailbox owner to explicitly keep a message (by pressing K) or discard it (by pressing D) before sending a receipt to the sender of that message. The server makes this decision only after a mailbox owner plays the entire message.

The presence of this feature bit works on a partially played message exactly as it does on a completely played message. Otherwise, it would be possible for the server to put a partially played message into a mailbox owner's saved queue but not send a receipt.

Feature bit 147 has an effect only when it is in the same FCOS as feature bit 145. Refer to Feature BitDescriptions for more information about how these two feature bits interact.

26.18.11 Message Waiting Types

The mailbox message waiting type tells the system what equipment, if any, is available to notify a mailbox owner of unplayed messages.

Note: The MITEL SX-200 DIGITAL PABX and SX-2000 PABX use message waiting types 0, 3, 5, and 7 only.

Default Message Waiting Types

MWI Type	Description
0: None	No message notification is available.
1: Not available	The mailbox does not have any message notification c apabilities.

MWI Type	Description
3: DTMF-to-PBX	The system sends DTMF signals over the telephone lines to control PBX message waiting indicators. This method is compatible only with certain PBXs. For this protocol to be used, the technician must program codes to control lights and to configure a line group with at least one port dedicated as a message lights outdialer.
5: Pager	This message waiting type is used to activate a radio pager, or to provide message delivery, when a message is left in a mailbox. The Pager application must be configured for the system to support pagers and/or message delivery. Mailbox programming for this message waiting type is complex. Refer to Pagers and Message Delivery, for information on adding a pager or programming message delivery for a mailbox.
7: Program RS232	Allows servers to turn PBX message waiting indicators on and off by sending signals to the PBX over RS-232 d ata links. The data links connect to modems that are con nected to analog ports on the PBX.
11: Centrex	Allows servers to turn PBX message waiting indicators on and off by sending signals to the PBX over RS-232 d ata links. The data link is a direct serial connection to th e PBX.
16: HIS PMS	Optional RS-232 message waiting system for PMS
17: Unified Integrations	Outgoing MWI programming for mailboxes with mapp ings from several extensions. See ESMDI in the NuPoint UM Optional Integrations Guide for more information.
28: MiTAI Messaging	MiTAI MWI uses proprietary MiTAI messaging to co mmunicate directly with the MiVoice Business ICP to acti vate message waiting indicators on designated phones.

26.19 Distribution List Configuration

This procedure summarizes the steps for allowing distribution lists as a user option, and for configuring the available types and functions of distribution lists in a server.

1. Customize an FCOS to include some or all of the following feature bits, as applicable:

   - **20** (make messages)
   - **24** (give messages)
   - **32** (make to user distribution list)
   - **33** (give to user distribution list)
   - **34** (make to master distribution list)
   - **35** (give to master distribution list)
   - **36** (auto-receipt for user dist list msgs)
   - **40** (receive messages from other users)
   - **44** (receive user dist list messages)
   - **45** (receive master dist list messages)
   - **70** (User Options Menu)
   - **74** (create or modify user distribution list)

   Note:
   Feature bit 74 alone does not allow all distribution lists to be modified; you must also allow change rights in the mailbox configuration.

2. Customize an LCOS to include the desired limits parameters from the table below:

   - Max Number of Distribution Lists
   - Max Members Per Distribution List
   - Max Recipients Count
   - Min Number of Recipients for Receipt Summary
   - Other limits parameters as required

3. Customize a GCOS to include a group shared by all members of the same distribution list.
4. Configure the appropriate mailboxes, entering the correct FCOS, LCOS, GCOS and allowing review and change rights for distribution lists as required.

After mailboxes have been appropriately configured, distribution lists (including master distribution lists) can be created and maintained from the mailboxes. In addition, you can create distribution lists for mailbox owners (and master distribution lists) from the List Maintenance Menu.

Web Console:

- *Configure a Mailbox for Distribution Lists*

Text Console:

- *Configure a Mailbox for Distribution Lists*

26.19.1 Configure for Name and Greeting Broadcast

The mailbox used for broadcasting greetings or names can be a standard mailbox, broadcast mailbox, or tree mailbox.

To use a distribution list for broadcasting greetings or names:

1. Customize an FCOS to include the following feature bits, as applicable:
   - **174** (define broadcast greeting mailbox) in the FCOS assigned to the mailbox that will broadcast greetings.
   - **175** (receive broadcast greeting) in the FCOS assigned to the mailbox that will receive broadcast greetings.
   - **178** (define broadcast name mailbox) in the FCOS assigned to the mailbox that will broadcast names.
   - **179** (receive broadcast name) in the FCOS assigned to the mailbox that will receive broadcast names.
2. Create DistributionLists 1 and 9 to contain the greeting or name broadcast list.

To broadcast messages and greetings to the same list of recipients, make Distribution List 1 for broadcasting messages and keep Distribution List 9 for broadcasting greetings and names. Make Distribution Lists 1 and 9 identical in content.

26.19.2 Allow Broadcasting to a Broadcast Mailbox

Use this procedure to allow a broadcast mailbox to send a message to another broadcast mailbox, which can rebroadcast the message.

1. Customize an FCOS to include some or all of the following feature bits, as applicable:
   - **174** (define broadcast greeting mailbox)
   - **175** (receive broadcast greeting)
   - **178** (define broadcast name mailbox)
   - **179** (receive broadcast name)
2. Assign the number **1** to the distribution list in the receiving broadcast mailbox.
3. Include the receiving broadcast mailbox in Distribution List 1 of the sending broadcast mailbox.

4. Configure the receiving broadcast mailbox with the applicable FCOS, LCOS, and GCOS the same as for any distribution list message receiving.

26.19.3 Nest a Distribution List or Prevent Nesting

This procedure describes the nesting of a distribution list within a distribution list. It also describes how to prevent mailbox owners from nesting distribution lists.

Nesting a Distribution List

To nest a list:

1. Specify the list as a member of the list being created or modified.
2. • Make sure the number of a nested list is different from the number of the distribution list that contains it.

Preventing a Nested Distribution List

- To prevent nesting, customize an FCOS to include feature bit 222 (deny nesting of distribution lists) and assign it to the required mailboxes.

26.19.4 Overview

System-wide distribution lists are created in the administrator's mailbox. These are called **master lists**, and can be accessed by any mailbox on the system. Master lists eliminate the need to store the same large distribution list in more than one mailbox.

For example, one list may contain the mailboxes of everyone in the company; a second list may exist for the Personnel Department; a third may list mailboxes in the Finance Department.

Like ordinary distribution lists, master lists are created from the User Options Menu. They are numbered from 01 to 09, like users' personal distribution lists. When users want to send messages to a master list, they must add an extra zero to the beginning of the list number to tell the system to access a master list and not a personal distribution list. (For example, users enter **001** to access Master List 01.)

Using a Master Distribution List

- To **make** a message for a Master List the mailbox must have feature bit **020** (Make) and feature bit **034** (Make to master distribution list) in its FCOS.
- To **give** messages to a master list, the mailbox must have the feature bit **035** (Give to master distribution list) in its FCOS.
- To **receive** a Master Distribution List message:
- • The mailbox can receive a master list message either through the Make or Give command.
  - The mailbox must have feature bit **045** (Receive master distribution list message) in its FCOS.

To distinguish a master list from an ordinary distribution list, users must add an extra zero (0) to the beginning of the master list number.

To send a message to the members of Master List 01:

1. Log in to your mailbox.
2. Press **M** to Make a message. The system prompts: "Enter mailbox number to make message for."
3. Enter **001**.
4. The system prompts: "Record a message for Master List <name>."

26.19.5 Create a Master Distribution List by Phone

To create a Master (System) Distribution list:

1. Ensure the administrator's mailbox has an FCOS that supports distribution lists.
2. *E*nter the server's extension number.
3. Log into the administrator's mailbox (the following steps are typical. Logging into the administrator's mailbox could differ at your installation, depending on integrations and other optional features that are installed):
4. Press the * button and enter the administrator's mailbox number.

   - Enter the administrator's passcode.
   - Press **8** for **User Options**.
   - Press **5** to create or modify a list.
   - Enter the list number preceded by a 0 (zero); valid list numbers are 1 to 99, entered as "01" through "099."
   - Press **6** to name the list.

     - Record a list name.
     - Press **9** to save the name.
   - Press **2** to add a member name to the list. Enter the number of the mailbox that you wish to add.

     - The server confirms the entry: "<user's name> added." Repeat this step for each mailbox to be added.
   - Press **9** to save your entries and exit to the Main Menu.

Modify a Master Distribution List

1. Enter the server's extension number.
2. Log into the administrator's mailbox (the following steps are typical. Logging into the administrator's mailbox could differ at your installation, depending on integrations and other optional features that are installed):

   - Press the * button and enter the administrator's mailbox number.
   - Enter the administrator's passcode.
   - Press **8** for User Options.
   - Press **5** to create or modify a list.
   - Enter the number of the list to be changed. The system indicates: "You are modifying <list name>."

3. Press **P** (the **7** key) to Play all the members of the list. This step is not essential, but it may prevent you from modifying the wrong list.
4. Press **A** (the **2** key) to Add a name to the list, *or Press **D** (the **3** key) to Delete a name and then enter the* number of the mailbox to add/delete. The system confirms the entry: "<User Name> added (/ deleted)."
5. Repeat Step 4 for each mailbox to be modified.
6. Press **X** (the **9** key) to save the modified list and exit to the Main Menu.

26.20 Record Company Greetings

Overview

The Company Greeting is the message that outside callers hear when they access the system. You can record two greetings: one to play during regular working hours, and one to play during evening or weekend hours. Company greetings are made by recording a greeting in the administrator's mailbox for each line group.

The system ports are divided into line groups. Each line group can have a different administrator's mailbox and, therefore, a different company greeting. More than one administrator's mailbox may be configured. (To view system line groups in the Web Console, click **Active Configuration > View System Configuration**. In the Text Console, see Statistics Reports.)

For example, with NP Receptionist, you can record appropriate greetings for the automated receptionist number and the message center number. Separate day and night greetings can be recorded for both administrator's mailboxes. (If only one greeting is recorded, it is played during both time periods.)

The software contains a pre-recorded **Wait Prompt**, which issues the message: "Please enter an extension number or wait for assistance." Check your system Configuration Report to see whether this prompt is disabled. Disabling this prompt allows you to record the text of this message in the same voice as the rest of the company greeting.

If you do not record a personalized company greeting, NP Receptionist issues the default greeting: "Welcome to the Automated Attendant."

You can also configure a schedule for playing company greetings using the Text Console (only).

Programming

This procedure describes how to record a company day greeting and night greeting. This procedure assumes that you have defined an administrator mailbox for the line group.

1. Log into the administrator's mailbox.

   - Enter the server extension number.
   - Press the **star (*)** then enter the administrator's mailbox number.
   - Enter the administrator's passcode.

2. Record the company greeting.

   - Press the **8 button** for User Options.
   - Press the **4 button** for Greetings. The server prompts, "Press D to record the day greeting; N to record the night greeting."
   - Press D or N, then record the appropriate greeting.
   - After you have recorded the greeting, press the **7 button** to review it.

     - To add information to it, press the **2 button**.
     - To discard it and record a new one, press the **3 button**.
     - To abandon the task, press the **3 button** then press the **9 button** before the recording prompt plays.
   - When you are satisfied with the greeting that you have recorded, press the **9 button** to save the recording and return to the Main Menu.
3. To record a company greeting for the other period, repeat the process described in step 2. If either a day greeting (only) or a night greeting (only) is recorded, the following prompt plays during the period for which no greeting was recorded:

   "Welcome to the message center. Please enter a mailbox number or wait."
4. If you have administrator's mailboxes defined for other line groups and you want a company greeting to play in those line groups:
5. Log into the administrator's mailbox for the appropriate line group.
6. Record the company greeting.

26.20.1 Record an Alternate Company Greeting

This procedure describes how to record an alternate greeting that, when enabled, plays instead of the company greeting. This procedure assumes that you have defined an administrator's mailbox for the line group.

To record an alternate greeting:

1. Log into the administrator's mailbox.

   - Dial the server extension number.
   - Press the **star (*)** button then enter the administrator's mailbox number.
   - Enter the administrator's passcode.
2. Record the alternate greeting.

   - Press the **8 button** for User Options.
   - Press the **4 button** for Greetings.

     - For an alternate day greeting, press the **3 button** followed by the **7 button.**
     - For an alternate night greeting, press the **6 button** followed by the **7 button**.
     - For an alternate to both day and night greetings, press the **2 button** follwed by the **7 button**.

3. After you have recorded the greeting, press the **7 button** to review it.

   - To add information to it, press the **3 button**.
   - To discard it and record a new one, press the **3 button.**
   - To abandon the task, press the **3 button** then press the **9 button** before the recording prompt plays.
4. When you are satisfied with the greeting that you have recorded, press the **9 button** to save the recording and return to the Main Menu.
5. If you have administrator's mailboxes defined for other line groups and you want an alternate greeting to play in those line groups:

   - Log into the administrator's mailbox for the next desired line group.
   - Record the alternate greeting for that administrator's mailbox.

26.20.2 Allow a Transfer Automatically After a Greeting

To allow a caller to be transferred automatically to an attendant or a mailbox extension after playing a greeting:

Transfer to an Attendant

1. Ensure that the mailbox from which a caller is transferred contains the desired greeting.
2. Specify an attendant extension in the mailbox. For the **Attendant extension** number**:** field or prompt, enter the **number** of the attendant's extension that the caller is automatically transferred to after playing the greeting.
3. Customize an FCOS to include feature bit **063** (Call mailbox attendant after greeting). Ensure that this FCOS does not include bit 062 (Hang up immediately after greeting).
4. Assign the FCOS to the mailbox that transfers a caller to an attendant after the greeting plays.

Transfer to a Mailbox Extension

1. Ensure that the mailbox from which a caller is transferred contains the desired greeting.
2. Specify an extension for the mailbox. For the mailbox **Extension number:** field or prompt, enter the **number** of the mailbox's extension that the caller is automatically transferred to after playing the greeting.
3. Customize an FCOS to include feature **064** (Call mailbox user extension after greeting). Ensure that this FCOS does not include bit 062 (Hang up immediately after greeting).
4. Assign this FCOS to the mailbox that transfers a caller to the mailbox's extension after the greeting plays.

26.20.3 Configure for Name and Greeting Broadcast

The mailbox used for broadcasting greetings or names can be a standard mailbox, broadcast mailbox, or tree mailbox.

To use a distribution list for broadcasting greetings or names:

1. Customize an FCOS to include the following feature bits, as applicable:
   - **174** (define broadcast greeting mailbox) in the FCOS assigned to the mailbox that will broadcast greetings.
   - **175** (receive broadcast greeting) in the FCOS assigned to the mailbox that will receive broadcast greetings.
   - **178** (define broadcast name mailbox) in the FCOS assigned to the mailbox that will broadcast names.
   - **179** (receive broadcast name) in the FCOS assigned to the mailbox that will receive broadcast names.
2. Create DistributionLists 1 and 9 to contain the greeting or name broadcast list.

To broadcast messages and greetings to the same list of recipients, make Distribution List 1 for broadcasting messages and keep Distribution List 9 for broadcasting greetings and names. Make Distribution Lists 1 and 9 identical in content.

26.20.4 Configure for a Receipt Notice or Summary

This procedure describes how to delay a requested receipt notice, configure the playing of a receipt summary, and allow a distribution list message to automatically generate a receipt notice.

Delaying a Receipt Notice

Customize an FCOS to include feature bit 223 (delay requested receipt for 24 hours) and assign to the required mailbox. When this bit is in the FCOS, the mailbox owner will not hear any requested receipts until 24 hours later.

Allowing an Automatically-Generated Receipt Notice

1. Customize an FCOS to include the following feature bits and assign to the **sending** mailboxes:
   - **36** (auto-receipt for user dist list msgs)
   - **20** (make messages)
   - Either **32** (make to user distribution list) OR **33** (give to user distribution list)
2. Customize an FCOS to include feature bit **44** (receive user dist list messages) and assign to the **receiving** mailboxes.

When bit 36 is in the FCOS, the server automatically generates a receipt notice for a message sent to a distribution list. When mailbox owners log into their mailboxes, the receipt announces:

"The following users have not played your message." (list of mailbox names)

"The following users have played your message." (list of mailbox names, each followed by the time the user played the message)

Each time mailbox owners log in, they hear the updated receipt notice. Receipts are updated until mailbox owners discard them.

Configuring for a Receipt Summary

1. Set the **Min Number of Recipients for Receipt Summary** parameter in the LCOS to a number from 1 through 65,535. Specify 0 to disable the playing of a receipt summary.
2. Assign the LCOS to the mailbox that will receive receipts.
3. After a distribution list message is made to at least the number of recipients specified, the server plays the following receipt summary, in this order:

   "n recipients could not receive your message."

   "n recipients have not played your message."

   "n recipients have played your message."

26.20.5 Record the Message of the Day

The Message of the Day is made by recording a greeting in the **attendant's mailbox**. This message is sent to every mailbox on the system. After the message is broadcast, it automatically plays the next two times a user logs in. (For example, in a hotel environment, each guest might hear "Thank you for staying with ABC Hotels. Don't forget our free breakfast buffet available at 8 AM every day." the first two times they log in to access their voice mail.)

Note:
Mailboxes must have FCOS feature bit 043 to receive the Message of the Day.

More than one attendant's mailbox may be configured on your system; the Message of the Day must be recorded from the primary attendant's mailbox. (The others are used only to store messages when the primary mailbox is full.) The primary attendant's mailbox is the first mailbox number listed in the Configuration Report.

To record the Message of the Day:

1. Enter the system's main extension number to reach the attendant/NP Receptionist.
2. Log in to the attendant's mailbox:

   - Press the * key (star).
   - Enter the attendant's mailbox number.
   - Press the * key (star) to indicate that you are the owner of this mailbox.
3. Enter the attendant's passcode.
4. Press **U** (the **8** key) for User Options.
5. Press **G** (the **4** key) to record a Greeting.

6. At the "Press M to change the Message of the Day..." prompt, press **M** (the **6** key) to Change the Message of the Day.
7. Press **R** (the **7** key) to Record the Message of the Day.
8. Record your message (speak the Message of the Day).
9. Press **R** (the **7** key) to Review your recording.

    - Press **A** (the **2** key) to Add information to the message.

    - Press **D** (the **3** key) to Discard the message and record a new one.
10. When you are satisfied with this message, press **X** (the **9** key) to save the recording and return to the Main Menu.
11. Press **L** (the **5** key) to Listen to the message.
12. Press **X** (the **9** key) to Exit.

Delete or Change the Message of the Day

The Message of the Day can be deleted by recording a new Message of the Day. Every new mailbox receives the Message of the Day that is stored in the attendant's mailbox, regardless of when the message was recorded.

If you do not regularly record a Message of the Day, you must be sure to delete messages that are no longer up-to-date. Once deleted, users do not hear the old Message of the Day, even if they have not logged in since the new message was created.

To Delete the Message of the Day

1. Follow Steps 1 through 6 in "To Record the Message of the Day", above.
2. Press **L** (the **5** key) to Listen to the message.
3. Quickly press **D** (the **3** key); **immediately** press **X** (the **9** key). The system responds: "Nothing recorded. Greeting changed."

To Change the Message of the Day

1. Follow Steps 1 through 6 in "To Record the Message of the Day", above.
2. Press **L** (the **5** key) to Listen to the message.
3. Press **R** (the **7** key) to Record the Message of the Day.
4. Record over your previous message (say the new Message of the Day).

26.20.6 Enable or Disable a Message of the Day

This procedure describes how to record a message of the day, and how to prevent a message of the day from playing. This procedure assumes that you have defined an attendant's mailbox for the line group.

Enabling a Message of the Day

1. Customize an FCOS to contain feature bit 43 (Receive Message of the Day) and assign to each mailbox you want to receive the message of the day.
2. Record the message of the day in the attendant's mailbox.
3. Dial the server extension number.
4. Log in to the primary attendant's mailbox (the first mailbox number listed in the configuration report).

    - Press the ***** button, and then enter the attendant's mailbox number.
    - Enter the attendant's passcode.

        - Press the **8** button for User Options.
        - Press the **4** button. The server prompts, "Press M to record the message of the day ; T to record the site tutorial ."
        - Press the **6** button to record the message of the day.
        - Press the **7** button to start recording the message.
        - After you have recorded the message of the day, press the **7** button to review it:
        - To add information to the message, press the **2** button.
        - To discard the message and record a new one, press the **3** button.
        - To abandon the task, press the **3** button then press the **9** button before the recording prompt plays.
        - When you are satisfied with the Message of the Day that you have recorded, press the **9** button to save the recording and return to the Main Menu.

Disabling a Message of the Day

To disable a message of the day by phone, record a new message then discard it:

1. Dial the server extension number.
2. Log into the Attendant's Mailbox.

    - Press the ***** button, and then enter the attendant's mailbox number.
    - Enter the attendant's passcode.
3. Press the **8** button for User Options.
4. Press the **4** button. The server prompts, "Press M to record the message of the day ; T to record the site tutorial ."
5. Press the **6** button to record the message of the day.
6. In quick succession, without recording any words, press the **3** button, and then press the **9** button. You will hear "Nothing recorded. Message changed." The original message and anything just recorded are deleted.

26.20.7 Extended Absence Greetings

An Extended Absence Greeting (EAG) tells callers that the person they are calling is away for an extended period of time. Callers do not have the option to skip the greeting. At the end of the greeting, callers can leave a message, transfer to the line-group attendant, or end the call.

You must assign FCOS 297 (Enable Extended Absence Greeting) to a mailbox to allow the user to record and enable an EAG. You can also assign 298 (Disable message delivery when Extended Absence Greeting is enabled). For information about how users can record and enable an EAG greeting for their mailbox, refer to the *NuPoint Unified Messaging User Guide*.

EAG is included in the base software and can be enabled for any NuPoint Unified Messaging user

Note:
When EAG is enabled, you cannot log in to the Message Center directly from a remote phone. You must press the star (*) key before entering your mailbox number.

26.20.8 Record a Site Tutorial

The site tutorial, like the Message of the Day, is made by recording a greeting in the attendant's mailbox. It may consist of any instructions the administrator considers necessary. This tutorial plays after the standard tutorial when a mailbox is created or when the mailbox user enables the tutorial feature, from the User Options Menu.

More than one attendant's mailbox may be configured on your system. The site tutorial can be recorded only from the primary attendant's mailbox. (The others are used to store messages only when the primary mailbox is full.) The primary attendant's mailbox is the first mailbox number listed in the Configuration Report.

To record a site tutorial:

1. Enter the system's main extension number to reach the attendant/NP Receptionist.
2. Log in to the attendant's mailbox:
   - Press the ***** key (star).
   - Enter the attendant's mailbox number.
   - Press the ***** key (star) to indicate that you are the owner of this mailbox.
3. Enter the attendant's passcode.
4. Press **U** (the **8** key) for User Options.
5. Press **G** (the **4** key). The system prompts: "Press M to change the Message of the Day; T to change the Site Tutorial."
6. Press **T** (the **8** key) to record the site Tutorial.
7. Press **R** (the **7** key) to Record.
8. Record your message (say the site tutorial).
9. Press **R** (the **7** key) to Review it.
   - Press **A** (the **2** key) to Add information to the message.
   - Press **D** (the **3** key) to Discard the message and record a new one.

10. When you are satisfied with the site tutorial, press **X** (the **9** key) to save the recording and return to the Main Menu. The system indicates: "Greeting changed."
11. Press **L** (the **5** key) to Listen to your new message.
12. Press **X** (the **9** key) to Exit this menu.

26.21 Managing Mailboxes

You manage mailboxes from the "Mailboxes" data view. You can add, edit, delete, search for, and show all mailboxes from this view.

The Mailbox data view is divided into 2 distinct areas: the search area and the list area. Because there may be thousands of mailboxes in a system, you can perform a search for a single mailbox, or a range of mailboxes, to display. The resulting list is sorted in ascending order by mailbox number. You can then select from the list a single mailbox, or a range of mailboxes, to add, edit, or delete.

The Mailbox Data View

To open the Mailbox data view

- In the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
- Use the **Search** or **Show All** button to display mailbox information.

A common view is displayed, from which you can add, edit, delete, search for and show all mailboxes.

Since a mailbox has a lot of programmable data, the data is categorized and presented under different tabs. Each mailbox has a Basic view, which provides the tabs required for basic mailbox configuration, and an Advanced view, which enables more tabs so you can configure additional features. Tabs are context specific so some tabs do not appear under some conditions.

The following list contains all of the available tabs:

- General
- Class of Service
- Message Waiting
- Outdial Applications
- Personal Distribution Lists
- System Distribution Lists
- UI Mapping
- Statistics
- Miscellaneous

For a complete listing of the parameters on these tabs, see Mailbox Parameters.

To page through the Mailbox Data View

- You can navigate any multi-page display using the page number links or the Next/Previous/First/Last links on the right side of each page, at the top and bottom of the list.

To select a mailbox

- Select a check box beside the mailbox to modify OR you can click **Edit > Range** and then enter a range of mailboxes to modify.

To display mailbox data

- Each mailbox displays number, name, extension, and department data. Each mailbox in the list is also a link to the detailed configuration for that mailbox. To modify mailbox data, you can click the mailbox link OR you can select the mailbox check box and then click **Edit**.

Note:
Rotational mailboxes must be configured using the **Text Console**.

26.21.1 Mailbox Parameters - Web Console

This topic discusses the parameters used to configure a mailbox. The information is presented in the same layout you see when using the Web Console. For the Text console layout, see Mailbox Parameters - Text Console.

The mailbox data view is the form where you enter data when you add or edit a mailbox or multiple mailboxes. You open this view from the Mailboxes window, when you add or edit/view mailbox data. The following tabs are available:

- General Tab: The General tab is where you enter the personal information for the mailbox user.
- Class of Service Tab: The Class of Service tab contains all of the possible class of service options that can be set for a mailbox. You can only edit named COS.
- Message Waiting Tab: The Message Waiting tab allows you to set parameters like message waiting types, frequencies, and intervals.
- Outdial Applications Tab: The Outdial Applications tab allows you to set parameters for Fax and NP-UM Wake Up.
- Personal Distribution Lists Tab: The Personal Distribution Lists tab allows you to set up personal distribution lists. As the administrator, you can create a personal distribution lists in your own mailbox and then assign that list to other mailbox users as a system distribution list.
- System Distribution Lists Tab: The System Distribution List Tab contains all of the system distribution lists that are programmed in the system and allows you to assign System Distribution Lists that to a mailbox. The system distribution lists are the personal distribution lists of the administrator mailbox. This tab is not available when you add mailboxes.
- UI Mapping Tab: The UI Mapping Tab allows you to assign more than one extension to a mailbox. The tab is available only if the ESMDI feature is configured for the system.
- Stats Tab: The Statistics Tab allows you to view basic statistics for a mailbox.
- Miscellaneous Tab: The Miscellaneous tab allows you to set other miscellaneous parameters.

Basic and Advanced Views

The default view of mailbox data is the Basic View, which displays only the General, Class of Service and Message Waiting tabs. There is also an Advanced View, which displays the General, Class of Service, Message Waiting, Outdial Applications, Personal Distribution Lists, System Distribution Lists, Statistics, and Miscellaneous tabs. To display either the Basic or Advanced view, click Basic or Advanced.

Mailbox Tabs Field Descriptions

General Tab (Back to Top)				
Field	Displayed in View		Description	Values
Basic	Advanced			

General Tab (Back to Top)				
Name	ü	ü	Name of the mailbox user. If you enter a name, it is assigned to ALL mailboxes being created. Enter the name in either of two formats: <LN>, <FN> or <FN> <LN> (for example "Smith, Harry" or "Harry Smith"). Make sure to include a comma if you use <LN>, <FN> format and a space if you use <FN> <LN> format. The mailbox name is displayed any time that mailbox information is requested. **Note**: • If a user's name includes accented characters (example, "L'Abbé"), ensure that you enter the accented characters for proper SAA recognition.	Maximum 31 characters. Accented characters count for two characters. Default is blank.

General Tab (Back to Top)				
			• For SAA recognition, you must you must enter the mailbox name according to these guidelines.	
Passcode	ü	ü	Passcode of the mailbox user. Used to access the mailbox. If a passcode is specified, it is assigned to ALL mailboxes being created. If no passcode is specified, one is not assigned to the mailbox when it is created. For Administrator mailbox passcode requirements see Administrator Passcodes.	Minimum 4 digits, maximum 10 digits. Default is blank.
Force Passcode C hange		ü	Select this check bo x to force users to change the default passcode at initial l ogin. After successf ul change, this chec k box is cleared.	Default is disabled (cleared).

General Tab (Back to Top)				
Department		ü	Contains a department number code to indicate the department of the mailbox user. If a department is specified, it is assigned to ALL mailboxes being created.	Maximum 10 alpha numeric and special characters. Default is blank.
Extension	ü	ü	Extension number of the mailbox user. If you enter an extension and it differs from the first mailbox number being created, then it is assigned to ALL mailboxes being created. If the field is left blank, then an extension number is assigned by default to be the same number as the mailbox for each mailbox being created.	Maximum 11 digits. Default is blank.

General Tab (Back to Top)				
Pre-dial string		ü	This drop-down list contains the pre-dial indices that have been programmed by the technician. Select to specify a string that must be dialed prior to the extension in order to reach that extension. If a string is selected, it is assigned to ALL mailboxes being created.	Default is 0.
Alternate Extension (1-4)		ü	You can add alternates for this extension so that up to 4 other phones (like a cell phone, for example) can share this mailbox.	Default is blank.
Attendant Extension	ü	ü	This is the number that is called if user dials 0 to return to the attendant. If an attendant extension is defined, it is assigned to ALL mailboxes being created.	Maximum 15 digits. Default is blank.
Pre-dial string		ü	This drop-down list contains the pre-dial indices that have been programmed by the technician. Select to specify a string that must be dialed prior to the extension in order to reach that extension. If a string is selected, it is assigned to ALL mailboxes being created.	Default is 0.
Enable Tutorial		ü	Allows you to enable the introductory tutorial for a new mailbox. If this option is cleared, it is applied to ALL mailboxes being created.	Default is enabled (selected).

General Tab (Back to Top)				
UM Audio Encoding	ü	ü	Allows you to configure the audio encoding method to use for this mailbox. **ADPCM**: Microsoft audio encoding (default) **GSM 6.10**: Audio encoding with wider support for mobile devices **MP3**: Use MP3 only if ADPCM and GSM 6.10 cannot be played on the user device, or if the user is employing a hosted/webmail web service such as Gmail or Yahoo Mail. **Notes**: • The three different audio encoding types are available to all user types (Standard, Advanced UM, and UM-SMTP). • MP3 may result in poorer sound quality than the other audio encoding methods.	Default is ADPCM.

General Tab (Back to Top)				
Email Address			E-mail address for UM-SMTP user. This is the e-mail address where the user receives the e-mail copy of each message. From the drop-down box beside the message field (if displayed), select the delivery option for voice messages • Audio Attachment • Speech-to-Text	Maximum 64 characters. Must be a valid e-mail address. Default is blank.

General Tab (Back to Top)				
Standard Email Address (1, 2 and 3)	ü	ü	E-mail addresse(s) for Standard UM user (availability of multiple addresses depends on the class of service for the mailbox). This is the e-mail address where the user receives the e-mail copy of each message. If an e-mail address is entered, it is assigned to ALL mailboxes being created. From the drop-down box beside the message field (if displayed), select the delivery option for voice messages: • Audio Attachment • Audio Link • Web View Link (except MiCollab) • Text Notification • Speech-to-Text If Audio Link is selected, messages that are played in Web View will be marked as read in the voice mailbox. For more details on how to play the Audio Link messages, see **Note**: If the system is not licensed to use the Standard	Maximum 64 characters. Must be a valid e-mail address. Default is blank.

General Tab (Back to Top)				
UM-Web View Email Address	ü	ü	E-mail address to which to save Web View messages (availability depends on the class of service for the mailbox). If the user selects a message in Web View and clicks the **Save** button, the message will be sent to this e-mail address. If an e-mail address is entered, it is assigned to ALL mailboxes being created. If the system is not licensed to use the Standard UM features, then this field will not be displayed. If the feature is licensed but the mailbox does not have the FCOS to use the feature, then the field will be displayed but will be disabled until the mailbox does have the correct FCOS to have access to this feature.	Maximum 64 characters. Must be a valid e-mail address. Default is blank.

General Tab (Back to Top)				
Advanced UM Email Alias / Full Name / Address	ü	ü	The field name is dependant upon the type of mail server that is in use: • **Advanced UM Email Alias** displays for MS Exchange. Enter an alias for the username. • **Advanced UM Email Full Name** displays for Lotus Domino. Enter the complete username in the following format: FirstNameLastName/ Region/ Company. • **Advanced UM Email Address** displays for Google Apps. Enter an email address for the username. If the field is left blank, or contains spaces, the Advanced UM feature will not function for the mailbox. If the system is not licensed to use the Advanced UM features or the correct class of service is not applied to the mailbox, then this field will not be displayed.	Maximum 64 characters. Must not contain spaces. Default is blank.
			This field and the Advanced UM Email Password	

General Tab (Back to Top)				
Advanced UM Email Password	ü	ü	Password for Advanced UM users (availability depends on the class of service for the mailbox). If the field is left blank, or contains spaces, the Advanced UM feature will not function for this mailbox. If the system is not licensed to use the Advanced UM features, then this field will not be displayed. This field is not displayed if: • FCOS bit 295 is not set for the user • the mail server type is Google Apps • the mail server type is MS Exchange, the adapter type is IMAP, and the superuser account is programmed	Maximum 64 characters. Must not contain spaces. Default is blank.
Advanced UM Speech-to-Text Transcription	ü	ü	Select this check box if you need text transcription of voice messages for Advanced UM NuPoint users. (Users can also set this option on the Settings tab of the Web View.)	Default is blank.

General Tab (**Back to Top**)				
Class of Service Tab (Back to Top)				
Field	Displayed in View		Description	Values
	Basic	Advanced		

General Tab (Back to Top)				
Feature	ü	ü	The Feature Class of Service (FCOS) controls mailbox user privileges and outside caller functions for the mailbox. Individual privileges and restrictions are designated by numbers, which are referred to as "feature bits". Each FCOS has its own unique combination of these feature bits. For example, a user's ability to make, give, or answer messages is controlled by the FCOS assigned. The FCOS that you specify is assigned to ALL mailboxes being created. • To view the FCOS available on your system, select an FCOS from the Feature drop-down list, and then click View. • Tip: To list, create, edit, or delete an FCOS, see Feature Class of Service.	Default is 1.

General Tab (Back to Top)				
Limits	ü	ü	The Limits Class of Service (LCOS) imposes limits on mailboxes. It can be a valuable tool for allocating disk storage space and port use. Each LCOS can set the maximum times allowed for recording mailbox greetings, user messages, caller messages, and mailbox names; it can limit the amount of time a user remains logged in during one session. The LCOS can specify the maximum time that a played or unplayed message can be stored in a mailbox before it is erased by the automatic purge. It can specify the maximum number of messages that a user can accumulate in a mailbox. You can also modify an LCOS to specify secondary language prompts. The LCOS that you specify is assigned to ALL mailboxes being created. • To view the LCOS that are configured on your system,	Default is 1.

General Tab (Back to Top)				
Group		ü	The Group Class of Service (GCOS) is the group management resource that keeps track of large systems with many groups. Each GCOS consists of 128 possible groups. Any or all of the 128 groups can be assigned or deleted from the GCOS. The GCOS that you specify is assigned to ALL mailboxes being created. • To view the GCOS that are configured on your system, select a GCOS from the Group drop-down list, and then click View. • To list, create, edit, or delete a GCOS, see Group Class of Service.	Default is 1.

General Tab (Back to Top)				
Restriction		ü	The Restriction Class of Service (RCOS) is an element of NPA/NXX call screening that restricts mailbox outdials to certain area codes or prefixes within an area code. One RCOS is assigned to each mailbox. The RCOS that you specify is assigned to ALL mailboxes being created. • To view the RCOS that are configured on your system, select an RCOS from the Restriction drop-down list, and then click View. • To list, create, edit, or delete an RCOS, see Restriction Class of Service.	Default is 1.

General Tab (Back to Top)				
Network		ü	The Network Class of Service (NCOS) controls users network access. NCOS settings control whether a mailbox owner can send, give, or answer messages over the network. You can configure up to 64 NCOS and combine features to create NCOS that provide network privileges for specific user groups. NCOS is part of the NP-UM Net Digital Network optional feature. Only available in Advanced view. The NCOS that you specify is assigned to ALL mailboxes being created. • To view the NCOS that are configured on your system, select an NCOS from the Network drop-down list, and then click View. • To list, create, edit, or delete an NCOS, see Network Class of Service.	Default is 1.

General Tab (Back to Top)				
Tenant		ü	The Tenant Class of Service (TCOS) is used with the ESMDI "Multi-Tenant" application to manage mailbox interaction between user communities. The TCOS that you specify is assigned to ALL mailboxes being created. • To view the TCOS that are configured on your system, select a TCOS from the Tenant drop-down list, and then click View. • To list, create, edit, or delete a TCOS, see Tenant Class of Service.	Default is 1.
Message Waiting Tab (Back to Top)				
Field	Displayed in View		Description	Values
	Basic	Advanced		

General Tab (Back to Top)				
Message Waiting #1 Type	ü	ü	Select one of the three supported types of message waiting notification: • DTMF to PBX • HIS PMS • Pager • Unified Integration • Program RS232 • Hitachi PMS • Centrex RS232 • MiTAI Messaging The Details link is enabled if the type of notification that is selected requires you to define additional parameters. Click the Details link to display these parameters. If no additional parameters are required, then the Details link is disabled. **Note**:If you select "Pager", you must specify at least the pager number for the primary or alternate pager.	Default is None.
Message Waiting #2 Type Message Waiting #3 Type	ü	ü		

General Tab (Back to Top)		
Pager Details Form	When you select "Pager" as Message Waiting #1 Type or #2 Type, click the Details link to open the Pager Details form. **Note**: For each Message Waiting Type (#1 and #2), the mailbox can have a Primary and an Alternate pager. The parameters you must set for both pagers are the same. The fields for the alternate pager are disabled by default, and you can enable them by selecting the "Enable Alternate Pager/Telephone Number" check box.	
Page/call on Urgent Messages only.	Select this check box for notification of urgent messages only.	Default is cleared (not selected).
Type	Select "Paging" or "Message Delivery".	Default is "Paging".
Telephone Number	*Required field. Enter the paging or message delivery telephone number.	The length of this number is determined by the LCOS for Paging-Phone Length or Message delivery-Phone Length. Maximum 16 digits. Default is blank.

General Tab (Back to Top)		
Post Pager Number	(Optional field.) Enter a number that will be displayed on the screen of a display pager.	Maximum 24 digits. Default is blank.
Access type	(Optional field.) Select a dial string to indicate how to place a call and where the call should be billed, unbilled, or if it is internal.	Default is undefined.
Frequency	*Required field. Defines the number of times that the system retries the delivery of a page or message waiting notification if there is not a busy signal. In the event of a page, this could occur if the pager was out of range or the paging system was down. In the event of message delivery this could mean that somebody is answering the message delivery number, but it is not the mailbox owner (no passcode).	Digits in the range of 0-255 only. Default i s 3.

General Tab (Back to Top)		
Interval	*Required field. Defines the amount of time, in seconds, that the server will wait between Frequency retries.	Digits in the range of 0-255 only. Default is 2.
Busy Attempts	*Required field. Defines the number of times that the system retries the delivery of a page or message delivery message, when the paging number is busy.	Digits in the range of 0-255 only. Default is 3.
Interval	*Required field. Defines the amount of time, in seconds, that the server will wait between Busy Attempt retries.	Digits in the range of 0-255 only. Default is 2.
Start Time	The time of day that the paging or message delivery is turned ON for a mailbox.	AM/PM format. Hour field allows digits in the range of 1-12, and the minute field allows digits in the range of 1-59. Default is 12:00 AM.

General Tab (Back to Top)				
Stop Time			The time of day that the paging or message delivery is turned OFF for a mailbox. **Note**:The Stop time must be equal to or after the Start time.	AM/PM format. Hour field allows digits in the range of 1-12, and the minute field allows digits in the range of 1-59. Default is 12:00 AM.
Enable Alternate Pager/Telephone Number			Select to enable and define parameters for an alternate pager. The fields to program are the same as for the primary pager (see above).	Default is cleared (not selected).
Outdial Applications Tab **Note**: This tab is available in the Advanced view only. (Back to Top)				
Field	Displayed in View		Description	Values
	Basic	Advanced		
Fax		ü	The Fax optional feature must be installed and configured on the NuPoint Unified Messaging system, and this mailbox must have the proper Fax COS assigned to it for you to define the parameters in this section. If the feature is not installed, this section is not displayed.	Default is cleared (not selected).

General Tab (Back to Top)				
Fax call access type		ü	This field contains dial strings that in dicate how to place a call and where the call should be billed, unbilled or internal.	Default is undefined.
Default fax number		ü	This is the number o f the fax machine.	Digits only. Max imum digits is deter mined by the LCOS Maximum Number of digits for Telep hone Number for a Fax. Default is bl ank.
Send Email Fax C onfirmation to		ü	E-mail address to which to fax transmission confirmation messages are sent. The subject line of the message includes the following information: success/failure status, number of pages, and date and time of transmission attempt. Leave this field blank to receive confirmation by voice mail only.	Maximum 64 chara cters. Must be a val id e-mail address. D efault is blank.

General Tab (Back to Top)				
NP-UM Wake Up		ü	The NP-UM Wake Up optional feature must be installed on the NuPoint Unified Messaging system for you to define parameters in this section. If the feature is not installed, this section is not displayed. If you enable the NP-UM Wake Up outdial application, you must enter a Number. To enable an NP-UM Wake UP application for this mailbox, select the NP-UM Wake Up check box.	Default is cleared (not selected).
Frequency		ü	Defines the numb er of times NP-UM Wake Up will try to deliver the wakeup message.	Digits in the range of 0-255 only. Default i s 3.
Interval		ü	Defines the amount of time in minutes th at the system will w ait between retries to deliver the message.	Digits in the range of 0-255 only. Default i s 2.
Number		ü	*Required field (if NP-UM Wake Up is selected). The telephone number that the NP-UM Wake Up software will call to deliver the wakeup message.	The length of this number is determi ned by the LCOS NP-UM Wakeup Pho ne Number length. Maximum 11 digits allowed. Default is blank.

General Tab (Back to Top)				
Access Type		ü	The drop-down list c ontains dial strings that indicate how t o place a call and w here the call should be billed, unbilled, or if it is internal. The access types display ed in this list must be set up through t he Text Console by t he administrator.	Default is Undefined.
Access Types		ü	This section of the page allows you to set up the preferences for each type of access. There are settings for Internal, Billed, and Unbilled types. The access types displayed in drop down lists must be set up through the Text Console by the administrator. The dial first option allows the user to specify whether the billing number or the telephone number should be dialed first. By default this field is set to Billing Number. These billing settings are not enabled unless the user specifies a Billed access type. By default all access types are undefined.	N/A

General Tab (Back to Top)				
Internal access type		ü	Defines the type of internal access.	Default is Undefined.
Billed access type		ü	Defines the type of billed access. The Billed access type requires you to co nfigure settings for Billing Number and Dial first.	Default is Undefined.
Billing Number		ü	Defines the phone number for billed call s.	Maximum length is 25 digits. Default is blank.
Dial first		ü	Defines which ac cess type to dial fi rst.	Default is Billing N umber.
Unbilled access type		ü	Defines the type of unbilled access.	Default is Undefined.
Call placement a ccess type		ü	Defines the type of call placement acces s.	Default is Undefined.

Personal Distribution Lists Tab

Note:
This tab is available in the Advanced view only.

Tab Description: For each Personal Distribution List, you can specify a name, the list contents, and you can set preferences on whether the mailbox owner can edit or view the list.

(Back to Top)

Field	Displayed in View		Description	Values
	Basic	Advanced		

General Tab (Back to Top)				
Number		ü	Each mailbox can have lists numbered 01 to 99. Lists 1 and 9 can be used by the system for system distribution lists. The actual number of lists depends on a LCOS. If the user can only have 2 lists, then this drop down list will only show entries for 01 and 02. If the user had more lists before the LCOS was changed to limit list access, then those lists are not deleted, but the user will not have access to them. When the tab is first opened, the data for list 01 is displayed. The list may be empty, or have already been programmed. The list drop down list contains entries for all the possible Personal Distribution Lists that a mailbox can have, whether they are programmed or not. When you select another list number from the Number drop-down list, the data displayed in this tab changes to the info for the chosen list.	1-99. Default is 1. Number of allowed lists depends on an LCOS.

General Tab (Back to Top)				
Name		ü	(Optional field). Defines the name of the distribution list.	Maximum 31 alpha numeric characters. Default is blank.
Allow user to change		ü	Defines whether the user has permissions to change the contents of the distribution list. You can clear this option to prevent the user from changing the list.	Default is selected (enabled).
Allow user to review		ü	Defines whether the user has permissions to view the contents of the distribution list. You can clear this option to prevent the user from viewing the contents of the list.	Default is selected (enabled).
Keep Sorted		ü	Defines whether newly added list entries should be put at the end of the list or inserted in the list sorted. Existing list entries are not affected.	Default is selected (enabled).
List Members			This area shows the content of the distribution list. For each list member, the type of number, the number, and the name are displayed. The maximum number of members in a distribution list depends on the LCOS Maximum members per Distribution List. If the user has reached that limit, then the Add and the Address Book buttons will be disabled.	Maximum number of members is defined by the LCOS Maximum members per Distribution List.

General Tab (Back to Top)				
Add button		ü	To add a member to a list, click Add, and then select the type of number to add from the drop-down list, and enter the number. To browse for a member to add, click Address Book.	N/A
Type to add (drop-down list)		ü	Select one of the following types of numbers to add to the list: • Mailbox • Personal Distribution List • System Distribution List • Phone Number • Remote Mailbox • Remote Mailbox with network presence • AMIS Analog	Default is Mailbox.
Number to add		ü	Enter the number of the member to add.	Maximum 30 digits (no hyphens).

General Tab (Back to Top)				
Address Book button		ü	To browse for a member to add, click Address Book. From the Address Book View, you can view the lists of mailboxes, personal, and system distribution lists. By picking a list type in the View List drop-down list, you can view the contents of the list in the list control. You can then scroll and select one or multiple items to add to the list. Click Add to move selected items to the Add to Distribution List, or click Remove to remove selected items from the distribution list. When you reach the limit of the number of members allowed in a distribution list (defined by LCOS Maximum Members per Distribution List) the Add button is disabled. To search by for someone in the address book by name, enter a name and press Search. the list will be populated with the possible matches from the viewed list only (for example,	N/A

General Tab (Back to Top)				
Delete button		ü	To Delete list members, select the items to be deleted and click Delete. The list is updated to remove the deleted items.	The button is disabled unless a member is selected for deletion.

System Distribution List

Note:
This tab is available in the Advanced view only. It is not displayed when you add a mailbox.

(Back to Top)

Tab Description	Values
The System Distribution lists are created by the you, the administrator, through your own account. When you create personal distribution lists in the administrator mailbox, these lists become the system distribution lists that are displayed in this System Distribution list tab. When you view the list of System lists in the mailbox data view, you can select the System lists that the mailbox will be able to use. The tab displays 10 system lists per page.	Default is cleared.

UI Mapping Tab

Note:
This tab is available in the Advanced view only, and is not displayed when you are creating a mailbox.

(Back to Top)

UI Mapping Tab Description

General Tab

(Back to Top)

There are many ways that UI mapping can be used. For example, you can map several different extensions to one mailbox, OR in the case of a multi-PBX environment you can map the same extension in several different ways (i.e. 520-12324 and 560-1234) to its mailbox. A maximum of 16 extensions can be mapped to a mailbox. In this tab, you can add new extensions to a mailbox or edit and delete existing extensions.

Field	Available in View		Description	Values
	Basic	Advanced		
Extension		ü	To add an extension, click Add. To edit an extension, select a row and click Edit. To delete an extension, select a row and click Delete.	Maximum 11 digits.
Switchgroup		ü	Allows you to select a switchgroup for the extension. Select fro m 1-32.	Default is 1.
Tenant		ü	Allows you to define a Tenant number for the extension.	Maximum 4 digits in the range of 1-1000.
In Permission		ü	Allows you to enable In Permissions. Cle ar the check box to disable.	Default is selected.
Out Permission		ü	Allows you to enable Out Permissions. Cl ear the check box to disable.	Default is selected.
No Answer Greeting		ü	Allows you to select the number of the g reeting to be played when a call gets a No Answer Greeting.	0-4. Default is 0.
Line Busy Greeting		ü	Allows you to select the number of the g reeting to be played when a call gets a Line Busy Greeting.	0-4. Default is 0.

General Tab (Back to Top)				
Call Forward Greeting		ü	Allows you to select the number of the greeting to be played when a call gets a Call Forward Greeting.	0-4. Default is 0.

Stats Tab

Note:
This tab is available in the Advanced view only.

(Back to Top)

Stats Tab Description
This tab displays a summary of the number of unplayed messages and saved messages in the mailbox, the last time the mailbox was logged in to, and the number of unsuccessful login attempts. These fields are read-only.

Miscellaneous Tab

Note:
This tab is available in the Advanced view only.

(Back to Top)

Field	Displayed in View		Description	Values
	Basic	Advanced		

General Tab (Back to Top)				
Receptionist Settings		ü	The NP-UM Receptionist settings must be installed and configured on the NuPoint Unified Messaging system for them to be displayed here. The Receptionist settings are disabled unless you select the corresponding settings check boxes.	N/A
Day treatment		ü	Select check box to enable this setting.	Default is 1 - treatment 1.
Night treatment		ü	Select check box to enable this setting.	Default is 1 - treatment 1.
Miscellaneous		ü	This section allows you to define miscellaneous mailbox settings.	
Access Code		ü	Defines an access code for the mailbox. It will be validated as the user exits the field and if there is invalid input, the error The access code must contain only digits. will be displayed.	Maximum 11 digits allowed.

General Tab (Back to Top)				
Time Zone Offset		ü	The time zone setting for a mailbox is a number that the server adds to or subtracts from the hour portion of the time stamp on a message. This allows mailbox owners to convert the time stamp on a message to the time zone of their choice. This occurs in the mailbox, so only a mailbox owner hears the converted time stamp. Users sending messages to or receiving messages from the server hear the server's normal time stamp. The time zone offset also applies to personal Call Director call flows containing weekly and holiday schedules. These call flows automatically "inherit" the time zone offset of the mailbox. Note that call flows associated with line groups continue to use the system time. **Note**: Set the time zone offset in either the call flow or	The values range from 23 to +23. Default is 0.

26.21.2 Search for a Mailbox

You can perform a basic search or an advanced search for mailboxes you want to view. You can also specify how many results to view per page: 10, 15, 20, 30 or 50.

When the search results are displayed, you can select mailboxes from the list to edit.

Basic Mailbox Search

The basic search allows you to specify the mailbox number, or range of numbers, you want to see. You can also view all mailboxes by leaving the Number field empty and clicking **Show All**. When the search is complete, the results are displayed in the list area of the Mailboxes window.

To perform a basic search for one or multiple mailboxes

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. In the Mailboxes window, click the Search tab.
3. In the Search for Mailbox Number or Range field, enter a mailbox number and/or range of numbers (see Mailbox Search Fields table below).
4. From the View drop-down list, select the number of mailboxes to display per page.
5. Click Search.

To display a complete list of mailboxes

- Leave the Search for Mailbox Number or Range field blank, and click Search or Show All.

Advanced Mailbox Search

The advanced search allows you to perform a Boolean search (using the "and" operator only), by defining up to six different search criteria.

1. In the Mailboxes window, click the Advanced Search tab.
2. In the **Search for** list, select a field to search for (see "Values" column in the Mailbox Search Fields table, below).
3. In the **equals** field, enter a valid parameter for the selected field (see "Values" column in the Mailbox Search Fields table, below).
4. To add another search criterion (up to six in total), click the plus (+) button.
5. To remove a criterion, click the minus (-) button.
6. Click Search.

Example of Advanced Search

To search for all mailboxes in the 1500-1599 range that have an FCOS of 1, define two search criteria:

- **Mailbox** equals **1500-1599 +**
- **FCOS** equals **1**

Mailbox Search Fields

Type of Search	Field	Description	Values
Basic	Search for Mailbox Number or Range	Allows you to enter a mailbox number or range of numbers. Multiple mailbox numbers must be separated by a comma or a space, or be entered as a range (for example: 1001, 1003 1005-1009)	1-999999999. Maximum 40 characters (digits, commas, and hyphens).
	View ... at a time	Allows you to define the number of mailboxes to display per page. Select from the drop-down list.	10, 15, 20, 30 or 50 results per page.
Advanced	Search for	Allows you to select a field type to search for.	Mailbox, Extension, Name, FCOS, Department and Message Waiting type)

Type of Search	Field	Description	Values
	equals	The allowable values dif fer for each type of field. See Values.	All criteria have a maximum of 40 characters. Mailbox values: • Single (i.e. 1500) • Multiple individual (i.e. 1500, 1502, 1505) • Range (i.e. 1500-1510) • The single, individual and range can be combined (i.e. 1500 1501 1600-1620) • Valid characters 0-9, space, comma Extension values: • Single (i.e. 1500) • Multiple individual (i.e. 1500, 1502, 1505) • Range (i.e. 1500-1510) • Valid characters 0-9, space, comma Name values: • Name is a fuzzy match. Searches for the specified substring. The search is case insensitive and there will be no wild cards. • Valid characters: all alphanumeric. FCOS values: • 1 FCOS from the drop down list of existing FCOS. Department • 1 department name or code, and it must be an exact match • Valid characters: all

Type of Search	Field	Description	Values
	View ... at a time	Allows you to define the number of mailboxes to display per page. Select from the drop-down list.	10, 15, 20, 30 or 50 results per page.

26.21.3 Add Mailboxes

You can add one or many mailboxes at a time.

To add mailboxes:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Click Add. The Mailbox Data View is displayed.
3. Enter the required information as described here:

Create Mailboxes

This section of the view is always displayed if you are adding new mailboxes.

Field	Displayed in View		Description	Values
	Basic	Advanced		
Mailbox Number	ü	ü	Enter a single mailbox number to create a single mailbox, or enter multiple mailbox numbers separated by a comma or space. You can also enter a range. (For example, 1000, 1002 1004-1010).	1-999999999

Field	Displayed in View		Description	Values
Copy from another mailbox	ü	ü	Allows you to copy data from an existing mailbox. Enter a mailbox number in this field to copy the data from that mailbox into the new mailboxes you are creating, and then click Copy. All the fields from that mailbox are displayed now for the new mailboxes, except for the Name and the Extension fields.	Existing mailbox number.

1. To copy data from another mailbox, in the Add Mailboxes section enter the mailbox number in the Copy from another mailbox field, and then click Copy.
2. Define the required parameters in the General Tab.
3. Define the required parameters in the Class of Service Tab.
4. Define the required parameters in the Message Waiting Tab. This tab allows you to set up message waiting notification for a mailbox.

The following tabs are available only in the Advanced view:

1. Define the required parameters in the Outdial Applications Tab. This tab allows you to specify the Fax, NP-UM Wake Up, Call Placement, and Access Types parameters for the mailbox.
2. Define the required parameters in the Personal Distribution Lists Tab. This tab allows you to set up the personal distribution lists for a mailbox.
3. Define the required parameters in the Miscellaneous Tab. This tab allows you to set addition mailbox preferences.
4. When you have finished defining mailbox parameters, click Save.

Note:
If you experience an error when you attempt to save a new mailbox, simply re-enter the information and save it again.

26.21.4 Edit Mailboxes

You can edit a single mailbox or multiple mailboxes at the same time. When editing multiple mailboxes, changes are applied to all mailboxes being edited.

Edit a single mailbox

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Click a mailbox link OR select a mailbox in the list, and then click Edit > Selected. The Mailbox data view is displayed, populated with data for the selected mailbox. To view and edit advanced data, click the Advanced link in the Mailbox form.
4. Edit the mailbox parameters as required. At any time before you save your changes, you can click Cancel or the Back button on your Web browser to discard all changes without saving.
5. Click Save.

Edit multiple mailboxes

Changes are applied to all mailboxes being edited.

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select the mailboxes you want to edit and then do one of the following:

   - To edit the selected mailboxes:
     - Click Edit > Selected.

     OR
   - To edit a range of mailboxes:
     - Click Edit > Range.
     - Enter mailbox numbers separated by a comma, a space or a range (for example: 1001,1003 1005-1007).
     - Click Load. A blank Mailbox data view is displayed unless all the selected mailboxes have the same settings.
4. To edit any field, select the corresponding check box, and then modify the value. Note the following form behavior for editing multiple mailboxes:

   - If you leave a check box cleared, then the field's previous value remains unchanged for each mailbox.
   - If you enable a check box and assign the field a new value, then that value is assigned to all mailboxes being edited.
   - If you enable a check box and then leave the field blank (as in the case of a text field), then that field is cleared for all the mailboxes. In the case of list boxes, these will revert to their default values (for example, the Access type and Pre-dial string lists will default to "undefined").
   - At any time before you save your changes, you can click Cancel or the Back button on your Web browser to discard all changes without saving them.

5. Click Save.

26.21.5 Delete Mailboxes

You can delete a single mailbox or multiple mailboxes. You can click Cancel at any time before you confirm the deletion to cancel the delete operation and retain the mailbox.

Delete a Single Mailbox:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select a mailbox in the list, and then click Delete. The system prompts you to confirm the deletion.
4. To confirm that you want to delete the mailbox, click Yes. (If you click No, the deletion is halted and the mailbox remains.)

The Mailboxes list is updated.

Delete Multiple Mailboxes

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select the mailboxes you want to edit from the list of mailboxes , and then click Delete > Selected.

   OR

   To delete a range of mailboxes

   - Click Delete > Range.
   - Enter mailbox numbers separated by a comma, a space or a range (for example: 1001,1003 1005-1007).
   - Click Delete.
4. The system prompts you to confirm the deletion. To confirm that you want to delete the mailboxes, click Yesto delete the displayed mailbox or click Yes to Allto delete all mailboxes in the selected range. If you click No, the selected mailbox is not deleted. You can also click Cancelduring a range deletion to cancel the deletion.

The Mailboxes list is updated.

26.21.6 Unlock Mailboxes

Some mailboxes may be locked through the Web View interface. You can unlock these mailboxes by following the steps below. You can unlock a single mailbox or unlock multiple mailboxes at the same time.

Unlock a single mailbox:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.

2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select the mailbox to unlock and then click **Unlock > Selected**.
4. A confirmation message appears when the mailboxes are unlocked.

Unlock multiple mailboxes:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Click **Unlock > Range** and enter the mailbox numbers to unlock, separated by a comma, a space, or as a range (for example: 1001,1003 1005-1007).
4. Click **Unlock**. A confirmation message appears when the mailboxes are unlocked.
5. Click **Done**.

26.21.7 Set or Clear Mailbox Passcode or Tutorial

To reset a mailbox passcode:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select the mailbox you want to modify, and then click Edit.
4. On the **General** tab, highlight the existing **Passcode** and enter the new passcode.
5. Click Save.

To set or clear the mailbox tutorial:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select the mailbox you want to modify, and then click Edit.
4. Click Advanced.
5. Do one of the following:

   - to enable the tutorial, select the **Tutorial** check box.
   - to disable the tutorial, clear the **Tutorial** check box.

26.21.8 Set Passcode Expiry

To set a passcode expiry for a mailbox:

1. Customize an LCOS to include a value (0-365 days) for the **Passcode Expiry Period** limit. (Default is 0 or disabled.)
2. Assign the new LCOS to the appropriate mailboxes.

26.21.9 Managing Distribution Lists

The Personal Distribution Lists tab allows users to set up personal group distribution lists. System Distribution lists are created by you, the administrator, through your own account. When you create personal distribution lists in the administrator mailbox, these lists become the system distribution lists that are displayed on the System Distribution list tab. When you view the list of System Distribution Lists in the mailbox data view, you can select those System lists to assign to other mailbox users as Master or System distribution lists.

This procedure assumes that *Distribution Lists Configuration* has been completed.

To create a Distribution list:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for the mailbox to which you want to add a distribution list.
3. Click the mailbox link OR select the mailbox in the list, and then click Edit. The Mailbox data view is displayed (Basic view), populated with data for the selected mailbox.
4. Click Advanced.
5. On the **Personal Distribution** tab, select a **Number** to apply to this distribution list.
6. Enter a **Name** for the list. (For example, "Sales Team".)
7. To have newly added list entries inserted in the list sorted, select **Keep Sorted**. To have new entries added at the end of the list, clear the Keep Sorted check box.
8. To allow users to change the contents of the distribution list, select **Allow user to change**. Clear this check box to prevent users from making changes.
9. To allow users to view the contents of the distribution list, select **Allow user to review**. Clear this check box to prevent users from viewing the list.

To add (or delete) members in a distribution list:

1. Access the **Personal Distribution** tab of the Edit Mailbox page (see steps 1-4 above), and under **List Members**, click **Add** (or Delete).
2. Do one of the following:

   - Use the Address Book button to add members from the system address book

     OR
   - Enter member information manually :

     - In the **Type** list, select the **member** type to add (or delete).
     - In the **Number** field, enter the mailbox or distribution list **number**.
3. Click **Save**.

26.21.10 Import/Export a Distribution List

Distribution Lists can be imported or exported in CSV format.

This procedure assumes that *Distribution Lists Configuration* has been completed.

Importing Distribution Lists

To import a Distribution List:

1. From the navigation tree, click **Mailbox Maintenance**, and then click **Mailboxes**.
2. Search for the mailbox you wish to update.
3. Click the mailbox link OR select the mailbox in the list, and then click **Edit**. The Mailbox data view is displayed (Basic view).
4. Click Advanced.
5. On the Per Dist Lists tab, select the **Number** of the distribution list you wish to update.
6. Click **Import List**. The Import Distribution List window appears.
7. Click **Choose File** and browse to the location of the Distribution List.
8. Select the file, click **Open** and then click **OK**.
9. The Distribution List is now imported into the system.

File Import Error Report

If you attempt to import a Distribution List that contains an error such as a non-existent mailbox number, the invalid data will be excluded and a dialog will display alerting you to the fact that an error report was created. You can access the report immediately by clicking the **Download Error Report** button and following the prompts or you can view the report at a later time by logging in to the system using SSH/ PuTTY and then downloading the Distribution_list.txt file from the following location: **/usr/vm/log/**. The report lists the total number of "successful" and "unsuccessful" records that you have attempted to import and provides an explanation for each unsuccessful record (for example, "Does not exist", "Invalid type", etc.).

Exporting Distribution Lists

Distribution Lists can also be exported to a specified location. Exporting a Distribution List does not remove it from the system; it is still available on the system from where it was exported.

To export a Distribution List:

1. From the navigation tree, click **Mailbox Maintenance**, and then click **Mailboxes**.
2. Search for the mailbox you wish to update.
3. Click the mailbox link OR select the mailbox in the list, and then click **Edit**. The Mailbox data view is displayed (Basic view).
4. Click Advanced.
5. On the Per Dist Lists tab, select the **Number** of the distribution list you wish to update.
6. Select a Distribution List to export.
7. Click **Export**. The File Download window appears.
8. Click **Save** and then specify a location for the file.
9. Click **Save** again.
10. The Distribution List is now exported to the specified location.

You may now modify the list in a speadsheet application such as OpenOffice Calc. You can add, delete and update data.

Note:

- The CSV file name has the following format: **DL_<mailbox_number>_<DL_number>.csv**
- The CSV file has two columns:
  - **Type**: The item type (Mailbox, Personal Distribution List, System Distribution List, AMIS Analog, Phone Number, Remote Mailbox on Network, Remote Mailbox). The records in this column do not need to be in any particular order. For example, Phone Number entries can be listed before Mailbox entries.
  - **Number**: The mailbox and distribution list number.
- As a minimum, the CSV file requires one entry (a single complete row in the file).
- When you import a CSV file, matching entries will be overridden to avoid duplicating data.
- The CSV file requires valid data. For example, you cannot import an entry for a mailbox that does not exist. Nor can you import an entry with non-numeric characters.
- The Distribution List export/import feature is supported only in the NuPoint Web Console. It is not available in the Text Console or Web View.

26.21.11 Set Languages for Prompts

If an additional language (besides the default languages) is required, the appropriate additional language prompts must be licensed and installed before performing this procedure.

To set prompt language:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups**, select the line group you want to modify, and then click **Edit**.
4. On the **Voicemail** tab, in the **Default Prompt Language** section, select the additional language from the drop-down list. **Note**: If the required language does not appear in the list, ensure that it has been properly licensed and installed.
5. Click Save.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.22 Mailbox Parameters - Text Console

This topic discusses the parameters used to configure a mailbox.

Mailbox to Create (Mailbox Number)

All data in the mailbox file is referenced by the mailbox number. This number must conform to the mailbox dialing plan of your system; otherwise the user will not be able to access the mailbox. For an explanation, see “Dial Plan”. The dialing plan for your system may be found in the Configuration Report.

Note:
When creating a range of mailboxes:

Enter the first and last numbers in the series, separated by a hyphen (for example: 222-314).

- Numbers must conform to your system's mailbox dialing plan.

Mailbox Name

The mailbox name may consist of up to 31 alphanumeric characters. Enter the name in either of two formats: <LN>, <FN> or <FN> <LN> (for example "Smith, Harry" or "Harry Smith"). Make sure to include a comma if you use <LN>, <FN> format and a space if you use <FN> <LN> format. The mailbox name is displayed any time that mailbox information is requested. If you do not want to enter a mailbox name, press <Enter>.

Note:
If a user's name includes accented characters (example, "L'Abbé"), ensure that you enter the accented characters for proper SAA recognition.

Suggestions for this field are

- User’s name, if mailboxes are held by individuals. **Note**: You should maintain a uniform format for Dial-by-Name; for example, all uppercase (capital) letters.
- Mailbox functions, if the mailbox is dedicated to a specific purpose.
- Useful criterion for a mailbox search.

Note:
When creating a range of mailboxes, Mailbox name is given to every mailbox in the range.

Department Code

The department code can be up to 10 alphanumeric and special characters. This field is intended to hold a department name or similar designation.

- Use as a search criterion (for example, display all mailboxes that belong to Department 04A).
- Use for billing.
- Video Dispatch application can display department codes at the top of the screen.

Note:
When creating a range of mailboxes thedepartment code is assigned to every mailbox in the range.

Access Code

The access code is a specific code that the caller must enter in order to leave a message. To leave this entry blank (no access code), press <Enter>.

Note:
When creating a range of Mailboxes the Access code is assigned to every mailbox in the range.

Receptionist Day Treatment/Receptionist Night Treatment

Enter the number of the Receptionist treatment type that best matches the way that the mailbox owner wants calls processed during regular working hours. Treatment types are described in the NP Receptionist Treatment Types section.

Select "Mailbox only" treatment if

- Mailbox owner does not have a PBX extension.
- Mailbox owner wants all calls received during regular working hours to be transferred directly to the mailbox.

Note:
When creating a range of mailboxes the Receptionist treatment is assigned to every mailbox in the range.

Mailbox's Primary Extension Number

The mailbox's extension number is the number that NP Receptionist calls during the day or night if the mailbox has a Day/Night Treatment Type other than "Mailbox only".

- If the user's extension number is the same as the mailbox number, press <Enter>.
- Enter the user's PBX extension number if it is different from the mailbox number.
- If you want NP Receptionist to call a number outside the PBX network, refer to Programming NP Receptionist to Dial an Outside Mailbox Extension Number.

Note:
When creating a range of mailboxes:

- If you press <Enter>, NP Receptionist automatically assigns a matching mailbox extension number to every mailbox in the range.
- If you enter a mailbox's extension number that differs from the first mailbox number in the range, all mailboxes are given the same mailbox's extension number—the number that you just entered.

Mailbox's Extension Pre-dial Index

The pre-dial index represents a dial string that is programmed by the system technician. This entry is required only if the mailbox's extension number is long (as is the case when the mailbox's extension number is actually an outside number).

- If the mailbox's extension number is a PBX extension and/or no pre-dial index is needed, press **Enter**.

Note:

- When creating a range of mailboxes, if you enter a pre-dial index, it is assigned to all mailboxes in the range.
- When mailbox programming is complex enough to require a pre-dial index, it is better to create the mailboxes individually. See Pre-extension Dial Strings Report (available via Text console only.)

Mailbox's Alternate Extension (1-4)

You can add alternates for this extension so that up to 4 other phones (like a cell phone, for example) can share this mailbox.

Attendant Extension Number

The Attendant extension number is called if users—who are logged in to their mailboxes—press 0 (zero) in response to the prompt: "Press P to play the current message, X to exit the system, zero to return to the attendant."

- Mailbox FCOS must contain feature bit 002.
- If a personal attendant number is not defined, the PBX console attendant number is called (if defined by the technician).

With NP Receptionist, the attendant extension number is also the personal assistance number for callers to this mailbox. NP Receptionist calls this number

- Any time callers request (or wait for) assistance after they enter the user's extension number.
- If the user's (for example, Mary Smith) treatment type specifies call screening: NP Receptionist announces to the attendant, "Hello, <John Jones> calling for <Mary Smith>."
- If the attendant extension number is not defined in the mailbox: NP Receptionist transfers callers to the system attendant extension.
- If neither a **personal** attendant extension number nor a **system** attendant extension number is defined, callers are transferred to the attendant's mailbox and are prompted to leave their names, numbers, and messages.

Note:
When creating a range of mailboxes,the attendant's extension number (if any) that you assign to the first mailbox is given to all others in the range.

Features Class of Service (FCOS)

The FCOS controls mailbox user privileges and outside caller functions for the mailbox. Individual privileges and restrictions are designated by numbers called feature bits. The FCOS is a combination of these feature bits. For example, a user's ability to make, give, or answer messages is controlled by the FCOS assigned.

To view the FCOS available on your system, you can run an FCOS Report (Text Console only). The FCOS section of this guide describes FCOS and feature bits in detail and gives instructions for building additional FCOS.

Note:
When creating a range of mailboxes, the same FCOS is given to all mailboxes in the range.

Limits Class of Service (LCOS)

The LCOS imposes certain time limits on mailboxes. It can be a valuable tool for allocating disk storage space and port use.

Each LCOS can set the maximum times allowed for recording mailbox greetings, user messages, caller messages, and mailbox names; it can limit the amount of time a user remains logged in during one session. The LCOS can specify the maximum time a played or unplayed message can be stored in a mailbox before it is erased by the automatic purge. It can specify the maximum number of messages that a user can accumulate in a mailbox. You can also modify an LCOS to specify secondary language prompts.

To view the LCOS configured on your system, run an LCOS Report (text console only). The Limits Class of Service section describes the LCOS parameters in detail and gives instructions for building and modifying the LCOS.

Note:
When creating a range of mailboxes, the same LCOS is given to all mailboxes in the range.

Group Class of Service (GCOS)

The GCOS is the group management resource that keeps track of large systems with many groups.

Bitmapped GCOS, numbered 1 through 64, make up a collection of groups. Each GCOS consists of 128 possible groups. Any or all of the 128 groups can be assigned or deleted from the GCOS.

Affinity group GCOS, numbered 65 through 32,267, work well when mailboxes require communication within particular groups; they do not work across groups.

The Group Class of Service section discusses GCOS in detail and provides information about restrictions and interactions between mailboxes and FCOS.

Note:
When creating a range of mailboxes, the same GCOS is given to all mailboxes in the range.

Network Class of Service (NCOS)

The NCOS controls user's network access. NCOS settings control whether a mailbox owner can send, give, or answer messages over the network. You can configure up to 64 NCOS and combine features to create NCOS that provide network privileges for specific user groups. NCOS is part of the NP Net Digital Network optional feature.

The Network Class of Service section in the NP Net optional feature chapter discusses NCOS and provides configuration instructions.

Note:
When creating a range of mailboxes, the same NCOS is given to all mailboxes in the range.

Tenant Class of Service (TCOS)

The TCOS is used with the ESMDI "Multi-Tenant" application to manage mailbox interaction between user communities.

See "ESMDI Integration" in the *NuPoint Unified Messaging Optional Integrations Guide* for more information and configuration instructions.

Note:
When creating a range of mailboxes, the same TCOS is given to all mailboxes in the range.

Restriction Class of Service (RCOS)

The RCOS is an element of NPA/NXX call screening that restricts mailbox outdials to certain area codes or prefixes within an area code. One RCOS is assigned to each mailbox.

The Restriction Class of Service section discusses RCOS and provides configuration instructions.

Note:
When creating a range of mailboxes, the same RCOS is given to all mailboxes in the range.

Enter a Temporary Passcode

A temporary passcode provides security until the new user logs in (that is, when a new user accesses the mailbox and enters a personal passcode).

- Default passcode length is 10 digits (this parameter may be changed by the technician who programs your system).

- Once logged in, a tutorial instructs a new user to enter a personal passcode and record greetings and names for mailboxes.

The Configuration Report (text console only) shows the default passcode length for your system.

Note:
If you enter a temporary passcode when creating a range of mailboxes, it is assigned to all mailboxes in the range.

Force Passcode Change (Y/N)

You can force users to change the default passcode at their initial login.

Tutorial (Y/N)

You can choose to activate tutorials to guide users to enter personal passcodes and record greetings and names for mailboxes. The standard tutorial, which gives basic instructions to a mailbox owner on how to set up a new mailbox, is automatically enabled when a mailbox is created. The standard tutorial is *not* available, however, if NP TDD is enabled. When the tutorial is accessed the first time on a new mailbox, it directs the new owner to record a name and greeting, and to set a passcode. There are times when mailbox owners do not want to hear the tutorial (for example, if they are setting up a series of tree mailboxes for directory assistance). The Set Passcode/Tutorial option from the Mailbox Maintenance menu is used to disable (or enable) a standard tutorial, when desired.

Instead of the standard tutorial, customized information tailored to an individual installation can be recorded in the attendant's mailbox and played for new mailbox owners. This is a site tutorial, a greeting typically recorded by a server administrator.

Enter Internal Outcall Index

The index number (0 to 15) that represents the access code for internal calls.

Enter Billed Outcall Index

The index number (0 to 15) that represents the access code for outdials to be charged to a billing account.

Enter Unbilled Outcall Index

The index number (0 to 15) that represents the access code for outdials not charged to a billing account.

Enter Billing Number (appears only when Billed Outdial Index is configured)

The number of the account (up to 24 digits) to which outdials are billed.

Enter Billing Dialing Order (appears only when Billed Outdial Index is configured)

The order in which the system processes the billing number and destination telephone number in the outdial dial string. You select **BN** to require the billing number to be processed before the destination telephone number, or **NB** to require the destination telephone number to be processed before the billing number.

Configure NP Wake Up?

See NP Wakeup for information about NP WakeUp feature parameters.

Message Waiting Type #1

The message waiting indicator type tells the system how to notify a user of unplayed messages in the mailbox. The type selected depends on what is available on the system. The system supports the following message waiting types:

0: None

1: Not available

3: DTMF to PBX

5: Pager (Outdial)

7: Program RS232

9: Centrex RS232

11: Centrex

16: HIS PMS

17: Unified Integrations (UI)

21: Hitachi PMS

28: MiTAI Messaging

See Message Waiting Types for more information.

Note:

- The MITEL SX-200 DIGITAL PABX and SX-2000 PABX use message waiting types 0, 3, 5, and 7.
- When creating a range of mailboxes, the same message waiting type is assigned to all mailboxes in the range, however,
- If you choose message waiting type #2 (AC message indicators), the system automatically assigns sequential message waiting light addresses to the mailboxes in the range.

EXAMPLE: If you assign address D2 to the first mailbox in the range, the second mailbox is addressed D3, the third D4, and so on.

- If you are assigning pagers and/or message delivery, create the mailboxes individually.

Pager Parameters (appear only when MWI Type 5 Pager is configured)

See Mailboxes for Paging for information about paging parameters. See Pagers and Message Delivery for more information about Paging.

Message Waiting Type #2

Message waiting type #2 allows the system to notify a user of unplayed messages in two different ways. For example, the system can activate a radio pager and update a video dispatch screen at the same time.

All message waiting indicator types can be used as message waiting #2 indicators. You can have up to four radio pagers per mailbox.

When creating a range of mailboxes

- The same message waiting type #2 (if any) is assigned to all mailboxes in the range.
- Message waiting type exceptions listed for message waiting type #1 apply to message waiting type #2.

Message Waiting Type #3

Type 3 is restricted to one of the following:

- 0 for None
- 9 for Centrex RS-232
- 17 for Unified Integrations

Fax Retrieval Pager Access Type (Fax Call access type)

This parameter contains dial strings that indicate how to place a Fax call. See Configuring Fax Applications for more information.

Default Telephone Number for Fax Retrieval (Default Fax Number)

This is the number of the fax machine and is a required entry for Fax.

Call Placement Pager Access Type

Defines the type of call placement access. Enter a pager system between 0 and 15, you may also choose to use the billed index:

I - Internal outdial index

B - Billed outdial index

U - non-billed oUtdial index

N or - uNdefined index

Time Zone Offset

The offset (hours) between the time zone in which the mailbox owner is located and the time zone in which the server is located.

Lists with Change Rights

The number(s) of distribution lists in the mailbox that the owner is allowed to change; the default is ALL.

Lists with Review Rights

The number(s) of distribution lists in the mailbox that the owner is allowed to review; the default is ALL.

Configure UI Mailbox Mappings?

There are many ways that UI mapping can be used. For example, you can map several different extensions to one mailbox, OR in the case of a multi-PBX environment you can map the same extension in several different ways (for example, 520-1234 and 560-1234) to its mailbox. A maximum of 16 extensions can be mapped to a mailbox.

26.22.1 Create a Standard Mailbox

This procedure describes how to configure a standard mailbox on the server. It can be used either to create a new mailbox or to modify an existing mailbox. Before you begin, complete the Mailbox Individual Worksheet.

To create a standard mailbox:

From the Main Menu, select **(M) Mailbox Maintenance**. Enter the requested information, as described in the following steps, from your completed Mailbox Worksheet.

1. Select **(C) Create New Mailboxes** and enter the *n*umber of the new mailbox you want to configure.

   OR

   Select **(M) Modify Mailboxes** to modify an existing mailbox.
2. Enter the *n*umber of the mailbox you want to create or modify. The number must conform to the Dial Plan. (Prompts are almost the same for creating a new mailbox and modifying an existing one, except that "New" precedes each prompt when you select Modify Mailboxes.)

Note:
Mailbox prompts depend on the optional features that are installed on your server. See the Optional Features section if you have questions about responding to prompts that are not explained here.

3. At the **Name** prompt, enter a name for the mailbox (or if modifying an existing mailbox, press **Enter** to go to the next prompt.) Use a name (up to 31 alphanumeric characters) that describes the purpose, membership, ownership, or function of the mailbox. Enter the name in either of two formats: <LN>, <FN> or <FN> <LN> (for example "Smith, Harry" or "Harry Smith"). Make sure to include a comma if you use <LN>, <FN> format and a space if you use <FN> <LN> format. If you plan to implement Dial-by-Name, use the Last Name First Flag to specify which name should be entered first, the user's first name or last name, when using this feature. By default, callers must enter the user's last name first when using Dial-by-Name.
4. At the **Department code** prompt, enter the department code or alternate code (a string (directory number) of up to 10 digits that is the alternate code the server transmits after the pre-DN ON string) if required for message waiting lights. For DTMF-to-PBX MWI, valid characters are: 0-9, * and #.
5. At the **Access Code** prompt, specify the access code that must be dialed before an outside caller can access the mailbox, if required. The access code can be up to 10 characters that specify how callers can reach the mailbox:

M	to require the caller to enter a mailbox number
P	to require the caller to enter a mailbox number and a passcode
code	to require the caller to enter a specific access code of up to 10 digits. Valid characters are 0-9, A-D, * (star key),and # (pound key).

You can enter any combination of the above. Leave this field blank for no access code.

Note:
You must also assign an FCOS with feature bit 137 to enable the access code.

6. If **NP Receptionist** is installed in your server, refer to NP Receptionist for Receptionist parameters; otherwise, press **Enter** to skip the parameters.

7. If this mailbox uses DTMF-to-PBX message waiting lights or if NP Receptionist is installed in your server, specify the **Mailbox's primary extension number** if different than the mailbox number. Enter one of the following:
8. The PBX extension **number plus dial string codes**, from Table 1 at the end of this procedure.

    - A **string**, as explained in the NP Receptionist Manual, if NP Receptionist is installed in your server.
    - Leave blank if the extension number is the same as the mailbox number.
9. If NP Receptionist is installed in your server, refer to *NP Receptionist* for the **Mailbox's extension pre-dial index**; otherwise, press **Enter** to skip over the parameter.
10. At the **Mailbox's alternate extension** prompts, you can enter alternates for this extension so that other phones (like a cell phone, for example) can share this mailbox. Enter the phone number of another phone that will share this mailbox, or leave blank.
11. At the **Attendant's extension number** prompt, specify the attendant extension number if an attendant is available to this mailbox. Enter one of the following:

    - The extension number of the mailbox attendant that the mailbox owner or caller is transferred to after pressing 0.
    - Leave blank.
    - Refer to *NP Receptionist* for directions, if NP Receptionist is installed in your server.
12. If the attendant extension exceeds 15 digits, or if NP Receptionist is installed in your server, you must specify the **Attendant extension pre-dial index**. Do one of the following:

    - enter the dial string characters that point to the dial string the server must process before dialing the attendant extension number
    - leave blank
    - Refer to *NP Receptionist* for directions, if NP Receptionist is installed in your server.
13. At the **Features Class of Service** prompt, enter the number (1-640) of the FCOS that governs this mailbox. The default value is 1. Enter **?** for a list of defined FCOSs. You are prompted for FCOS again.
14. At the **Limits Class of Service** prompt, enter the *n*umber (1-640) of the LCOS that governs this mailbox. The default value is 1. Enter **?** for a list of defined LCOSs. You are prompted for LCOS again.
15. At the **Group Class of Service** prompt, enter the *n*umber (1-32,000) of the GCOS that governs this mailbox. The default value is 1. Ente**r ?** for a list of defined bitmapped GCOSs. You are prompted for GCOS again.
16. If NP Net is installed in your server, refer to the NP Net chapter for the **Network Class of Service**.
17. If Enhanced SMDI is installed in your server, refer to the Enhanced SMDI Integration Installation section of the *Optional Integrations Guide* for the **Tenant Class of Service**.
18. At the **Restriction Class of Service** prompt, enter the *n*umber (1-64) of the RCOS that governs this mailbox. Enter **?** for a list of defined RCOSs. You are prompted for RCOS again.
19. At the **UM audio encoding** prompt, select an encoding format (0-2) for audio files for this mailbox. Enter one of the following:

    a. **0** - ADPCM Microsoft Audio encoding (default)
    b. **1** - GSM 6.1 (Wider support for mobile devices)
    c. **2** - MP3 (Use MP3 only if ADPCM and GSM 6.10 cannot be played on the user device, or if the user is employing a hosted/webmail web service such as Gmail or Yahoo Mail. MP3 may result in poorer sound quality than the other audio encoding methods.)

20. At the **Enter a Temporary Passcode** prompt, do one of the following:

    a. enter 4-10 digits (0-9) to set a specific passcode
    b. enter **S** to make the passcode the same as the mailbox number
    c. enter **R** to have the server generate a passcode for you (and display it in the mailbox configuration report that automatically appears after you respond to the last mailbox parameter)
    d. press **Enter** to leave the passcode unchanged
21. At the **Force passcode change (y/n)** prompt, select **Y** to enable or **N** to disable the option to force users to change their passcode at their next login. (A user's successful passcode change resets this option to 'n'.)
22. At the **Tutorial** prompt, select **Y** to enable or **N** to disable the standard tutorial (also called new user tutorial, user tutorial, and NuPoint Voice tutorial). The server default is generally for the standard tutorial to play when a new mailbox is created.
23. At the **Standard UM Email address** prompt, enter the email address (max 64 characters) where the user receives an email copy of each message, or leave blank. Availability of multiple addresses depends on the class of service for the mailbox.
24. At the **Standard UM Email Option** prompt, select the delivery option for each email address:

    a. **0** for **Audio Attachment** (Wave, ADPCM Codec),
    b. **3** for **Audio Link** (Wave, ADPCM Codec),
    c. **6** for **Web View Link**,
    d. **7** for **Text Notification**
    e. **8** for **Speech to Text**
    f. or leave blank
25. At the UM WebView Email address prompt, enter the email address to which to save Web View messages, or leave blank. When the user selects a message in Web View and clicks the **Save** button, the message will be sent to this e-mail address. (Availability depends on the class of service for the mailbox.)

> **Note**:
> If outdials from this mailbox are being billed to a long distance carrier or other account, continue with the next step, otherwise, press **Enter** to skip to the Message Waiting Type parameter configuration in step 31.

26. At the **Internal Outcall Index** prompt, *enter t* he index number (0-15) representing the access code for internal calls or enter **?** for a list of defined index numbers. You are prompted for the index again.
27. At the **Enter Billed Outcall Index** prompt, enter the index number (0-15) representing the access code for outdials to be charged to a billing account or enter **?** for a list of defined index numbers. You are prompted for the index again.

> **Note**:
> The Internal Outcall Index and the Billed Outcall Index must be different numbers.

28. At the **Non-billed Outcall Index** prompt, enter the index number (0-15) representing the access code for outdials not charged to a billing account, or enter **?** for a list of defined index numbers. You are prompted for the index again.
29. At the **Enter Billing Number** prompt, enter *t*he calling card number, up to 24 digits, to which outdials are billed.

> **Note**:
> If you use this field then you cannot use MWI2 with an alternate pager.

30. At the **Enter billing dialing order** specify the order in which the server processes the billing number and destination telephone number in the outdial dial string. Enter one of the following:

    a. **bn** to require the billing number to be processed before the destination telephone number
    b. **nb** to require the destination telephone number to be processed before the billing number
31. At the **Message wating type #1** prompt, specify the type of MWI using a number from the following table:

Number	Message Waiting Type
0	None
3	DTMF to PBX
5	Pager (See Pager Application)
7	Program RS232
9	Centrex RS232
11	Centrex
16	HIS PMS
17	Unified Integration
21	Hitachi PMS

Number	Message Waiting Type
28	MiTAI Messaging

If more than one type of message waiting indication is used, this is the primary type.

32. At the **Message wating type #2** prompt, you can specify a secondary MWI type. If message waiting type 5 was specified at the first or second message waiting type parameter, set the mailbox parameters for paging or message delivery, or both.
33. If you need a third type of message waiting indication, specify it.
34. At the **Fax retrieval pager access type**, enter one of the following access types: enter a pager system between 0 and 15, or select one of the following from the billed index:

    a. I - **I**nternal outdial index
    b. B - **B**illed outdial index
    c. U - non-billed o**U**tdial index
    d. N or. - u**N**defined index
35. At the **Default telephone number for fax retrieval** prompt, enter up to 25 digits for the telephone number.
36. If call placement will be used, specify the **Call placement pager access type**; otherwise, press **Enter** to skip to the next parameter. Enter either a number from 0 to 15 representing the pager access index number, or a billed index:

B	for Billed Outdial Index
I	for Internal Outdial Index
N	for Undefined Index
U	for Non-billed Outdial Index

37. At the **Time zone offset** prompt, specify an offset if required. Enter the hours of difference, from -23 through 23, between the mailbox owner's time zone and the NuPoint Voice module time zone.
38. At the **Lists with change rights** and the **Lists with review rights** prompts, allow the mailbox owner to have review rights or change rights, or both, for the selected distribution lists by entering one of the following:

    - A single list, for example **2**
    - A series of lists, for example, **1,3,4,6**
    - A range of lists, for example **1-6**
    - A combination of any of the above entries; for example: **1-5,8,12,50-70,90**
    - **A** for all distribution lists
    - **N** for no distribution lists

Note:
This mailbox parameter alone does not allow change rights; you must also include feature bit 74 (create or modify user distribution list) in the FCOS.

39. After the last entry, the server displays the mailbox configuration and then prompts for the next mailbox number to create/modify.
40. If required, you are prompted to **Configure UI mailbox mappings?** Select ***Y*** *if this mailbox should have a mapping configured for the UI application or* **N**if no mapping is required.

At this point, the parameter settings are saved and you can continue with mailbox configuration or press **Enter** to exit.

26.22.2 Define an Administrator Mailbox

To define an administrator's mailbox:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:
3. Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
4. Otherwise, select **(E) Modify Active Configuration**.
5. Select **(G) Group Selected** and enter the number of the line group that this administrator's mailbox serves.
6. Check the dialing plan for the specified line group. Ensure the administrator's mailbox number that you want to designate is compatible with the number of digits allowed by the plan, does not start with a prohibited digit, and so on.
7. From the Voice Configuration Menu, select **(M) Modify Application**, and then **(Z) Dial String and Mailbox** menu.
8. Select **(C) Administrator's Mailbox #** and enter the number you want to designate as the administrator's mailbox. The administrator's mailbox can be the default (998), one of the numbers already reserved for it, or any other number in the server, as long as it matches the dialing plan. Numbers reserved for the administrator's mailbox are:

98	9999998
998	99999998
9998	999999998
99998	9999999998

999998	99999999998

9. Exit to the Main Menu to save the mailbox designation you just entered.

   - If the administrator's mailbox number is not the default or is not one of the numbers reserved for it, create the mailbox through the Mailbox Maintenance Menu. Set the mailbox parameters the same as for a standard mailbox, with this exception:

10. Assign an FCOS that contains all the features of a typical administrator's mailbox such as default FCOS **1 (Unlimited)** or default FCOS **10 (VIP)** to the mailbox.

> **Note**:
> For enhanced server security, we recommend that you select a number other than the default or one of the reserved numbers.

11. To define an administrator's mailbox for another line group, select the desired line group, and repeat the preceding steps. You can use a different number for each administrator's mailbox if you want each line group to have a different company greeting.

Administrator Passcodes

When creating the administrator mailbox, you must ensure that the passcode you enter is not trivial. If you use the following types of passcodes, NuPoint UM will accept the entry but you will not be able to log in to the admin mailbox on subsequent attempts:

- do not use the mailbox number
- do not use consecutive digits (like 1234)
- do not use repeated digits (like 1111)

Examples of valid passcodes are: 1397 or 2684 (as long as the mailbox number is not the same).

26.22.3 Define an Attendant Mailbox

To define an attendant's mailbox:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:
3. Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
4. Otherwise, select **(E) Modify Active Configuration**.

1. Select **(G) Group Selected** and enter the number of the line group that this administrator's mailbox serves.

2. Check the dialing plan for the specified line group. Ensure the attendant mailbox number that you want to designate is compatible with the number of digits allowed by the plan, does not start with a prohibited digit, and so on.
3. From the Voice Configuration Menu, select **(M) Modify Application**, and then **(Z) Dial String and Mailbox** menu.
4. Select **(D) Attendant's Mailbox #** and then enter the number or numbers you wish to designate as the attendant's mailbox (or mailboxes). Up to five attendant's mailboxes can be defined per line group. Enter multiple attendant's mailbox numbers separated by commas; for example: 5999,6999,7999,8999,9999

   The attendant's mailbox can be the default (999), one of the numbers already reserved for it, or any other number in the server, as long as it matches the dialing plan. Numbers reserved for the attendant's mailbox are:

99	9999999
999	99999999
9999	999999999
99999	9999999999
999999	99999999999

5. Exit to the Main Menu to save the mailbox designation you just entered.
6. If the attendant's mailbox number is not the default or is not one of the numbers reserved for it, create the mailbox through the Mailbox Maintenance Menu. Set the applicable mailbox parameters the same as for a standard mailbox.

Note:
For enhanced server security, we recommend that you select a number other than the default or one of the reserved numbers.

To define an attendant's mailbox for another line group, select the desired line group, then repeat the preceding steps. Use a different number for each attendant's mailbox.

26.22.4 Modify or Delete Mailboxes

The **Modify** option allows you to change any parameters of an existing mailbox.

1. From the Main Menu, select **(M) Mailbox Maintenance Menu**.
2. Select **(M) Modify**.

3. At the **Mailbox to Modify** prompt, enter the mailbox number you want to update. The system displays existing mailbox information and prompts you for changes.
4. Enter new values and press **Enter** for any value you do not want to modify.
5. When all mailbox information has been displayed/modified, the system displays the new information and prompts for the next mailbox number. Enter another mailbox number, *or* press <Enter> to return to the Mailbox Maintenance Menu.

The **Delete** option allows you delete a single mailbox or a range of mailboxes:

To Delete a Single Mailbox

1. From the Main Menu, select **(M) Mailbox Maintenance Menu**.
2. Select **(D) Delete**.
3. Enter the number of the mailbox to delete. The system displays the mailbox information and prompts you to confirm this delete.
4. Enter **Y** to delete the mailbox OR to leave the mailbox unchanged, enter **N** or press **Enter**. The system prompts for the next mailbox number to delete. Enter another mailbox number, *or* press **Enter** to return to the Mailbox Maintenance Menu.

To Delete a Range of Mailboxes

1. From the Main Menu, select **(M) Mailbox Maintenance Menu**.
2. Select **(D) Delete**.
3. Enter the first and last numbers of the mailboxes in the range to be deleted, separated by a hyphen (for example: 101-203). The system asks for confirmation.
4. Type **delete** (lower-case).
5. You are prompted to confirm. Ensure that the mailbox numbers in the range are correct and then enter **Y** to delete this range of mailboxes.
6. The system prompts for the next mailbox number to delete. Enter another mailbox number, OR press **Enter** to return to the Mailbox Maintenance Menu.

26.22.5 Find Mailbox Information

There are several options available for displaying and reporting mailbox information for a specified mailbox or group of mailboxes:

Mailbox Search : use this option to program the system to display information on all mailboxes that match the mailbox parameters or a group of parameters that you select.

Inquire About Mailboxes : use this option to display mailbox information for a specified mailbox number or for a range of mailbox numbers. This option produces the Mailbox Data Inquiry Report.

Mailbox Block Inquiry : use this option to create the Mailbox Blocked Report information (available through the Billing Menu) in a "blocked" format—without titles or summaries. The data can then be redirected to a personal computer, manipulated using a spreadsheet program, and used for invoices or monthly statements.

Mailbox Dump :use this option as a troubleshooting aid. It allows you to obtain a comprehensive report on a specific mailbox.

Mailbox Data : use this option (in the Reports Menu) to create a complete information report on all mailboxes.

Mailbox Search

The Search function lets you program the system to display information on all mailboxes that match the mailbox parameters or a group of parameters that you select.

The available selection criteria include:

• FCOS	• Mailbox name
• LCOS	• Message waiting type
• GCOS	• Mailboxes without passcodes
• NCOS	• Attendant extension number
• Mailbox extension number	• Attendant extension pre-dial index
• Mailbox extension pre-dial index	• Mailbox number or range of numbers
• Department code	• Mailboxes with new user tutorial enabled

Any of these features may be specified as criteria for your search. The system can search the mailbox data files of all mailboxes or a specified range of mailboxes.

EXAMPLE:

The following example is a search for all mailboxes in the Accounting Department; it has mailbox code 045 to match the department number, and we want to find out what mailboxes, if any, are not passcode-protected.

Because all mailboxes on the system in the 600 to 900 range are utility mailboxes, we will only search the mailbox range 100 through 599.

To Perform a Mailbox Search

1. From the Main Menu, select**(M) Mailbox Maintenance**.
2. Select**(S) Search**. The search criteria list is displayed.
3. Select **(H) Department Code** and enter code (in this example: **045). The search form display is updated to reflect your choice.**

4. **Further refine your search by selecting(N) No passcode. The screen is updated to display Department Code 045 mailboxes that have no passcode.**
5. **Select(R) Range of mailboxes(to restrict the utility mailboxes from the output) and enter the range (in this example,100-599).**
6. **Select(S) Searchto begin the search. The requested search information is displayed in the following format:**

   >>>ABC Corporation<<<

   Mailbox Search Utility

   Fri Jan 29, 1996 8:15 am

   MAILBOX: 313

   MSGS: 6 UNPLAYED: 0 URGENT: 0 RECEIPT: 0.4

   LCOS: Default : 1 FCOS: VIP : 1

   GCOS: 1 NCOS: Default : 1

   BAD LOGS: 0 LAST LOG: 01/29/96 7:34 am MINS: 0

   PASSWD: Y TUTOR: N DAY: M NIGHT: M

   NAME: Allan Donald CODE:

   EXTEN: INDEX: 0

   ATTEN DN: INDEX: 0

   TOTAL Mailboxes: 1 Messages: 6 Unplayed: 0 Urgent: 0 Minutes: 0.4
7. Enter **X** to exit to the Mailbox Maintenance Menu after the Search is complete.

Inquire About Mailboxes

The Inquire About Mailboxes option asks the system to display mailbox information for a specified mailbox number or for a range of mailbox numbers. This option produces the Mailbox Data Inquiry Report.

The Mailbox Data Inquiry Report shows

- Message counts
- Class of service assignments
- Message waiting type
- Passcode status
- Login status

To Run the Mailbox Data Inquiry Report

1. From the Main Menu, select **(M) Mailbox Maintenanc**e.
2. Select **(I) Inquire About Mailboxes**.
3. Select an output routing for your report: (C) Console or (P) Console with Pause.
4. Enter a mailbox **number** or range of numbers in the format first-last (for example: 4000-4999). The system displays a list of all mailboxes specified; the system shows message statistics, classes of service, message waiting type, and login status of each mailbox.

The system displays information in the following format:

Box	Msgs	Unp	Urg	Rec	Mins	FCOS	LCOS	GCOS	NCOS	MWI	Pswd
501	2	1	0	0	1.3	1	1	13	1	DTMF to PBX	Y
502	2	1	0	0	9.7	1	1	12	1	DTMF to PBX	Y
503	11	10	1	0	28.2	2	1	1	1	Pager	Y
504	0	1	0	0	0.0	7	1	1	1	DTMF to PBX	Y (t)

Reading the Mailbox Data Inquiry Report

Columns of data in the Mailbox Data Report indicate the following information:

Box	Mailbox number
Msgs	Total played, unplayed, and urgent messages in the m ailbox.
Unp	Unplayed messages.
Urg	Urgent messages.
Rec	Receipts (requested and forced).
Mins	Length of all messages (in tenths of a minute).
FCOS LCOS **GCOS NCOS**	Classes of service assigned to the mailbox.
MWI	Message waiting type assigned to the mailbox.
Passwd	
Y	There is a passcode for this mailbox, and the mailbox owner has logged in.
N	There is no passcode for this maibox, and the mailbox owner has logged in.
Y(t)	There is a temporary passcode for this mailbox and the owner has not logged in yet. The tutorial is activated (but has not been played yet.)

1. Enter additional mailbox numbers *or press**Enter**to exit.*

Mailbox Block Inquiry

The Mailbox Block Inquiry option presents the Mailbox Blocked Report information in a "blocked" format—without titles or summaries. The data can be redirected to a personal computer and manipulated by using a spreadsheet program for an invoice or monthly statement.

To Run the Mailbox Block Inquiry Report

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(B) Mailbox Block Inquiry**.
3. Select an output routing for your report: (C) Console or (P) Console with Pause.
4. At the **Mailbox to display:** prompt, enter a mailbox number or range of numbers in the format first-last (for example: 4000-4999). The system displays an unformatted report of all billing statistics that have been configured for each mailbox specified and the rate set for each statistic.
5. Enter additional mailbox numbers, *or* press **Enter** to exit.

Mailbox Dump

The Mailbox Dump option is a useful troubleshooting aid. It allows you to obtain a comprehensive report on a specific mailbox. The report consists of four parts:

- Login status
- Configuration
- Usage statistics (labelled "contents")
- Message queues

These entries show the number of messages free, played, unplayed, urgent, and undelivered; the number of message receipts; and the number of future delivery messages.

To Run the Mailbox Dump Report

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(E) Mailbox Dump**.
3. At the **Mailbox #** prompt, enter the selected mailbox number. You are prompted to select the labeled report version:
4. Select (M) for mailbox information in ASCII (text) OR
5. Select (D) for mailbox information in hexadecimal

   The system displays the login status, configuration, usage statistics, and message queue statistics for the specified mailbox.
6. Enter another mailbox number *or* press **Enter** to exit.

Note:
The report can only be displayed on the maintenance console; it cannot be routed as output to an output device (printer).

Mailbox Data

The Mailbox Data Report provides statistics for every mailbox on the system. Refer to the Mailbox Data Report in the Reports chapter for instructions to run and interpret this report.

26.22.6 Configure a Rotational Mailbox

To Set the Index:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(R) Rotational Mailbox**.
3. At the **Mailbox number to be rotated:** prompt, enter the number of the rotational mailbox.
4. At the **Period (hours):** prompt, press **Enter**.
5. At the **Index:** prompt, press **Enter** if you want the rotation to begin with the lowest-numbered mailbox in the list. Valid indexes depend on the number of mailboxes that you add to the distribution list.

Note:
To reset a period rotation to an index rotation, enter 0 (zero) for the period.

At the **Set start date** for mailbox prompt, press **Enter** to return to the Mailbox Menu

To Set the Period:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(R) Rotational Mailbox**.
3. At the **Mailbox number to be rotated:** prompt, enter the number of the rotational mailbox.
4. At the **Period (hours):** prompt, enter the number of hours that one child greeting will play before rotating

   to the next greeting. Valid hours are 1 through 255.
5. At the **Start date (MM-DD-YY):** prompt, enter the month, day, and year when you want to start the cycle

   (for example: 06-20-10).

6. At the **Start time (HH:MM [am/pm]):** prompt, enter the hour and minute when you want to start the cycle

   (for example: 02:10 indicates 2:10 a.m.). If you do not specify a.m. or p.m., then a.m. is assumed.
7. At the **Set start date for mailbox** prompt, press **Enter** to return to the Mailbox Maintenance Menu.

26.22.7 Set or Clear Mailbox Passcode or Tutorial

The tutorial provides users with basic instructions about setting up a new mailbox. It is automatically enabled when a mailbox is created. There are times when users may not want to hear the tutorial (for example, when setting up a series of chain mailboxes for directory assistance).

This procedure describes how to set or clear a passcode for a mailbox, and how to turn on or off the tutorial. You must also have configured the desired passcode parameters (*Configure Mailbox Passcode Parameters by Line Group*).

1. From the Main Menu, select **(M) Mailbox Menu**.
2. Select **(P) Set Passcode/Tutorial**.
3. When prompted, enter the **mailbox number** for which to set the passcode.
4. When prompted for **New passcode**, do one of the following:

   - Enter a passcode with four to 10 digits (0 to 9) OR
   - Press **Enter** to leave passcode unchanged, OR
   - Enter **0** (zero) if you want to clear an existing passcode, OR
   - Enter **S** to make passcode the same as the mailbox number, OR
   - Enter **R** for a random generated number.
5. At the **Tutorial?** prompt, do one of the following:

   - Enter **Y** to enable the tutorial. The first time that the system is accessed, it directs the new user to record a name and a greeting for callers and to enter a passcode. The system confirms passcode and tutorial settings.
   - Enter **N** to clear the tutorial if the user has already set up the mailbox. The system confirms passcode setting and that the tutorial is cleared.
6. The system prompts you to set the next mailbox passcode. Press **Enter** to return to the Mailbox Maintenance menu.

26.22.8 Set Passcode Expiry

To set a passcode expiry for a mailbox:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(L) Limits COS**.
2. In the Limits COS menu, select **(L) Set Limits for Selected LCOS**.
3. In the Limits Parameters menu, select **(P) Mailbox Passcode Expiry**.
4. Enter a number of days (**1-365**) that passcodes will remain valid before expiring, or enter "0" to disable passcode expiry.
5. Exit the Limits menu and then select **(X) Exit --Save Changes**.

Note:
You need to activate this configuration before these changes can take effect in your system.

26.22.9 Test Mailbox Capabilities

To test mailbox capabilities that have been established by an FCOS, LCOS, and GCOS:

1. If you have not already done so, obtain a System Configuration Report. Refer to the report as needed for such information as the FCOS, LCOS, and GCOS that have been assigned to mailboxes.
2. If you have not already done so, obtain these reports:
   - Feature Class of Service Report
   - Limits Class of Service Report
   - Group Class of Service Report
3. Create two test mailboxes ("test mailbox A" and "test mailbox B") that include each FCOS, LCOS, and GCOS used. (See Create a Standard Mailbox.)
4. Refer to the Feature Class of Service Report as needed to identify the feature bits in the FCOS assigned to the mailbox you are going to test.
5. Configure the Event Recorder program to be set for options: (1=Detailed NuPoint Voice, 7=Open Account Admin, 8=DTMF to PBX, and 12=Send NuPoint Voice) and then run the program. These options will provide useful details. (For more information about Event Recorder, see the Troubleshooting chapter of the NuPoint UM Technician's Handbook.)
6. Call test mailbox B and leave a message.
7. Check the called telephone (test mailbox B) to verify that the message waiting indicator (light or tone) is turned on.
8. Log into test mailbox B and play the message.
   - Verify that your message completes under each of the following conditions:
     - You stop speaking and the server hears 3 seconds of silence.
     - You entered a valid DTMF tone (if the Caller's Menu is enabled in the mailbox's FCOS).
     - The server hears 5 seconds of dial tone.
     - You reach the maximum message length established by the LCOS assigned to the mailbox.
   - Test all the capabilities of the mailbox allowed by the feature bits in the FCOS.
   - Leave or make messages as appropriate to test the various feature bits.
   - Verify that all appropriate prompts are played.
   - Pay particular attention to possible feature bit conflicts.
9. Refer to the Limits Class of Service Report as needed to identify the limits parameters.
10. Test the mailbox for all limits parameters that comprise the LCOS. For example, make a message and test the length limit.
11. Log out of test mailbox B.
12. Verify that the message waiting indication is turned off.
13. Log into test mailbox A.

14. Refer to the Group Class of Service Report as needed to identify groups.

    - Make three messages and send them to test mailbox B with these respective special delivery options:
    - Mark one of the messages urgent.
    - Mark one of the messages confidential.
    - Request a receipt for one of the messages.
15. Log into test mailbox B, play the messages, and verify that they are urgent and confidential, respectively.
16. Log out of test mailbox B.
17. Log into test mailbox A and verify that it plays the receipt notice.
18. Create a distribution list that includes test mailbox B.
19. Make a message to the distribution list that includes test mailbox B.
20. Log out of test mailbox A.
21. Log into test mailbox B and play the distribution list message.
22. Log out of test mailbox B.
23. Log into test mail box A and verify the answer from test mailbox B.

26.22.10 Configure a Mailbox for Distribution Lists

To configure a mailbox for distribution lists:

Note:
This procedure assumes that *Distribution Lists Configuration* has been completed.

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** or **(M) Modify Mailboxes**.
3. At the **Mailbox to create/modify:** prompt, enter the number of the mailbox to configure for distribution lists. If you want this mailbox to hold master distribution lists, specify the administrator's mailbox number.
4. Press **Enter** until you reach the **Feature Class of Service** prompt.
5. At the (new) **Features class of service:** prompt, enter the **n umber** of the FCOS (1-640) that is customized for distribution lists.
6. Press **Enter** until you reach the **Limits Class of Service** prompt.
7. At the (new) **Limits class of service:** prompt, enter the **n umber** of the LCOS (1-640) that is customized for distribution lists.
8. Press **Enter** until you reach the **Group Class of Service** prompt.
9. At the (new) **Group class of service:** prompt, enter the **n umber** of the GCOS (1-32,000) containing a group that is shared by all members of the same distribution list.

10. Press **Enter** until you reach the **Lists with review rights:** prompt and then enter any of the following:

    - **A** for all distribution lists
    - A single **list**, for example, 2
    - A series of **lists**, for example, 1,3,4,6,
    - A **range of lists**, for example, 1-6
    - A combination of any of the above entries; for example, 1-5,8,12,50-70,90

> **Note**:
> This mailbox parameter alone does not allow change rights; you must also include feature bit 74 (create or modify user distribution list) in the FCOS.

11. At the **Lists with change rights:** prompt, make the same entry as you did in step 10.
12. After the last entry, the server displays the mailbox configuration, then prompts for the next mailbox number. The parameter settings are saved. You can continue with mailbox configuration or exit.

26.22.11 Create or Modify a List for Mailbox Owners

To add members or delete members in a single distribution list, or a master distribution list:

1. From the Main Menu, select **(M) Mailbox Maintenance**, and then **(L) List Maintenance.**
2. Select **(C) Create, Modify, or Show Distribution Lists**.
3. At the **Mailbox:** prompt, enter the **n umber** of the mailbox that contains the list you want to add to or delete from. To modify a master distribution list, enter the administrator's mailbox.
4. At the **Distribution List:** prompt, enter the **n umber** of the list you want to add to or delete from (1-99). For mailboxes that rotate on full, tree mailboxes, NP Forms mailboxes, and broadcast mailboxes, specify 1. For a name greet mailbox, specify 9.
5. At the **(S)orted or (U)nsorted list ?** prompt, select **U** if the list is in a tree mailbox OR **S** for all other types of mailboxes. Keep in mind that sorting of lists longer than 190 members can be slow.
6. At the **Check for duplicate before add (y/n) [Y]?** prompt, enter **Y** if you want the server to make sure the member is not already in the list, or **N** to bypass the check.
7. At the **(A)dd, (D)elete, or (S)how list ?** prompt, select **A** to add a member, or **D** to delete a member.
8. At the **Member:** prompt, enter the **member** you want to add or delete. All of the following are valid members:
9. **Mailbox number**
10. **M** and a remote mailbox with a telephone number for AMIS Analog; the remote mailbox and telephone number are separated by a comma (for example, M3788,4283788)
11. **N** and a remote mailbox for networking
12. **T** and a telephone number for off-server messaging
13. **D** and a distribution list number, except in a broadcast mailbox
14. **S** and a master distribution list number, except in a broadcast mailbox

Mailbox numbers can be entered in any of the formats shown below; the other numbers must be entered one at a time:

- A single mailbox number, for example, 3788
- A continuous range of mailbox numbers, for example, 3001-3788
- A series of mailbox numbers, for example, 3781,3782,3786,3788

You can mix formats of mailbox number entries, so you can specify all the mailbox numbers necessary in one attempt. For example, this entry is valid: 208,222-308,333,334,661

1. After the server confirms that the member just specified was added or deleted, continue adding or deleting or complete the activity. At the **(A)dd, (D)elete, or (S)how list ?** prompt, do one of the following:
2. To add or delete more members from the current list, enter A or D as described in step 7.
3. To complete adding or deleting members, press **Enter**. When the server asks if you want to save changes to the distribution list, press Y. The server reports the current members, reflecting members just added or deleted, and your additions and deletions are saved.

26.22.12 Delete a Distribution List

To delete distribution lists from a mailbox:

1. From the Main Menu, select **(M) Mailbox Maintenance**, and then **(L) List Maintenance**.
2. Select **(D) Delete Distribution Lists**.
3. At the **Mailbox for distribution list to delete:** prompt, enter the **n umber** of the mailbox containing the distribution list you want to delete.
4. At the **List to delete:** prompt, enter the **n umber** of the list (1-99) you want to delete from this mailbox. The server shows the current members in the list.
5. At the **Delete (y/n):** prompt, enter **y** to delete. The server confirms that the specified list was deleted.
6. At the **Mailbox for distribution list to delete:** prompt, enter same mailbox **number** as in step 1 if you want to delete more distribution lists from it; otherwise, enter the **number** of another mailbox that has distribution lists you want to delete. When you have finished deleting distribution lists, press **Enter**. You are returned to the List Maintenance Menu.

26.22.13 Delete a Member from All Distribution Lists

To delete a member from all distribution lists in the server:

1. From the Main Menu, select **(M) Mailbox Maintenance**, and then **(L) List Maintenance**.
2. Select **(F) Find and/or Delete Mailboxes From All Lists**.
3. At the **Mailbox to search for:** prompt, enter the **n umber** of a mailbox to be deleted from all distribution lists.
4. At the **Enter another mailbox or <CR>:** prompt, enter *a*nother mailbox **number** of a mailbox to be deleted from all distribution lists, or press **Enter** if you are finished entering mailbox numbers.
5. At the **Delete from lists?** prompt, enter **Y** to remove mailbox(es) from all distribution lists in the server. The server responds with a message telling you which lists the member was deleted from.
6. At the **Mailbox to search for:** prompt, enter another mailbox **number** (member) to delete, or press **Enter** to return to the List Maintenance Menu.

26.22.14 View All Lists Containing a Specified Member

To find and view all distribution lists containing a specified member:

1. From the Main Menu, select **(M) Mailbox Maintenance**, and then **(L) List Maintenance**.
2. Select **(F) Find and/or Delete Mailboxes From All Lists**.\
3. At the **Mailbox to search for:** prompt, enter the ***n*** **umber** of a mailbox (member) that you want to find.
4. At the Enter another mailbox or <CR>: prompt, enter ***a***nother mailbox **number** of a mailbox to be found, or press **Enter** if you are finished entering mailbox numbers.
5. At the Delete from lists? prompt, enter **N** for no. The server responds with a message telling you which lists in which mailboxes contain the specified member.
6. At the **Mailbox to search for:** prompt, enter ***t***he next mailbox **number** (member) to find, or press **Enter** to go back to the List Maintenance Menu.

26.22.15 View Members of a Single List

To view the members of a distribution list:

1. From the Main Menu, select **(M) Mailbox Maintenance**, and then **(L) List Maintenance**.
2. Select **(C) Create, Modify, or Show Distribution Lists**.
3. At the **Mailbox:** prompt, enter the ***n***umber of the mailbox that contains the list you want to view.
4. At the **Distribution list:** prompt, enter the **n umber** of the list you want to view.
5. At the **(S)orted or (U)nsorted list ?** prompt, enter **U** if the list is in a tree mailbox, or **S** for all other types of mailboxes. Keep in mind that sorting of lists longer than 190 members can be slow.
6. At the **Check for duplicate before add (y/n)?** prompt, enter **N** to bypass the check.
7. At the **(A)dd, (D)elete, or (S)how list ?** prompt, select **S** to show the list. The server lists the current members and their names.
8. At the **Mailbox:** prompt, enter the next mailbox **number** containing a distribution list you want to view, or press **Enter** to return to the List Maintenance Menu.

26.23 Schedule Company Greetings

Note: This procedure is not available in the Web Console.

To designate when a company day greeting plays and when a company night greeting plays:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:
3. Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
4. Otherwise, select **(E) Modify Active Configuration**.

1. Select **(G) Group Selected** and then enter *t*he **number** of the line group (1-24) for which you want to schedule greetings.
2. Select **(M) Modify Application**, and then **(N) Day/Night**.
3. Select **(S) Start Time of the Workday** and enter the **time** a workday starts, which will be the time when the company day greeting begins to play. Enter the time in the format indicated by the prompt; for example, 8:30am. If you do not specify "a.m." or "p.m.," the server assumes that the time is "a.m."
4. Select **(E) End Time of the Workday** and enter the **time** a workday ends, which will be the time when the company night (off hours; after hours) greeting begins to play. Enter the time in the format indicated by the prompt; for example, 5:30pm. If you do not specify "a.m." or "p.m.," the server assumes that the time is "p.m."

Note: To have the same greeting play all the time, specify 12:00pm as both the start and end times of the workday.

1. Select **(W) Weekend Days** and enter **N** or **D** in each of seven positions. **N** designates weekend days; **D** designates work days. For example, a work week of Monday through Friday, which is the default, is designated by DDDDDNN. (The company day greeting does not play on weekend days.)
2. Save your entries by exiting to the Main Menu.
3. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.23.1 Enable an Alternate Company Greeting

Note: This procedure is not available in the Web Console.

This procedure describes how to enable an alternate greeting once an alternate greeting has been recorded. This procedure assumes that you have defined an administrator's mailbox for the line group (Define an Administrator's Mailbox).

To enable an alternate greeting:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(K) Copy/Delete/Enable Mailbox Greetings**.
3. At the **COMMAND (Copy, Delete, or Enable ?):**, enter **E** for enable.
4. At the **Enter mailbox to enable greeting:**, enter the administrator's mailbox **number**.
5. At the **COMMAND (Enter type of greeting to enable (a/d/p) [p]):** prompt, enter **A** for the alternate greeting.
6. At the **COMMAND (Copy, Delete, or Enable ?):** prompt, press **Enter**.
7. Exit to the Main Menu to make the recorded alternate greeting take effect. The alternate greeting plays instead of the company day greeting and night greeting.

26.23.2 Copy a Mailbox Greeting

Note:
This procedure is not available in the Web Console.

This procedure describes how to copy a mailbox greeting, or name from one mailbox to another. You must perform this procedure at a server maintenance console, after a greeting has been recorded for the source mailbox. (See the NuPoint UM Web View help for instructions to record source mailbox greetings.)

To copy a mailbox greeting:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(K) Copy/Delete/Enable Mailbox Greetings**.
3. At the **COMMAND (Copy, Delete, or Enable ?):** prompt, select **C** to copy.
4. At the **Enter mailbox to copy name/greeting from:** prompt, enter the mailbox **number** of the source mailbox.
5. At the E**nter mailbox to copy name/greeting to:** prompt, enter the mailbox **number** of the target mailbox. You can copy the greeting to more than one mailbox by using any of these formats:
6. A single mailbox number, for example 3788
7. A continuous range of mailbox numbers, for example 3001-3788
8. A series of mailbox numbers, for example 3781,3782,3786,3788
9. A mix of formats, for example 208,222-308,333,334,661
10. At the **COMMAND (Enter source name/greeting number (0-5) [1]):** prompt, select the greeting you want to copy:

    - For a **user's** mailbox:
    - enter **1 f**or the Personal greeting.
    - For an **administrator's** mailbox:
    - Enter **1** for the Day company greeting,
    - Enter **2** for the Night company greeting,
    - Enter **4** for the Alternate greeting.
    - For an **attendant's** mailbox:
    - Enter **1** for the Message of the Day,
    - Enter **4** for the Alternate greeting.
    - For **all** mailboxes:
    - Enter **0** for the Name,
    - Enter **5** for the Fax Cover Sheet
11. The server confirms that the greeting/name has been copied. You can choose to copy more greetings, or press **Enter** to exit to the Mailbox Maintenance Menu.

26.23.3 Select Languages for Prompts

If an additional language (besides the default languages) is required, the appropriate additional language prompts must be licensed and installed before performing this procedure.

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:
3. Select (F) Modify Inactive Configuration if you just made a change through the Offline Menu without activating it
4. Otherwise, select (E) Modify Active Configuration.
5. Select **(G) Group Selected** and enter the number of the line group (1-24) to modify.
6. Select **(M) Modify Application** to modify NP Receptionist.
7. Select **(L) Default Prompt Language**. In the Prompt Language Selection menu, the languages that are licensed for your system are listed.
8. Enter the **number** that corresponds to the language you want. Only languages already installed on the server are displayed.
9. Exit to the Main menu to save your changes.
10. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

To set up a secondary prompt language:

- Create an LCOS to specify that language. Then assign the LCOS to the those mailboxes that are to play the secondary prompt language.

26.23.4 Disabling a Message of the Day

Disabling a Message of the Day

You can disable a message of the day by phone or through the server console:

To disable a message of the day through the server console:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(K) Copy/Delete/Enable Mailbox Greeting**.
3. At the **COMMAND (Copy, Delete, or Enable ?):** prompt, enter **D** to disable.
4. At the **Enter mailbox to delete name/greeting from:** prompt, enter the attendant's mailbox **number**.
5. At the **COMMAND (Enter source name/greeting number (0-5):**, enter **1** for Message of the Day. The server displays a message confirming that greeting 1 (the message of the day) is deleted from the identified attendant's mailbox.
6. At the **COMMAND (Copy, Delete, or Enable ?):** prompt, press **Enter**.
7. Exit to the Main Menu.

26.24 Overview

In a hotel or motel environment, this system provides an electronic mailbox for each guest. The system provides advantages to guests, callers, and front-desk staff:

- Hotel and motel employees are not dedicated to the task of message-taking.

- Callers and guests are ensured message accuracy.
- Guests can listen to messages at their convenience, and they can discard or keep messages for future reference.
- Hotels and motels can bill guests for mailbox service.
- Optional language features improve usage.

26.24.1 Hotel/Motel Mailbox Structure

Four basic types of mailboxes are used in the Hotel/Motel application

- Guest mailbox
- Full-feature guest mailbox
- Check-in mailbox
- Check-out mailbox

Guest Mailbox

Mailboxes with Restricted FCOS (default FCOS 3) or optional Lodging FCOS are assigned to each guest. These FCOS are designed specifically for mailbox users and callers who may be unfamiliar with voice messaging systems.

- Restricted and Lodging mailboxes are controlled by Check-in and Check-out mailboxes. Guests do not need to perform any mailbox set-up (such as recording names and passcodes) before using mailboxes.
- This system integrates with the Hotel/Motel telephone system to allow guests to log in by pressing a button on the telephone keypad and by entering a passcode when prompted.
- After guests log in, the system automatically plays the first message; guests are prompted to keep or discard messages. After the choice is made, the next message (if any) plays without input from guests.
- Expanded prompts are helpful to uninitiated users:

  "Press K, the 5 key, to Keep this message..."

Note:
Languages other than English are optional features. If an additional language is desired, the appropriate alternate-language prompts blade must be installed. For a list of available languages, contact your authorized dealer.

Full-Feature Guest Mailbox

A hotel or motel may wish to assign the full-feature guest mailbox. This mailbox has Full Guest FCOS 2, which is the same as Unlimited FCOS (FCOS 1) except that the Check-in/Check-out feature is enabled. The desk clerk must still check this mailbox; however, guests can change names and passcodes, record personal greetings, and make messages for other guests' mailboxes. (FCOS 2—Full Guest provides a complete description of full-feature guest FCOS capabilities.)

Check-In Mailbox

The Check-in mailbox is used to record names and passcodes for guests. This mailbox has FCOS 4. Several desk clerks can call into a single Check-in mailbox at one time. This means that you need to create only one Check-in mailbox for your system. (FCOS 4—Check-In.)

Check-Out Mailbox

A Check-out mailbox is used to clear a recorded name and any messages stored in the guest's mailbox. This mailbox has FCOS 5. Several desk clerks can call into a single Check-out mailbox at one time. You need to create only one Check-out mailbox for your system. (FCOS 5—Check-Out.)

26.24.2 How the Hotel/Motel Application Works

Check-In

When the guest checks in, the desk clerk calls a Check-in mailbox and records a name and passcode to personalize a mailbox for the guest.

Mailbox Check-In Procedure

The clerk must perform the following mailbox check-in procedure:

1. When the guest checks in
   - Dial the system's main extension number. The company greeting plays.
   - Press the * key (star). NP Receptionist says: "Welcome to the Message Centre. Please enter a mailbox number, or wait."
   - Enter the number of the Check-in mailbox. If the Check-in mailbox has a **passcode**, you will be prompted to enter it now.
2. The system prompts: "Enter mailbox number to check in." Enter the mailbox number assigned to the room that the guest will occupy.
3. The system prompts: "Record a name" (beep). Record the guest's name.
4. The system requests a passcode. Enter a four-digit passcode.
5. The system confirms: "Passcode set to <number>. Check-in complete. Good-bye." The system disconnects the clerk.

Note:
If the system is not fully integrated (the guest cannot pick up messages by pressing a button), the clerk must supply the passcode and mailbox number to the guest.

During the Guest's Stay

When the guest is out of the room, or when the phone is busy, the operator transfers calls to voice mail. Callers are prompted to "Please leave a message for <guest's name>."

When the guest returns, a message waiting indicator on the telephone notifies the guest when there are unplayed messages in the mailbox. The mailbox passcode provided by the desk clerk at check-in time assures the guest that all messages remain confidential.

Check-Out

When the guest checks out, the mailbox is also checked out. A mailbox check-out clears the mailbox of the guest's name and passcode, announces the number of unplayed messages, and offers the desk clerk the opportunity to discard any messages stored in the mailbox.

Mailbox Check-Out Procedure

The clerk must perform the following mailbox check-out procedure:

1. When the guest checks out:
   - Dial the system's main extension number. The company greeting plays.
   - Press the * key (star). NP Receptionist says: "Welcome to the Message Centre. Please enter a mailbox number or wait."
   - Enter the number of the Check-out mailbox. If the Check-in mailbox has a **passcode**, you will be prompted to enter it now.
2. The system prompts: "Enter mailbox number to check out." Enter the departing guest's mailbox number. The system responds: "Mailbox <number> has <number> unplayed messages. Press K to keep the messages, D to discard them," OR "Mailbox <number> has no messages. Check-out complete, good-bye."
3. Press **D** (the **3** key) to Discard any messages.

Note:
To successfully check out the mailbox, **the clerk must discard the messages**. If the remaining messages are not discarded, the system responds: "Check-out canceled, good-bye."

26.24.3 Billing Guests

To bill guests, a Termination Report is run for each mailbox. This report can be run either before or after the mailbox is checked out, but the results will vary.

- If the Termination Report is run **before** the mailbox is checked out and there are unplayed messages, the system does not charge for disk usage for these messages because this resource is calculated after messages are deleted.

- If the Termination Report is run **after** the mailbox is checked out, the system charges for all messages because all messages must be deleted in order to check out the mailbox.

26.25 Overview

You can give a mailbox certain features by assigning a Features Class of Service (FCOS) to it. An FCOS is a collection of three-digit numbers, called “feature bits;” each feature bit represents a property of a mailbox, such as the ability to log in, or the ability to keep messages. NuPoint UM includes a set of default Features Classes of Service, or you can create your own custom FCOS as required. You can assign only one FCOS to each mailbox. If you do not assign an FCOS, the default, FCOS 1, is assigned.

Each FCOS is a list of feature bits that supply different functionality. For example, feature bit 001 means the user can log in to the mailbox; 020, the user can make messages; and 050, the user can keep messages. Each feature bit represents a different, specific feature. NuPoint Voice provides more than 250 feature bits. Certain feature bits require special attention:

- Some feature bits cannot function without a “master feature bit” in an FCOS. For example, an FCOS with feature bit 021 (make and request receipt) must also include the master feature bit 020 (make messages).
- Certain combinations of feature bits are incompatible. For example, if feature bits 039 (notification tone when new message arrives) and 047 (notification prompt with new message arrives) are in the same FCOS, the server uses feature bit 047, not 039.

There are 14 default FCOS, from the basic, like FCOS 1, to the specialized, such as FCOS 4 for hotel check in. You can also create a custom FCOS by copying a default and modifying its feature bits to suit your requirements. We recommend that you maintain the original default set to aid in troubleshooting, if required.

When designing your own FCOS, see the section on Feature Bits by Category. For example, to see which feature bits allow the system administrator to create and use master distribution lists, see Category 4, Master Distribution Lists.

For a detailed description of each feature bit, see the section on Feature Bit Descriptions.

Note:
Feature bits are sometimes called “FCOS bits.” This guide uses the term “feature bits” because “FCOS bits” causes confusion between the feature bit and the FCOS. Feature bits are also referred to as “features,” which can also cause confusion because many aspects of the system are also called features.

26.25.1 Default FCOS

Several FCOS are pre-programmed in the default configuration. This section describes the default FCOS. Within the feature bit list for each default FCOS, master feature bits appear in bold type. You can select a default FCOS that matches your needs and assign it to a mailbox, or you can customize your own FCOS, using a default FCOS as a template.

We recommend that you preserve these default COS settings and customize FCOS when you require extra features.

Note:
Operations that involve interactions with other mailboxes (make, give, answer) are limited to those mailboxes with compatible Group Class of Service (GCOS).

FCOS 1: Unlimited

This FCOS contains most standard feature bits, except for the message-addressing options. The user can record name and greeting, change the passcode, and receive messages from other users and outside callers. The user can also play, keep, discard, answer, give messages and make new messages for other system users or for distribution lists, as well as create and modify distribution lists. Although this FCOS suits the needs of users with standard applications, do not think of it as truly “unlimited,” which implies that the mailbox is not restricted. It is, more accurately, the basic FCOS for a system.

Note:
New mailboxes have FCOS 1 assigned to them by default unless you specify another FCOS.

FCOS 1 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

020 Make messages

024 Give messages

028 Give with comments

029 Answer messages

032 Make a user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Give to master distribution list

040 Receive messages from other users

041 Receive messages form outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist. list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

098 Say “Press 0” to caller before beep

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

FCOS 2: Full Guest

This FCOS is used in the hotel/motel environment where no Property Management System (PMS) integration is available. It has fewer capabilities than FCOS 1 (Unlimited). However, some feature bits allow check-in and check-out mailboxes to reach this type of mailbox.

FCOS 2 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

008 Mailbox can be checked in/out

020 Make messages

024 Give messages

028 Give with comments

029 Answer messages

032 Make a user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Change to master distribution list

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist. list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

092 User will be in Dial-by-Name database

098 Say "Press 0" to caller before beep

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

161 Conditional greetings

FCOS 3: Restricted

This FCOS is used by hotels. Guests cannot enter or change their names, greetings, or passcodes; make, answer, or give messages; or create or use distribution lists. They can, however, keep and discard messages. Only the attendant can record names and greetings and assign passcodes. For a hotel or motel environment, a name and passcode are usually entered for this mailbox from a special check-in (see default FCOS 4) mailbox. Callers hear the greeting “Please leave a message for [name].”

A guest logs into the mailbox and hears the count of unplayed messages. Unplayed messages play automatically (that is, the guest hears the first message and all succeeding messages without having to press P to play). All messages are automatically kept, unless the guest presses D (to delete messages) within a few seconds.

FCOS 3 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

008 Mailbox can be checked in/out

009 Automatic logout if no message/receipt

010 (ISO) Enhanced Outcall Paging Options

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list **050 Play messages**

052 Auto-play unplayed messages **053 Keep messages**

054 Auto-keep messages **055 Discard messages**

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet only mailbox

FCOS 4: Check In

This FCOS is used by hotels for a check-in mailbox, a special mailbox that manipulates other mailboxes. In a check-in mailbox, the system prompts for the mailbox number to be checked in, then prompts the attendant to record a name and enter a passcode for the mailbox. Guest mailboxes controlled by FCOS 4 must contain feature bit 008 (Mailbox can be checked in/out). Guest mailboxes are therefore usually assigned default FCOS 2 (Full Guest) or default FCOS 3 (Restricted).

FCOS 4 contains the following bits:

001 Login to mailbox

004 Outside caller functions

005 Play Outside Caller Menu prompts

066 Login during greeting in greet only mailbox

070 User Options Menu

071 Record or change mailbox name

072 Record or change greeting

090 Check in other mailboxes

FCOS 5: Check Out

This FCOS is used by hotels for a check-out mailbox that is the counterpart of the check-in mailbox. In a check-out mailbox, the server prompts for the mailbox number to be checked out. The attendant can then choose to either keep or discard any messages left in the mailbox. Finally, the server purges the guest's name, greeting, and passcode, and follows the attendant's command about messages. The mailbox is then ready to be checked in for the next guest.

You must create a check-out mailbox to use the hotel check-in/check-out feature. Guest mailboxes controlled by FCOS 4 must contain feature bit 008 (Mailbox can be checked in/out). Guest mailboxes are therefore usually assigned default FCOS 2 (Full Guest) or default FCOS 3 (Restricted).

FCOS 5 contains the following bits:

001 Login to mailbox **004 Outside caller functions**

005 Play Outside Caller Menu prompts

066 Login during greeting in greet only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change greeting

091 Check out other mailboxes

FCOS 6: Greeting Only

When a caller reaches a Greeting-Only mailbox, the server plays the greeting and then hangs up. For example, a theater manager wants callers to hear an announcement of show times. The manager creates a mailbox with this FCOS, logs in to the mailbox, and records a greeting that announces show times. The mailbox owner can change the mailbox name, greeting, and passcode, but cannot create or use distribution lists. A Greeting-Only mailbox cannot accept messages. A Greeting-Only mailbox must have a greeting; otherwise, the server considers the mailbox invalid. To log into a Greeting-Only mailbox that does not have a greeting, press the * (star) key, then enter the mailbox number. You can remove feature bit 066 (Login during greeting in greet-only mbx) after you record a greeting for the mailbox.

FCOS 6 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

060 Ignore DTMFs during greeting

062 Hang up immediately after greeting

066 Login during greeting in greet only mbx **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

FCOS 7: <TUI Emulation>

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions005 Play outside caller menu prompts

006 Rewind and fast-forward during playback

007 Pause in record or play

016 Deny recycling with * key

018 Give and mark urgent

019 Answer and mark urgent

020 Make messages021 Make and request receipt

022 Make to multiple destinations

023 Make and mark confidential

024 Give messages025 Give and request receipt

026 Give to multiple destinations

027 Give and mark confidential

028 Give with comments

029 Answer messages

030 Answer and request receipt

031 Answer and mark confidential

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Give to master distribution list

038 Attach original message to answer

039 Notification tone when new msg arrives

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist list messages

045 Receive master dist list messages

047 Notification prompt when new msg arrives

050 Play messages 053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

066 Login during greeting in greet-only mbx

070 User options menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

078 Activate user tutorial

084 Give receipt message with comments

085 Give receipt message to multiple dests

086 Give receipt message

087 Make and mark urgent

088 Receive urgent messages

094 Change Message Delivery options

095 Mark message for Future Delivery

098 Say "Press 0" to caller before beep

125 Clear user passcode

126 Make/Give to mailbox with empty GCOS

144 Skip forward to next message

190 Receive fax messages

191 Make fax messages

192 Give fax messages

193 Deliver fax to default number

194 Deliver fax online

195 Specify fax delivery number

196 Change default fax number

204 Message Skip, forward and backward

288 Enable TUI Emulation

FCOS 8: Chain

Chain mailboxes play a greeting, then route calls to the mailbox selected by the caller. A chain mailbox cannot accept messages. Assign this chain FCOS to a mailbox and record a greeting for the mailbox. A chain mailbox prompts callers to enter a mailbox number or to wait. If callers enter a mailbox number, the chain mailbox routes the call to that mailbox. If callers wait (do not immediately enter a mailbox number), NuPoint Voice transfers the call to the attendant's mailbox or to the attendant, depending on the configuration. When a mailbox owner logs in to this type of mailbox, NuPoint Voice prompts, "Press U to change user options, X to exit." The mailbox owner can change the mailbox name, greeting, and passcode, but cannot make messages or create or use distribution lists. Chain mailbox is a default, unless the FCOS has one of these feature bits: 062 (Hang up immediately after greeting), one of the receive message feature bits, or any of the tree, rotational, or broadcast mailbox feature bits. If these feature bits are not included, the general greeting plays, which asks the caller for a mailbox number.

Note:
NP Receptionist and the Chain FCOS: NP Receptionist is an optional feature. The server prompts the caller to enter an extension number, then transfers the caller to that extension. If the caller does not enter an extension, the server transfers the call to the attendant's extension, if one is defined; otherwise NP Receptionist transfers the call to the attendant's mailbox. If you include feature bit 141 (Define chain mailbox in Receptionist), a chain mailbox routes a call to an extension even if the chain mailbox has no greeting.

FCOS 8 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

066 Login during greeting in greet only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

141 Define chain mailbox in Receptionist

FCOS 9: Time

This is a Greeting-Only mailbox that plays its greeting, announces the system time, and asks for a mailbox number. Feature bit 065 (Play system time after greeting) plays the time; if you want this function without announcing the time, you can copy this FCOS to a new number and leave feature bit 065 out of the new version.

A user can log in and change user options (mailbox name, greeting, and passcode), but cannot create or use distribution lists. A time mailbox does not accept messages.

FCOS 9 contains the following bits:

001 Login to mailbox

065 Play system time after greeting

066 Login during greeting in greet only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

FCOS 10: VIP

This FCOS provides advanced options with more feature bits than FCOS 1. It contains these features: Multiple make/give, Attach original message to answer, and Message addressing options (New Message Notification, Mark Confidential, and Return Receipt). This FCOS also includes the Outside Caller's Menu, and will include the mailbox in the Dial-By-Name database.

FCOS 10 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

007 Pause in record or play

015 Change wakeup options

018 Give and mark urgent

019 Answer and mark urgent

020 Make messages

021 Make and request receipt

022 Make to multiple destinations

023 Make and mark confidential

024 Give messages

025 Give and request receipt

026 Give to multiple destinations

027 Give and mark confidential

028 Give with comments

029 Answer messages

030 Answer and request receipt

031 Answer and mark confidential

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Change to master distribution list

036 Auto-receipt for user dist list msgs

038 Attach original message to answer

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist list messages

046 Announce-receipt at login

047 Notification prompt when new msg arrives

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

061 Wait to record (timeout = # key)

066 Login during greeting in greet-only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

075 Audit receipt message

076 Play urgent messages in FIFO order

077 Change pager schedule

078 Activate user tutorial

082 Soft play (interrupt) message count

083 Soft play (interrupt) most prompts

084 Give receipt message with comments

085 Give receipt message to multiple dests

086 Give receipt message

087 Make and mark urgent

088 Receive urgent messages

092 User will be in Dial-by-Name database

094 Change message delivery options

095 Mark message for future delivery

096 Make messages before keep/discard

098 Say “Press 0" to caller before beep

110 Make/give to telephone number

124 Change paging phone number

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

161 Conditional greetings

250 Allow NP PWG View login.

251 Allow NP PWG View telephone playback/record

261 Allow NP PWG View WEB access to messages

289 Enable UM-SMTP

290 Enable UM-WebView

291 Enable RAC (Record a call)

292 Enable NP Director

295 Enable Advanced UM

FCOS 11 - 13: Reserved

FCOS 14: MiCollab

This FCOS is assigned by default to NuPoint Unified Messaging mailboxes when they are created using the MiCollab platform. This includes a set of features relevant to the license configuration bundled with the MiCollab product.

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play outside caller menu prompts

006 Rewind and fast-forward during playback

020 Make messages

024 Give messages

028 Give with comments

029 Answer messages

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Give to master distribution list

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist list messages

045 Receive master dist list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

066 Login during greeting in greet-only mbx

070 User options menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

081 Only One Correct Passcode for Login

098 Say "Press 0" to caller before beep

125 Clear user passcode

126 Make/Give to mailbox with empty GCOS

130 Passcode cannot be same as mailbox

201 Deny Trivial Passcode

290 Enable UM-WebView

291 Enable RAC (Record a call)

292 Enable NP Director

295 Enable Advanced UM

304 Enable UM Standard

FCOS 15: Tree

This FCOS is used to specify a tree mailbox. It plays a greeting and waits for the caller to enter a single digit. When the caller presses a digit, the call is transferred to another mailbox.

FCOS 15 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

066 Login during greeting in greet-only mbx **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Record or change mailbox greeting **121 Define tree mailbox**

FCOS 16: NP Forms

This “template” FCOS is used with NP Forms, an optional feature used to record information from callers in templates, “voice forms.” A mailbox with this FCOS plays the greetings stored in its child mailboxes, sequentially, and records a message after each greeting. A typical application might have a rotational mailbox (see FCOS 17), with several child NP Forms mailboxes, all pointing to the same list of Greeting-Only mailboxes. You can also use feature bit 139 (Template: assume last greet mbox FCOS).

FCOS 16 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt **004 Outside caller functions**

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

007 Pause in record or play **020 Make messages**

041 Receive messages from outside callers

043 Receive message of the day

048 Receive messages of the day

049 No auto-time stamp of played messages **050 Play messages**

052 Auto-play unplayed messages **053 Keep messages**

054 Auto-keep messages **055 Discard messages**

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

066 Login during greeting in greet-only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

133 Don’t say: “You may start your msg now”

135 Define template mailbox (NP Forms)

136 Don’t say: “End of message”

138 Don’t say: “Message complete”

FCOS 17: Rotational Mailboxes

Rotational mailboxes allow the caller to hear greetings that change. Greetings change either by time and date (in a “period” rotational mailbox) or with every call (in an “index” rotational mailbox).

FCOS 17 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

066 Login during greeting in greet-only mailbox

068 Define rotational mailboxes **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

You can also assign any one of the following additional feature bits to a rotational mailbox:

062 Hang up immediately after greeting

063 Call mailbox attendant after greeting

064 Call mailbox user ext after greeting

You can use rotational mailboxes with NP Forms (see FCOS 16) to route the caller to an NP Forms "template" mailbox; this requires feature bit 149 (Login to template thru rotational mbx).

Note:
Do not include feature bit 041 (Receive messages from outside callers) because it disables the mailbox's rotation features.

FCOS 18: Financial

This FCOS provides advanced options with more feature bits than FCOS 1, for administrator convenience. It contains the following features: Multiple make/give, Attach original message to answer, and Message addressing options (New Message Notification, Mark Confidential, and Return Receipt), the Outside Caller's Menu, and it will include the mailbox in the Dial-By-Name database. In addition, the FCOS gives users access to Unified Messaging Web access and access to the embedded secure media player.

FCOS 18 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

024 Give messages

028 Give with comments

029 Answer messages

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Change to master distribution list

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet-only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

098 Say “Press 0" to caller before beep

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

290 Enable UM Web View

293 Disable the <Save> <Reply> and <Forward> buttons on the UM Standard Web View web pages

294 Enable the Mitel embedded player on the UM_Std+MWI web pages

26.25.2 Suggested Additional FCOS

These additional FCOS are not defaults, but are suggestions for you to number and assign if needed. Create an FCOS, give it an unused number, assign the feature bits listed here, then assign the new FCOS to mailboxes as needed. Any FCOS number from 18- 20 or 25-640 is acceptable. See Customizing FCOS for more details.

Lodging

This FCOS, designed for hotel or motel applications, has fewer features for guests than default FCOS 2 (Full Guest), but more than FCOS 3 (Restricted). Also see “Hotel Guest: Basic” following this description.

You can create the Lodging FCOS with the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant **004 Outside caller functions**

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

008 Mailbox can be checked in/out

009 Automatic logout if no messages/receipts

040 Receive messages from other users

041 Receive messages from outside callers **050 Play messages**

052 Auto-play unplayed messages **053 Keep messages** **055 Discard messages**

057 Play saved messages in FIFO order

059 Play unplayed messages first

Hotel Guest: Basic

This FCOS is designed for hotel or motel environments, and has fewer features than FCOS 3 (Restricted). It provides basic play, keep, and discard capabilities and results in the simplest, most user-friendly menus for guests. Mailboxes using this FCOS require no passcodes, recorded names, or personal greetings. You can use this FCOS with a PMS integration or with NuPoint Voice alone. When using this FCOS, disable the passcode and user tutorial in the mailbox, and at the Temporary Passcode prompt, enter 0000.

You can create the Hotel Guest: Basic FCOS with the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

006 Rewind and fast-forward during playback

008 Mailbox can be checked in/out

009 Automatic logout if no messages/receipts

016 Deny recycling with * key

040 Receive messages from other users

041 Receive messages from outside callers **050 Play messages**

052 Auto-play unplayed messages **053 Keep messages 055 Discard messages**

057 Play saved messages in FIFO order

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

122 Define broadcast mailbox

123 Announce broadcast mailbox name

Broadcast

With this FCOS, both system users and outside callers can send a single message to multiple users.

You can create the Broadcast FCOS with the following required and optional feature bits:

Required Features

001 Login to mailbox

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist list messages

045 Receive master dist list messages

Optional Features

070 User Options Menu

071 Record or change mailbox name

073 Enter and change mailbox passcode

074 Create or modify user distribution list

122 Define broadcast mailbox

123 Announce broadcast mailbox name

Note: Feature bit 043 (Receive message of the day) is needed only if the broadcast mailbox is also the user's only mailbox. You can use other feature bits with broadcasting. They are not included in the Broadcast FCOS definition, but you can add or substitute them in a custom FCOS. See the feature bit descriptions for more information on these capabilities:

- 134 (Broadcast message waiting status)
- 174 (Define broadcast greeting mailbox)
- 178 (Define broadcast name mailbox)

Administrator's "No Login" Class of Service

This FCOS allows you to set up the administrator's mailbox to record company greetings and compile master distribution lists, and to prevent unauthorized access. The No Login FCOS is a copy of the FCOS 10 (VIP), but without feature bit 001 (Login to mailbox). Initially, assign the VIP FCOS to the administrator's mailbox. After you record company greetings and compile master lists, change the FCOS to No Login to prevent unauthorized use of the administrator's mailbox. You can switch the FCOS back to VIP whenever you need to access the administrator's mailbox again.

26.25.3 Customizing FCOS

There are two ways to create customized FCOS selections if you need to apply special features to mailboxes. You can:

- copy an existing default FCOS, rename it, re-number it, and add or delete feature bits as required

  OR
- create a new FCOS from scratch

Note:
We recommend that you do NOT modify the default FCOS selections for two reasons:

1. When you modify an FCOS already assigned to a mailbox, all mailboxes with that FCOS behave according to the new definition, and
2. You may need to restore a default FCOS to help in troubleshooting a problem.

Use an FCOS Worksheet and the guidelines in this section to design a customized FCOS. To customize an FCOS, you can either copy a default FCOS or create a new FCOS. If you copy an FCOS, you start with a copy of an existing FCOS, then add or delete the required feature bits. Give this copy a new name and new FCOS number; for example, “10-NoLogin,” if the new FCOS is a copy of FCOS 10 (VIP) without feature bit 001. Although creating a new FCOS gives the experienced system administrator the maximum flexibility to customize call processing, this is the more complex option. Be aware that not all feature bits are compatible. For more information, see Suggested Additional FCOS, Feature Bits by Category and Feature Bit Descriptions in this chapter.

COS Interactions

When you assign an FCOS, a Limits Class of Service (LCOS), and a Group Class of Service (GCOS) to a mailbox, certain options interact within and between each class of service. Some options require the presence of other options, and some combinations are not compatible. For more information see Other Classes of Service. Carefully analyze the intended function of each mailbox before you begin assigning classes of service.

Keep the following interactions in mind:

- The LCOS that you assign can affect the function of an FCOS feature. *For example:* If you give a mailbox the ability to receive user messages (feature bit 040), but you assign an LCOS with a User Message Length limit of 0 seconds, the mailbox will be unable to store an unplayed (or played) user message.
- Interaction between mailboxes is limited by the GCOS that you assign to each mailbox when it is created and by the FCOS assigned to other mailboxes within this GCOS. *For example:*If an FCOS allows a user to make private messages (feature bit 023), other users within the same GCOS must be able to receive messages from other users (feature bit 040) and to play confidential messages (feature bit 051); otherwise, the make private message feature is ineffective.

Note: When you create a COS using the Web console, you must provide a name for it. When you are using the Text console, however, you can create a COS with no name. Since the Web console does not allow you to view or edit an unnamed COS, you must use the Text console to modify (or name) any unnamed COS.

FCOS

Some features require a master feature bit in an FCOS, and some feature bits override others within the same FCOS. See Feature Bit by Category and Feature Bit Descriptions.

LCOS

The LCOS that you assign to each mailbox can affect how a feature functions. For example, if you assign an FCOS that allows a mailbox to make messages (feature bit 020), but you assign an LCOS with a User Message Length limit of 0 seconds, the mailbox user cannot record a message.

GCOS

The GCOS that you assign to each mailbox limits interaction between mailboxes. A user in one GCOS may not be able to receive any messages from a user in another GCOS, regardless of the FCOS. Also, the FCOS for the other mailboxes within one GCOS can affect mailbox interaction. For example, if an FCOS allows a user to make confidential messages (feature bit 023), the other users within the same GCOS must be able to receive messages (feature bit 040) and play messages (feature bit 050).

FCOS Worksheet

When you are familiar with the features you can add to an FCOS, use the FCOS and Feature Bit Descriptions in this section as a basis for completing your FCOS Worksheet. Fill in an FCOS number ("FCOS to modify") and name, and indicate if it is based on an existing FCOS ("FCOS to copy"). Circle all feature bits you wish to include. If you are including all the feature bits in a category, just circle the category name. Assign any number from 18-20 or 25-640 to your FCOS, and any name that helps you easily identify it. Complete one worksheet for each FCOS you design. Keep your completed sheets for future reference.

Note:
FCOS information is stored in blocks of 64 FCOS per OAA record. To save disk space, use all FCOS from 1 to 64 before using higher numbers. Then use 65 to 128, and so forth. You probably will not use all categories listed. For any categories you do use, be sure to include the master feature bits, those feature bits that enable other feature bits within the same category.

26.25.4 Managing FCOS

- Add an FCOS
- Edit an FCOS
- Delete an FCOS
- Assign a new FCOS to a Mailbox
- See FCOS Field Descriptions

Add an FCOS

1. In the navigation tree, click Class of Service, and then click Feature COS. The Feature COS list is displayed.
2. Click Add. The Add FCOS form is displayed.

3. Do one of the following:

   - Copy an existing FCOS by selecting one from the list and clicking the **Copy from** button. The parameters of that FCOS will be copied into your new FCOS, which you can then edit as required. The Next Available FCOS number is automatically applied.

     OR

   - Chose to manually select the feature bits for the new FCOS. In the **Number** field, enter a **number** for this FCOS, or click **Next Available** to automatically assign the next number.

4. In the **Name** field, enter a **name** (up to 15 alphanumeric characters) for this FCOS.
5. By default, the **Category** list displays a sorted list of all feature bits. If you know what category contains the feature bits you want to enable, you can expand the Category list and select the category. Only the feature bits that apply to that category appear.
6. In the **Display** section, you can select how you want to display the available feature bits (All, Checked, Unchecked).
7. Select the check box beside each feature bit that you want to enable for this FCOS. Clear a check box to disable the feature. See FCOS Fields Description in the table below for information.
8. Repeat steps 5 to 7 for additional categories, if required.
9. To save the FCOS and return to the Features COS list, click Save.

Edit an FCOS (Customize)

Best practices for troubleshooting dictate that you always keep your default FCOS settings intact. If you need to modify an FCOS, we suggest that you copy the most appropriate of the default FCOS into a new FCOS (see "Add an FCOS" above) and modify it there. After you save the new FCOS, you need to assign it to the appropriate mailboxes. If you have problems/conflicts with the new COS, you can always restore the default COS until you have finished troubleshooting.

Delete an FCOS

Deleting an FCOS that is in use by mailboxes will cause all of those mailboxes to be assigned the default (1) FCOS. A warning message will be displayed to allow you to cancel the operation. If you are deleting the default FCOS, the mailboxes that have it assigned will automatically be assigned the next available FCOS. You cannot delete the last remaining FCOS in the system; therefore, you cannot select all FCOS for deletion.

To delete one or multiple FCOS:

1. In the Feature COS list, select one or multiple FCOS, and then click Delete. The system will prompt you to confirm the deletion.
2. To confirm the deletion, click Yes to deletea single FCOS or Yes to allto delete all selected FCOS.

   OR

   To reject the deletion, click No.

Assign a New FCOS to a Mailbox

- Follow the procedure to edit a mailbox and when instructed to edit mailbox parameters, enter the new FCOS on the Class of Service tab.

FCOS Fields Descriptions

Field	Description	Values
Number	*Required field. Determines the number of the new FCOS. You can manually enter a number from 1-640 as long as it is not already assigned to an FCOS. You can also click the **Next Available** button to have the system assign the next available number to the FCOS.	Enter a number in the range of 1 -640. The number must not be alr eady used for an existing FCOS. Or click the "Use next available num ber" link.
Name	*Required field. This is the name of the FCOS. (Note: You can create unnamed FCOS using the Text con sole but they are not supported in t he Web console. If you encounter an unnamed FCOS, use the Text c onsole to name it.)	Maximum 15 alphanumeric characte rs.

Field	Description	Values
Category	Allows you to filter the list of features for easier selection. The categories are: • Greeting Features • Login Features • Logout Features • Attendant Call Features • Outside Caller Features • Prompts Features • Receive Messages Features • Play Messages Features • Answer Messages Features • Keep or Discard Messages Features • Make Messages Features • Give Messages Features • Message Addressing Features • User Options • User Distribution Lists Features • Master Distribution Lists Features • Check-In./Check-out • Super User Features • Message Waiting Indicator Features • NP-UM Fax Features • Paging and Message Delivery Features • Voice Gateway and E-mail Features • Network and NP-UM Forms • NP View Features • ISO User Interface Features • Short Message Service Features • NP Talk Features • Dial-back and CLI Features	Select a category (see Description column).

Field	Description	Values
Display	Allows you to choose how to disp lay the feature bits that are displa yed for the category you have select ed. You can choose to display all th e feature bits (both checked and unc hecked), only the selected (checked) bits, or only the cleared bits.	Select either All, Checked, or Unche cked.
Feature bit display area	This area displays the feature bits for the Category you have selected above and filtered with the Display s ettings. Select the check boxes besi de the feature bits that you want to enable for the FCOS. Clear the boxe s for the feature bits that you want to disable for the FCOS.	(Variable. See Description.)

26.25.5 Customize Your FCOS

When you are ready to customize an FCOS, use the FCOS and feature bit descriptions in this section to complete the FCOS Worksheet.

Modify a Copy of an Existing FCOS:

1. Select the existing FCOS that you want to use as a basis for your customized FCOS.
2. Complete an FCOS Worksheet.
3. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(F) Feature COS**.

> **Note**:
> You can quit at any point in the following steps before you exit the Feature Class of Service Menu. Quitting discards all entries you have made and leaves the FCOS settings the way they were before you reached the Feature Class of Service Menu. To quit, select (Q) Quit - Forget Changes from the Feature COS menu.

4. Select **(C) Current FCOS** and enter a **number** for your customized FCOS (18-20 or 25-640).
5. Select **(N) Name FCOS** and enter a descriptive **name** for the customized FCOS.
6. Select **(K) Copy FCOS** and enter the number of the FCOS you want to use as the basis for your customized FCOS. A copy of this FCOS is created and given the number and name you assigned above.

7. To add feature bits to the customized FCOS, select **(A) Add Features** OR to delete feature bits, select **(D) Delete Features** and enter feature bits in the following format:

   - a single bit, for example: 208
   - a range of bits, for example: 202-208
   - a series of bits, for example: 39,40,207,208
   - a mixed entry, for example: 37, 49, 52-72, 201,202 (do not enter spaces after commas and do not end the entry with a comma)
8. To verify that the information you have entered is correct, select **(S) Show FCOS** and enter the **number** of the customized FCOS version.
9. After verification, save the customized FCOS by exiting from the FCOS menu.

Create a New FCOS

To customize an FCOS by creating a new one:

1. Complete an FCOS Worksheet.
2. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(F) Feature COS**.
3. Select **(C) Current FCOS** and enter a **number** for your new FCOS (18-20 or 25-640).
4. Select **(N) Name FCOS** and enter a descriptive **name** for the new FCOS.
5. Select **(A) Add Features** and enter the feature bits that comprise the new FCOS in the following format:

   - a single bit, for example: 208
   - a range of bits, for example: 202-208
   - a series of bits, for example: 39,40,207,208
   - a mixed entry, for example: 37, 49, 52-72, 201,202 (do not enter spaces after commas and do not end the entry with a comma)
6. To verify that the information you have entered is correct, select **(S) Show FCOS** and enter the **number** of the customized FCOS version.
7. After verification, save the new FCOS by exiting from the FCOS menu.

26.25.6 Assign an FCOS to a Mailbox

The steps below assume you have already chosen the default FCOS desired or have already customized an FCOS.

To assign an FCOS to a new or existing mailbox:

1. From the Main Menu, select **(M) Mailbox maintenance**.
2. Select **(C) Create New Mailboxes** and enter the *n*umber of the new mailbox you want to configure.

OR

Select **(M) Modify Mailboxes** to modify an existing mailbox.

Note:
Prompts are almost the same for creating a new mailbox and modifying an existing one, except that "New" precedes a prompt when you select Modify Mailboxes.

1. Press **Enter** until the **Feature Class of Service** or **New FCOS** prompt appears.
2. Enter the **number** (1-640) of the FCOS that will govern this mailbox. The default value is 1. Press **?** for a list of defined FCOS. If you are modifying a mailbox, the FCOS you just entered replaces the existing FCOS.
3. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number. At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.25.7 Add or Delete Feature Bits for an Existing FCOS

It is possible to add or delete feature bits from an existing FCOS, however, we recommend that you do NOT use this as a method of customizing an FCOS. This procedure should only be used to make **global** changes to an existing customized FCOS. Do not add or delete feature bits to a default FCOS - customize an FCOS instead.

Example 1:

All Sales users have custom FCOS 97. You are asked to add feature bit **200 Personal Fax Cover Page** to ALL users who have FCOS 97. In this case, you can add the feature bit to the existing FCOS because ALL users will be affected.

Example 2:

All Sales and Security mailboxes have custom FCOS 92. You are asked to update only the **Sales** mailboxes so that user passcodes are optional, so you'll need to add feature bits 70, 73, and 125. If you add these bits to the FCOS, then ALL mailboxes, (including Security mailboxes), are given the optional passcode feature. In this case, you would copy FCOS 92, re-number it, add the new bits to it, and then apply it to the Sales mailboxes.

To add/delete feature bits to an existing customized FCOS:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(F) Feature COS**.
2. Select **(C) Current FCOS** and enter the **number** of the customized FCOS you want to modify.
3. Select **(A) Add Features** OR to delete feature bits, select **(D) Delete Features** and enter feature bits in the following format:

1.
   - a single bit, for example: 208
   - a range of bits, for example: 202-208
   - a series of bits, for example: 39,40,207,208
   - a mixed entry, for example: 37, 49, 52-72, 201,202 (do not enter spaces after commas and do not end the entry with a comma)

1. After confirming that additions and/or deletions are correct, exit from the Feature Class of Service Menu to save changes.

26.25.8 View FCOS Information

To display summary and detailed lists of FCOS, FCOS bits, and bit descriptions:

To View a Summary of FCOS

You can view FCOS summary information through the System Configuration Menu or the Reports Menu. A summary consists of the FCOS name, its number, and the numbers of the feature bits in the FCOS. FCOS are numbered from 1 to 640.

Sample Summary Report:

```
FEATURE CLASS OF SERVICE

Mon Oct 26 14:36:08 20XX

FCOS: Basic : 1

001 002 003 004 005 006 007 015 017 018 019 020 021 022 023 024 025 026 027 028

029 030 031 032 033 034 035 036 038 040 041 043 044 045 046 047 050 053 055 058

059 061 066 070 071 072 073 074 075 076 077 078 082 083 084 085 086 087 088 092

094 095 096 098 110 124 126 130 132 143 145 147 153 157 158 161 162 169 201 204

215 227

FCOS: CentrexCD 15.00 : 2

001 002 003 004 005 006 007 015 018 019 020 021 022 023 024 025 026 027 028 029

030 031 032 033 034 035 036 038 040 041 043 044 045 046 047 050 053 055 058 059

061 066 070 071 072 073 074 075 076 077 078 082 083 084 085 086 087 088 092 094

095 096 098 110 124 125 126 161 201 204 215 227 292
```

System Configuration Menu

1. From the Main Menu, select **(S) System Maintenance, (R) Reconfiguration**, and then **(F) Feature COS**.

2. *Select* **(S) Show FCOS** and enter your choice of summary in one of the formats shown below.

- A single FCOS **number**, for example 10
- A range of FCOS **numbers**, for example 1-6
- A series of FCOS **numbers**, for example, 1,4,5,12
- **A** for a summary of all FCOS
- **E** for a summary of even-numbered FCOS
- **O** for a summary of odd-numbered FCOS
- **L** for a summary of the lower half of FCOS
- **U** for a summary of the upper half of FCOS

Reports Menu

1. *F*rom the Main Menu, select **(R) Reports**.
2. Select **(F) FCOS**.
3. At the output routing prompt, select one of the following:

- **C** to send the report to the console without pausing
- **P** to send the report to the console, pausing as the screen fills,
- **F** to send the report to a file on the server,
- **A** to append the report to an existing file on the server, or
- **X** to exit report output options (no report)

To View a Description of FCOS

This report consists of the FCOS name, its number, and a description of each feature bit in the FCOS.

```
FCOS: CHECK IN : 4

001 Login to mailbox

004 Outside caller functions

005 Play outside caller menu prompts

066 Login during greeting in greet-only mbx

070 User options menu

071 Record or change mailbox name

072 Record or change mailbox greeting

090 Check in other mailboxes
```

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(F) Feature COS**.
2. Select **(R) Report FCOS** and enter your choice of summary in one of the formats shown below.

- A single FCOS **number**, for example 10
- A range of FCOS **numbers**, for example 1-6
- A series of FCOS **numbers**, for example, 1,4,5,12
- **A** for a summary of all FCOS
- **E** for a summary of even-numbered FCOS
- **O** for a summary of odd-numbered FCOS
- **L** for a summary of the lower half of FCOS
- **U** for a summary of the upper half of FCOS

To View a Description of All Feature Bits

To list all feature bits in numerical order, with a one-line description of each feature bit:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(F) Feature COS**.
2. Select **(H) Help FCOS**.

26.26 Feature Bits by Category - Overview

The following pages summarize all feature bits according to category (as presented in the Web Console). The category numbers are not used for FCOS configuration input, but are provided for reference when designing an FCOS.

Master feature bits appear in bold type. Not all categories have master feature bits. Some feature bit categories require optional feature software, which is described in the summary for each category. Other categories require optional feature software for specific feature bits, only. This is noted by an asterisk (*) at the beginning of the feature bit description. Certain feature bits require that a recipient's mailbox contain "message receiving feature bits," such as those listed under Category 7. Those feature bits are listed beside the required feature bits for making and sending messages. Refer to the Feature Bit Descriptions section for detailed information about each feature bit.

26.26.1 Category 1: Greeting Feature Bits

These feature bits control events that occur during or immediately after the mailbox greeting is played.

To allow the mailbox user to record the mailbox greeting, the FCOS must also contain the following feature bits:

- 070 (User Options Menu)
- 072 (Record or change mailbox greeting)

Bit	Description	Required	Incompatible
060	Ignore DTMF's during greeting		164
062	Hang up immediately after greeting		063, 064, 065
063	Call mailbox attendant after greeting		062, 064
064	Call mailbox user extension after greeting		062, 063
065	Play system time after greeting		
161	Conditional greetings	070	
162	General greetings	070	
164	Skip/pause greeting in greeting only mailbox	062	060
224	*Auto transfer to task before greeting	170	
297	Enable Extended Absence Greeting	161	
298	Disable Message Delivery when Extended Absence Greeting is Enabled	297	133

26.26.2 Category 2: Login Feature Bits

These feature bits control processing when a user logs into a mailbox.

Note:

Zero is an acceptable login character for a line group only when the Configuration Report shows “Key 0 for transfer to attendant during greeting = [N].”

Bit	Description	Required	Incompatible
001	Login to mailbox		
016	Deny recycling with * key		
066	Login during greeting in greet-only mailbox		
069	Passcode required for mobile DID		
081	Only one correct passcode needed for log in		
101-109	Deny login on line groups 1-9		
132	Bad passcode lockout if over limit		
151	Deny 333 access from mobile DID		
152	Deny login within tree	121	
156	Deny login after greeting		

Bit	Description	Required	Incompatible
160	Caller must enter line group access code		
165	Pound key (#) login		
218	Passcode not needed on direct calls		
219	Login in with 0 using cut through paging	171 or 172	
225	*Auto transfer to task upon login	170	

26.26.3 Category 3: Logout Feature Bits

These feature bits control exiting a mailbox. If users can log in, they automatically can log out, either by pressing X, by hanging up, or by not responding to repeated system prompts.

Bit	Description	Required	Incompatible
003	Return to welcome prompt		
009	Automatic Logout if no messages/receipts	052 or 089	
170	*Transfer to Email System	004, 005, 176	
220	No dial extension or Email if unplayed messages	170	
283	Say number of unplayed messages on last logout		

26.26.4 Category 4: Attendant Call Feature Bits

These feature bits control the process to reach an attendant. They allow the user or caller to call the mailbox attendant while logged into the mailbox, such as by pressing 0 (zero).

Bit	Description	Required	Incompatible
002	Transfer to mailbox attendant	004	
013	Operator Transfer via "6" key		
098	Say “Press 0” to caller before beep		
159	Say “Press 0 to return to Receptionist"		

26.26.5 Category 5: Outside Caller Feature Bits

These feature bits control the prompts and privileges that allow outside callers to review, discard, and append to their messages. This category also contains feature bits that require a caller to enter an access code before leaving a message.

Bit	Description	Required	Incompatible
002	Transfer to mailbox attendant		
004	Outside caller functions (Master)	041	
005	Play outside caller menu prompts	004, 041, 088	213
017	Fast line release from outside caller		

Bit	Description	Required	Incompatible
041	Receive messages from outside callers		068, 121
051	Do not switch language for outside callers		
092	User will be in dial-by-name database		
098	Say “Press 0” to caller before beep		
111-119	Deny message receipt on line groups 1-9		
137	Caller must enter access code		
160	Caller must enter line group access code		
176	Say ���Press pound [#] for more options” to callers	004, 005	
203	*Walkaway fax for callers 198		
221	Deny caller transfer to Email	170	176
279	Enable TollSaver for outsider leaving message		

26.26.6 Category 6: Prompts Feature Bits

Prompts feature bits allow the user to interrupt (soft play) prompts and to modify the prompts that the user hears. Also, these feature bits affect some NP Receptionist prompts.

Bit	Description	Required	Incompatible
051	Do not switch language for outside callers		
082	Soft play (interrupt) message count		
083	Soft play (interrupt) most prompts		
097	*Do not say “I will ring (recipients name)” in NP Receptionist		
098	Say “Press 0” to caller before beep		
131	Don't say limits of liability statement		
133	Don��t say “You may start your msg. now”	004, 041	
136	Don’t say “End of message”	050	
138	Don’t say “Message complete”	020	
140	Say full date when playing messages	050	048, 049, 204
146	Don’t say “NuPoint Voice storage is full”		

Bit	Description	Required	Incompatible
157	Repeat message for answering machine		
159	Say “Press 0 to return to Receptionist”		
163	*Don’t play message count		
176	*Say “Press pound [#] for more options” to callers	004, 005	
202	Do not play mailbox name or extension number	020	
208	*Play reorder tone after CTP or greet-only	171 or 172 or 062	
209	Tone only pager mailbox interface		
210	Numeric display pager mailbox interface		
211	Voice pager mailbox interface		
283	Say number of unplayed messages on last logout		
299	Allow choice of unplayed or saved messages during playback		

Bit	Description	Required	Incompatible
301	Enable "Press # when you are finished recording" prompt to make, forward, or answer a message for a mailbox		

26.26.7 Category 7: Receive Messages Feature Bits

These feature bits control processing of messages the user can and cannot receive, as well as notification of the arrival of new messages. Several message sending capabilities require one or more of these feature bits in a recipient's mailbox in order for messages to send properly.

Bit	Description	Required	Incompatible
039	Notification tone when new message arrives		047
040	Receive messages from other users		
041	Receive messages from outside callers		68, 121
043	Receive message of the day		
044	Receive user distribution list messages	040	
045	Receive master distribution lists messages	040	
046	Announce receipt count at login	050	

Bit	Description	Required	Incompatible
047	Notification prompt when new msg arrives		039
088	Receive urgent messages		
111-119	Deny message receipts on line groups 1-9		
127	Deny receipt of messages before tutorial run	070; 040 and/or 041	
173	*Receive cut-through page notify receipt	070, 075, and 171 or 172	
175	Receive broadcast greeting	161, 162	
179	Receive broadcast name		
185	*Receive wake-up call notification receipt	015, 070	
190	*Receive fax messages	040 or 041	
198	*Receive fax messages only	190	
199	*Auto-receipt for fax send	020, 070, 095,190	
223	Delay requested receipt for 24 hours	020, 021, 050	

Bit	Description	Required	Incompatible
241	Suppress broadcast forced receipt number		
279	Enable TollSaver for outside caller leaving message		
286	To allow Mailbox to accept calls without charge		

26.26.8 Category 8: Play Messages Feature Bits

Play Messages feature bits control processing when the user plays messages. This category also contains notification, time stamp, confidential and/or urgent, and order-of-play feature bits.

Bit	Description	Required	Incompatible
006	Rewind and fast forward during playback	050	
007	Pause in record or play	020 or 050 or 024 or 029	
039	Notification tone when new message arrives		047
046	Announce receipt count at login	050	
047	Notification prompt when new msg arrives		039
048	No auto-time stamp of unplayed msgs	050	

Bit	Description	Required	Incompatible
049	No auto-time stamp of played msgs	050, 053	
050	Play messages (Master)		
052	Auto-play unplayed messages	050	089, 227
057	Play saved messages in FIFO order	050, 053	
058	Play unplayed messages in FIFO order	050	
059	Play unplayed messages first	050, 053	
075	Audit receipt message	050	
076	Play urgent messages in FIFO order	050, 088	
089	Auto-play all msgs (new and saved)	050, 053	052, 227
144	Skip forward to next message		048, 049, 204
145	Message stays in original queue		
147	Send receipt after full play	145	

Bit	Description	Required	Incompatible
153	Don’t jump to new message from saved queue	050, 053, and 039 or 047	
163	Don't play message count		
204	Message skip, forward and backward		048, 049, 144
215	Don’t auto-play first msg (w/autoplay)	050, and 052 or 089	
216	Play receipts after urgent messages	050, 088	
255	Delete mailbox without unplayed messages	041, 050	
305	Do not play back the message Caller ID	050	
306	Play back Caller ID after ID	050	305

26.26.9 Category 9: Answer Message Feature Bits

This category controls the Answer function, including attach-message feature bits. Answer messages feature bits allow the user to directly answer messages from other users. For information about marking an answer “confidential,” and activating a return receipt for the answer, see Message Addressing, Category 13.

Bit	Description	Required	Incompatible
019	Answer and mark urgent	029, 040	

Bit	Description	Required	Incompatible
029	Answer messages (Master)		
030	Answer and request receipt	029, 040	
031	Answer and mark confidential	029, 040	
038	Attach original message to answer	029	
147	Send receipt after full play	145	
158	Continue sending message	020 or 024 or 029	
270	Enable Dial-back feature	263, 264, 280	

26.26.10 Category 10: Keep or Discard Messages Feature Bits

These feature bits control options for keeping and discarding messages after users play them. Include feature bit 050 (Play messages) for all keep and discard options. Include 053 (Keep messages) and/or 055 (Discard messages) for any mailbox that can receive messages; otherwise, the user cannot play more than one message during a single session.

Bit	Description	Required	Incompatible
053	Keep messages (Master)	050	
054	Auto-keep messages	050, 053	056

Bit	Description	Required	Incompatible
055	Discard messages (Master)	050	
056	Auto discard messages	050, 055	054, 227
145	Message stays in original queue		
227	Undelete last message with * key	050, 055	052, 056, 089

26.26.11 Category 11: Make Messages Feature Bits

These feature bits allow a user to record (Make) a message and send it to one or more users. This category also contains two feature bits for timing. Message Addressing, Category 13, controls marking messages “confidential,” and activating return receipts for the messages.

Bit	Description	Required	Incompatible
020	Make messages (Master)	040	
021	Make and request receipt	020, 040	
022	Make to multiple destinations	020, 040	
023	Make and mark confidential	020, 040	
032	Make to user distribution list	020, 040, 044	
034	Make to master distribution list	020, 040, 045	

Bit	Description	Required	Incompatible
061	Wait to record	022 or 026	
087	Make and mark urgent	020, 040	
092	User will be in Dial-by-Name database		
096	Make messages before keep/discard	020, 040	
110	Make/give to telephone number	020, 024. 040	
126	Make/give to mailbox with empty GCOS	020, 040, 041	
157	Repeat message from answering machine	110	
158	Continue sending message	020 or 024 or 029	
171	Cut-through Paging	070	
172	Cut-through Paging and messaging	070	
188	Append # to end of cut-through page number	070, 171 or 172	
191	Make fax messages	020	

26.26.12 Category 12: Give Messages Feature Bits

These feature bits control processing when users forward messages to single or multiple users, with or without additional comments. This category also contains receipt feature bits. This category does not allow users to send or broadcast messages marked “confidential.”

Bit	Description	Required	Incompatible
018	Give and mark urgent	024, 040	
024	Give messages (Master)	040	
025	Give and request receipt	024, 040	036
026	Give to multiple destination	024, 040	036
027	Give and mark confidential	024, 040	
028	Give with comments	024, 040	
033	Give to user distribution list	024, 040, 044	
035	Give to master distribution list	024, 040, 045	
061	Wait to record	022 or 026	
084	Give receipt message with comments	040, 075, 086	
085	Give receipt message to multiple destinations	024, 040, 086	
086	Give receipt message (Master)	040	
110	Make/give to telephone number	020 or 024, 040	

Bit	Description	Required	Incompatible
126	Make/give to mailbox with empty GCOS	020, 040	
157	Repeat message for answering machine	110	
158	Continue sending message	020 or 024 or 029	
192	Give fax messages	024, 190	

26.26.13 Category 13: Message Addressing Feature Bits

These feature bits control processing after a user makes, gives, or answers a message. They allow a user to make a message confidential, to make a message urgent, to request a return receipt, or to set future delivery.

Bit	Description	Required	Incompatible
018	Give and mark urgent	024, 040	
019	Answer and mark urgent	029, 040	
021	Make and request receipt	020, 040	
023	Make and mark confidential	020, 040	
025	Give and request receipt	024, 040	
027	Give and mark confidential	024, 040	

Bit	Description	Required	Incompatible
030	Answer and request receipt	029, 040	
031	Answer and mark confidential	029, 040	
087	Make and mark urgent	020, 040	
095	Mark message for future delivery	020, 040	
284	Provide Callback Number Delivery Options		

26.26.14 Category 14: User Options Feature Bits

These feature bits, some of which require optional feature software, allow users to reach the User Options menu and record names and greetings, set passcodes, make distribution lists, activate the user tutorial, allow a pager, and activate NP WakeUp.

Bit	Description	Required	Incompatible
015	*Change wakeup options	070	287
070	User Option Menu (Master)		
071	Record or change mailbox name	070	
072	Record or change mailbox greeting	070	
073	Enter or change mailbox passcode	070	

Bit	Description	Required	Incompatible
074	Create or modify user distribution list	032 and/or 033, and 070	
077	Change pager schedule	070	
078	Activate user tutorial	070	
093	Deny change of passcode in first tutorial		
094	Change message delivery options	070	
095	Mark message for future delivery	020, 040	
124	Change paging phone number	070	
125	Clear user passcode	070, 073	
127	Deny receipt of messages before tutorial run	040, 041, 070	
130	Passcode cannot be same as mailbox	070, 073	
142	Must run tutorial from own phone (SMDI)	070, 073, 093	
143	Change message delivery phone number	070	
148	*Change wakeup phone number	015, 070	

Bit	Description	Required	Incompatible
180	Record personal wake up message		
195	Specify fax delivery number		
196	Change default fax number		
201	Deny Trivial Passcode		
242	Save variable passcode prompts for business guest mailboxes		
249	Allow Transfer to Help Desk during tutorial		
287	*Enhanced auto wakeup		015
289	Enable UM - SMTP	161	
290	Enable UM - Web View		
291	Enable RAC (Record a call)		
292	Enable NP Call Director		
293	Disable the <Save> <Reply> and <Forward> buttons on the UM Standard Web View web pages		

Bit	Description	Required	Incompatible
294	Enable the Mitel embedded player on the UM Standard Web View web pages		
300	Enable secure tutorial		

26.26.15 Category 15: User Distribution Lists Feature Bits

These feature bits allow a user to create and use distribution lists, which designate a group of mailboxes to send a single message to. A user distribution list can have up to 65,535 members. Each mailbox can have up to 99 distribution lists. User distribution lists can be used only by the user who is logged in to the mailbox where the list is stored.

Bit	Description	Required	Incompatible
032	Make to user distribution list	020, 040, 044	
033	Give to user distribution list	024, 040, 044	
036	Auto receipt for user distribution list	020, 032 and/or 033, 040, 044	021, 025
044	Receive user distribution list messages	040	
074	Create or modify user distribution list	032 and/or 033, 070	
134	Broadcast message waiting status	040 and/or 044, 070, 074	122
222	Deny nesting of distribution lists	070, 074	

26.26.16 Category 16: Master Distribution Lists Feature Bits

These feature bits allow the system administrator to create and use master distribution lists. They also allow a user to make messages for a Master List and to receive Master List messages. Master Distribution Lists are stored in the administrator's mailbox and designate groups of mailboxes that a user can send a single message to. Master distribution lists are available to any mailbox with the appropriate feature bits, listed below. There are 99 master lists available. Master distribution list numbers use two leading zeros. To address a message to master list 1, enter 001. For master list 99, enter 0099.

Bit	Description	Required	Incompatible
034	Make to distribution list	020, 040, 045	
035	Give to distribution list	024, 040, 045	
045	Receive distribution list messages	040	

26.26.17 Category 17: Check In/Check Out Feature Bits

These feature bits allow a hotel, motel, or telephone answering service (TAS) operator to set up mailboxes for a guest or client by recording a name or greeting, setting a passcode, or activating the tutorial. The operator can also clear messages after a guest or client leaves.

Bit	Description	Required	Incompatible
008	Mailbox can be checked in/out		
090	Check in other mailboxes	008	
091	Check out other mailboxes	008	

26.26.18 Category 18: Super User Feature Bits

These feature bits allow the user to create tree, broadcast, and rotational mailboxes. These mailboxes require that the distribution lists indicate which child mailboxes the lists branch to.

Bit	Description	Required	Incompatible
068	Define rotational mailbox		041, 121, 122
120	Default to first child of tree mailbox	121	186
121	Define tree mailbox (Master)	070, 072	041, 122, 187
122	Define broadcast mailbox (Master)	040 and/or 044	068,121, 134
123	Announce broadcast mailbox name	040 and/or 044, 070, 071, 122	
141	*Define chain mailbox in Receptionist		
147	Send receipt after full play	145	
152	Deny login with tree	121	
174	Define greeting for broadcast mailbox	161, 162, 175	
178	Define name for broadcast mailbox	179	
186	Default to last child of tree mailbox	121	120
187	*Receptionist call-transfer tree mailbox		121
189	Rotate on full mailbox		

Bit	Description	Required	Incompatible
229	Play names of list 1 children		
231	Broadcast Mailbox passcode	232	
232	Allow receipt of Broadcast passcode		
234	Check message wait status of children	070, 072, 121, 134, 229	
255	Delete Maibox if no unplayed messages		
277	Send Mail Waiting Notice after Mbox Deletes		

26.26.19 Category 19

26.26.20 Category 20: NuPoint Fax Feature Bits

These feature bits control use of the NuPoint Fax optional feature. To use these feature bits, you must have purchased the Fax feature and installed it on the NuPoint Unified Messaging server.

Bit	Description	Required	Incompatible
190	Receive fax messages	040 or 041	
191	Make fax messages	020	
192	Give fax messages	024, 190	

Bit	Description	Required	Incompatible
193	Deliver fax to default number	070, 190 *110 is required to send a fax to an external machine. It is not required to send internal faxes.	
194	Deliver fax online	190	
195	*Specify fax delivery number	070, 190 *110 is required to send a fax to an external machine. It is not required to send internal faxes.	
196	*Change default fax number	070, 190, 193	
197	Fax-on-Demand for Greeting Only mailbox	004, 005, 190	
198	Receive fax messages only	190	
199	Auto-receipt for successful fax send	020, 070, 095, 190	
200	Personal fax cover page	190	
203	Walkaway fax for callers	190	
206	Discard fax message after delivery		237

Bit	Description	Required	Incompatible
207	Fax Verify (sending system not self)		198
230	Deny change of fax cover page options	070, 190	
235	Display FROM field on fax cover page	190	
236	Display Promotional Message on fax cover page	190	
237	Automatically delivers fax message to default number	070, 190	206
239	Retrieve fax on voice recording timeout	070, 190	
240	Receive fax on voice recording timeout	070, 190	
247	Don't play any prompt to fax call placement recipient		
256	Enable fixed greet 'Press1 or wait...' for walkaway fax	203	
290	Enable UM - Web View		

26.26.21 Category 21: Paging and Message Delivery Feature Bits

These feature bits control paging and message delivery options. Some of these feature bits allow a user to override a default schedule or pager number. Set up the Pager application to use these feature bits. Cut-through Paging is an optional feature.

Bit	Description	Required	Incompatible
077	Change pager schedule	070	
079	Set message wait #1 for urgent messages only	040, 041, 088	080, 228
080	Set message wait #2 for urgent messages only	040, 041, 088	079, 228
124	Change paging phone number		070
163	Don’t play message count		40-45, 88, 175, 179
168	Message wait 1, pager requeue		
169	Message wait 2, pager requeue		
171	Cut-through Paging	070	
172	Cut-through Paging and messaging	070	
173	Receive cut-through page notify receipt	070, 075, 171 or 172	

Bit	Description	Required	Incompatible
181	Paging over message delivery, message waiting 1 over message waiting 2	070, 077	
188	Append # to end of cut-through page number	070, 171 or 172	
208	Play reorder tone after CTP or greet-only	171 or 172	
209	Tone only pager interface		
210	Numeric display pager mailbox interface		
211	Voice pager mailbox interface		
212	Send page upon answer, greet-only mbox		
213	Edit CTP number with * key if no caller menu	171 or 172	005
219	Login with 0 using cut-through paging	171 or 172	
228	Set msg wait #3 for urgent msgs only	040 and/or 041, and 088	079, 080

26.26.22 Category 22: Email Feature Bits

These feature bits control use of the Email interface or the text counter. Other applications can use the text counter; for example, a hotel can use the text counter to show physical (written) messages waiting for a guest. The Email interface is optional.

Bit	Description	Required	Incompatible
154	Announce text (Email) message count		217
170	Transfer to Email System	004, 005, 176	
184	Append mailbox number to transfer		
205	Do not use text count for message waiting		
217	Announce text messages without count		154
220	No dial extension or Email if unplayed messages	170	
221	Deny caller transfer to Email	170	176
224	Auto-transfer to task before greeting	170	
225	Auto-transfer to task upon login	170	
226	Auto-transfer to task after unplayed messages	170	

26.26.23 Category 23: Network and NP Forms Feature Bits

These feature bits control processing for the AMIS Analog or NP Forms optional features.

Bit	Description	Required	Incompatible
135	Define template mailbox (NP Forms)		
139	Template: Assume last greet mailbox FCOS	135	
149	Login to template through rotational mailbox	135	
166	AMIS Analog networking		

26.26.24 Category 24: Web View (NP PWG) Feature Bits

The Web View (or Personal Web GUI -- PWG) optional feature integrates multimedia messaging by allowing a personal computer user to send, receive, create, edit, and store voice and fax messages in a Microsoft Windows environment.

Bit	Description	Required	Incompatible
110	Make/Give to telephone number	020, 024, 040	
250	Allow NP PWG login		
251	Allow NP PWG telephoneplayback/ record	250	259
252	Allow NP PWG client to change mailbox ID	250	
257	Prevent NP PWG client voice playback/record	250	251

Bit	Description	Required	Incompatible
258	Prevent NP PWG client from using local storage	250	
259	Restrict NP PWG client to play only faxes	250	251
260	Allow NP PWG user to have caller ID lookup	250	
261	Allow NP PWG View WEB access to messages		
262	Store caller line ID as a phone number	250, 260	
263	Store caller line ID as phone number or mailbox number		

26.26.25 Category 26: Short Message Service Feature

Bit	Description	Required	Incompatible
014	Outdial for SMSC		
167	(ISO) SMS Short Text Option Enabled		
214	(ISO) SMS Voice Messaging Option Enabled		
266	Enable SMSC for Callback Numbers		

Bit	Description	Required	Incompatible
267	Enable SMSC for Short Text Messages		
268	Enable SMSC Receipts		
269	(ISO) SMS Allow Urgent Delivery		
271	Send SMSC Cancel VMNs for ML_OFF		
272	Send SMSC Cancel CBNs for ML_OFF		
275	Enable SMSC customized text messages		
278	(ISO) SMS Callback Number Enabled		

26.26.26 Category 27: NP Talk Features

Bit	Description	Required	Incompatible
099	NP Talk with talkover		
100	Disable talkover		

26.26.27 Category 28: Dial-back and CLI Features

Bit	Description	Required	Incompatible
262	Store Caller Line ID as a phone number		

Bit	Description	Required	Incompatible
263	Store Caller Line ID as a phone or mailbox number		
264	Play outside caller user interface (with FCOS bit 280)		
265	Enable NP RapidDial Features		
270	Enable Dial-back Feature		
280	Enable CLI Outside Caller interface (with FCOS bit 264)		

26.27 Feature Bits 001 to 049

This section describes all feature bits, listed in numeric order. Master feature bits are identified in the feature bit title. If one feature bit overrides or conflicts with another, this fact is noted.

Note:
Remember that not only FCOS determine how NuPoint Voice behaves. Check that LCOS and GCOS are also set properly. For example, if you use bitmapped GCOS, and some mailboxes do not share GCOS, one mailbox cannot send a message to another, even though the FCOS contains the send and receive feature bits. For details, see chapter 8.

001 Login to Mailbox

Allows the user to reach the user's mailbox. If a passcode is set, the user must enter it to gain access. Without this feature bit, the server tells the user that the mailbox cannot be reached, then hangs up; this forces a user to contact the system administrator.

002 Transfer to Mailbox Attendant

Allows a user who is logged in—to press 0 at any time during the session, to reach an attendant for assistance. This feature also allows a caller—while connected to a mailbox—to press 0, which transfers

the call to an attendant. If the configuration is set for “Key 0 to reach attendant during greeting = N,” then a caller must wait until after the greeting. If a caller does not wait, the 0 is interpreted as a login character. The server transfers the caller or user to the system attendant’s extension; if that extension is not defined, the server connects the call to the attendant’s mailbox, which has special privileges. If neither attendant is configured, the user or caller hears, “I’m sorry. I don’t understand that command.” Requires feature bit 004 (Outside caller functions).

003 Return to Welcome Prompt

Also known as the “recycle” feature. Allows the user to log out by pressing X, then press any key to return to the main company greeting. Otherwise, a user must hang up and call back. This allows the user to avoid toll charges for succeeding calls.

If the user logs out from a port configured for NP Receptionist:

- The server prompts the user to press 0 to return to NP Receptionist. If the user presses 0, NP Receptionist prompts the user to enter an extension number.
- If the user presses any key other than 0, the server prompts the user to enter a mailbox number. After this point, users can be connected only to a mailbox, not transferred to an extension.

If the user logs out from a port configured as a message center, the user can press any key, including * or 0, during the logout prompt to interrupt and return to the welcome prompt. No prompts play for the recycle feature.

004 Outside Caller Functions (Master Feature Bit)

Allows outside callers to review, discard, append to, and re-record messages, and also to mark messages urgent. Without this bit, callers cannot use these options, and messages are delivered after five seconds of silence or when the caller hangs up.

This feature bit is also used for the Cut-Through Paging (CTP) optional feature. To activate CTP when outside caller functions are on, the caller presses the i key. To activate CTP when outside caller functions are off, the caller enters the telephone number directly. Requires feature bit 041 (Receive messages from outside callers).

Note: Include feature bit 005 (Play Outside Caller Menu prompts) allow the server to prompt for outside caller functions; however, prompts are not required.

005 Play Outside Caller Menu Prompts

Allows a caller to hear prompts in the caller’s menu: “Press R to review a message, A to append it, D to discard it, U for urgent, X to exit the system, and 0 to return to attendant.”

Requires the following feature bits:

- 004 (Outside caller functions)
- 041 (Receive messages from outside callers)
- 088 (Receive messages marked urgent)

Do not use with feature bit 213 (Edit CTP num with * key if no caller menu).

006 Rewind and Fast Forward During Playback

Although the system is not tape-based, it simulates a tape recorder. Allows a user playing a message to press the * (star) key to rewind the message or the # (pound) key to fast forward. Each time the user presses a key, a portion of the message rewinds or fast-forwards.

Requires feature bit 050 (Play messages).

007 Pause in Record or Play

Allows the mailbox user to press the 1 key to pause while recording or playing back a message. When the user presses the 1 key again, play resumes. No prompts play for this feature, and outside callers cannot use it.

Allows the mailbox user to press the 1 key to pause for 90 seconds while recording or playing back a message. When the user presses any other key, play resumes after the beep. No prompts play for this feature, and outside callers cannot use it. You should users if they have this capability. Users hear a beep every five seconds during the pause.

Requires at least one of the following feature bits:

- 020 (Make messages)
- 024 (Give messages)
- 029 (Answer messages)
- 050 (Play messages)

008 Mailbox Can be Checked In/Out

Allows a hotel desk clerk to:

- Record a name and greeting, and to assign a passcode to the mailbox of each new guest or customer.
- Clear the name, greeting, passcode, and messages from the mailbox of a departing guest or customer.

This is required for guest mailboxes, those assigned to individual guests, or customers.

009 Automatic Logout If No Messages/Receipts

Automatically logs the user out after the last message in the mailbox is either kept or discarded; the user can go through the queue of unplayed and played messages only once. If the user has no unplayed messages when logging in, the server Prompts, “You have no unplayed messages in your mailbox,” and automatically logs the user out.

Interacts with the following feature bits:

- 052 (Auto-play unplayed messages)
- 089 (Auto-play all msgs, new and saved)

The following table describes how feature bits 009, 052, and 089 interact in an FCOS.

Table: Logout Interaction with Auto-Play			
Message State	**Feature Bit 052**	**Feature Bit 089**	**NuPoint Voice Action**
No messages	In or out of FCOS	In or out of FCOS	Logs user out immediately.
All unplayed	In FCOS		Logs user out after user plays all messages.
In or out of FCOS	In FCOS	Logs user out after user plays all messages.	
Receipts only	In or out of FCOS	In FCOS	Logs user out after user plays all messages.
Receipts and all unplayed	In or out of FCOS	In FCOS	Logs user out after user plays all messages.
Played only	In FCOS		Prompts user to play mes sages.
In or out of FCOS	In FCOS	Automatically plays all messages, the logs user out.	
Played and receipts	In or out of FCOS	In FCOS	Automatically plays all receipts and messages, t hen logs user out.

010 (ISO) Enhanced Outcall Paging Options

There are two different outcall/paging features in the ISO user interface. When this feature bit is off, the basic outcall/paging feature is activated, and the enhanced outcall/paging feature is deactivated. When this feature bit is on, the basic outcall/paging feature is deactivated and the enhanced outcall/paging feature is activated.

Basic Outcall/Paging Feature

Users are prompted to set outcall/paging schedule and phone number in a particular sequence.

Enhanced Outcall Paging Options

Users are provided with an outcall/paging setup menu. The outcall/paging schedule and phone number can be set up in different sequences with the menu options. For information about enabling the phone number and schedule options in the outcall/paging setup menu, refer to bits 77, 94, 124 and 143.

011 (ISO) Play Standard Greeting

When this feature bit is on and a greeting name is not recorded, the company standard greeting will be played. When this feature bit is off, a general greeting is played.

012 (ISO) Short Message Service

When this feature bit is on and the ISO SMS optional feature is installed, the ISO SMS main menu is activated. The ISO SMS main menu provides options for sending a callback number, leaving a voice message, and leaving a short text message.

Related bits: 167, 214, 269, 278 and 284.

This feature bit also works with SMPP MWI and SMPP CBN.

013 Operator Transfer Via "6" Key

Not Used.

014 Outdial for SMSC

This feature bit is only used in SMS MWI software. With this feature on, the NuPoint system will dial the subscriber and log the user in to their mailbox whenever there are unplayed messages. This feature is not available with CDMS or SMPP software.

015 Change Wakeup Options

Allows the user to schedule wakeup calls through the TUI from the User Options menu. Do not use this with feature bit 287 (Enhanced auto wakeup).

Requires the following elements:

- Feature bit 070 (User Options Menu)
- A defined pager port
- NP WakeUp optional feature; for details, see the NP WakeUp Guide

016 Deny Recycling with * Key

Prevents the user from pressing the * (star) key to return to the company greeting during the prompt for a passcode. This prevents an unauthorized user or caller from “cycling” through mailboxes in search of one that is not passcode-protected.

You might want to omit this feature bit in an integrated environment to allow users to log in to their mailboxes from other users’ phones.

017 Fast Line Release from Outside Caller

Plays the caller’s menu only once. If the caller does not respond within ten seconds, the server thanks the caller and hangs up. Otherwise, the caller’s menu plays three times unless the caller presses X before hanging up. If the caller does not press X and hangs up, the line can be tied up until the menu plays three times. The exact length of the tie-up varies with the PBX.

018 Give and Mark Urgent

Allows the user to mark a message for another user as urgent. The user presses G to give the message and records any desired comments. To mark the message urgent, the user presses M to reach the Message Addressing menu, then presses U for urgent. (To cancel urgent, the user presses U again.) To send the message, the user presses X until the server announces “your message sent.” Urgent messages play before all other messages only if the recipient’s FCOS includes feature bit 088 (Receive urgent messages). Otherwise, the message plays with all other unplayed messages in the order received.

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other users) in the recipient mailbox.

019 Answer and Mark Urgent

Allows the user to mark an answer urgent to another user as urgent. The user presses A to answer the message. To mark the answer urgent, the user presses M to reach the Message Addressing menu, then presses U for urgent. (To cancel urgent, the user presses U again.) To send the message, the user presses X until the server announces “your answer sent.” Urgent messages play before all other messages only if the recipient’s FCOS includes feature bit 088 (Receive urgent messages). Otherwise, the message plays with all other unplayed messages in the order received.

Requires feature bits:

- 029 (Answer messages)
- 040 (Receive messages from other users) in the recipient mailbox.

020 Make Messages

Allows the user to make a message when in the mailbox by pressing M (for make), entering the recipient’s mailbox number, recording a message, and pressing X to send it.

Requires feature bit 040 (Receive messages from other users) in the recipient mailbox.

021 Make and Request Receipt

Allows the user to make a message and request a return receipt after the recipient plays the message. The user presses M to make a message. To request a receipt, the user presses M to reach the Message Addressing menu, then presses R to request a receipt. (To cancel the receipt, the user

presses R again.) To send the message, the user presses X until the server announces that it has sent the message. The return receipt works like the Auto-receipt feature for distribution lists described in feature bit 036 (Auto-receipt for user dist list msgs).

Requires feature bits:

- 020 (make messages)
- 040 (Receive messages from other users) in the recipient mailbox.

022 Make to Multiple Destinations

Allows the user to make a message and send it to up to 200 addresses per message without using a distribution list. After the user presses M for make, the server prompts for a mailbox number. The user adds mailboxes, presses the # (pound) key when done adding recipients, then records a message. The address list that the user builds can include other mailboxes or distribution lists, if the FCOS includes feature bit 032 (Make to user distribution list).

Requires feature bits:

- 020 (Make messages)
- 040 (receive messages from other users) in the recipient mailbox

023 Make and Mark Confidential

Allows the user to make a message that cannot be given by the recipient to another user. The user presses M to make a message, and records a message. To mark the message confidential, the user presses M to reach the Message Addressing menu, then presses C for confidential. (To cancel confidential, the user presses C again.) To send the message, the user presses X until the server announces that the message has been sent.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) in the recipient mailbox

024 Give Messages

Allows the user to send a copy of a message to another user by pressing G, entering the mailbox number of the recipient, and pressing X to send the message. The message cannot have been marked confidential by the original sender.

Requires feature bit 040 (Receive messages from other users) in the recipient mailbox.

025 Give and Request Receipt

Allows the user to give a message to another user and request a return receipt. The user presses G to give a message and records comments. To request a receipt, the user presses M to reach the Message Addressing menu, then presses R to request a receipt. (To cancel the receipt, the user presses R again.) To give the message, the user presses X until the server tells the user it has sent the message.

Overrides feature bit 036 (Auto-receipt for user dist list msg).

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other user) in the recipient mailbox

026 Give to Multiple Destinations

Allows a user to give a message to up to 200 addresses per message without using a distribution list. After the user presses G to give a message, the server prompts for a mailbox number. The user adds mailboxes, then presses the # (pound) key to send the message. The address list that the user builds can include distribution lists if the FCOS also includes feature bit 033 (Give to user distribution list).

Overrides feature bit 036 (Auto-receipt for user dist list msg).

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other users) in the recipient mailbox

027 Give and Mark Confidential

Allows the user to give a message that cannot then be given by the recipient to another user. The user presses G to give a message, and then records comments. To mark the message as confidential, the user presses M to reach the Message Addressing menu, and then presses C for confidential. (To cancel confidential, the user presses C again.) To give the message, the user presses X until the server announces it has sent the message.

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other users) in the recipient mailbox

028 Give with Comments

Requires the user to record additional comments when giving a message to one or more users.

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other users) in the recipient mailbox Do not add this to an attendant's mailbox.

029 Answer Messages

Allows the user to answer messages from other users. When a user plays a message from another user, the user can press A to answer the message. The server automatically enters the mailbox number of the sender, so a recipient does not need to know or enter the sender's mailbox number.

030 Answer and Request Receipt

Allows the user to request a return receipt when answering a message from another user. The user presses A to answer a message, and then records comments. To request a receipt, the user presses M to reach the Message Addressing menu, then presses R to request a receipt. (To cancel the receipt, the user presses R again.) To send the message, the user presses X until the server announces that the answer was sent.

Requires feature bits:

- 029 (Answer messages)
- 040 (Receive messages from other users) in the recipient mailbox

031 Answer and Mark Confidential

Allows the user to answer a message with a reply that cannot then be given by the recipient to another user. The user presses A to answer a message, then records an answer. To mark the message as confidential, the user presses M to reach the Message Addressing menu, and then presses C for confidential. (To cancel confidential, the user presses C again.) To send the message, the user presses X until the server announces that it has sent the message.

Requires feature bits:

- 029 (Answer messages)
- 040 (Receive messages from other users) in the recipient mailbox

032 Make To User Distribution List

Allows users to make and send messages to distribution lists or mailboxes and distribution lists, instead of entering each mailbox number individually.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) and 044 (Receive user dist list messages) in the recipient mailbox

033 Give To User Distribution List

Allows a user to give a message to a distribution list, instead of entering each mailbox number individually. The message cannot have been marked confidential by the original sender. (A user can also enter both individual mailboxes and distribution lists.)

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other users) and 044 (Receive user dist list messages) in the recipient mailbox

034 Make To Master Distribution List

Allows the user to record a message for delivery to a master distribution list.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) and 045 (Receive master dist list messages) in the recipient mailbox.

035 Give To Master Distribution List

Allows the user to give a message to a master distribution list. The message cannot have been marked confidential by the original sender.

Requires feature bits:

- 024 (Give messages)
- 040 (Receive messages from other users) and 045 (Receive master dist list messages) in the recipient mailbox.

036 Auto-receipt for User Dist List Msgs

Allows the server to automatically generate a receipt for a message sent to a distribution list. When the user logs in to a mailbox, the receipt announces which users have not played the message and which

users have played the message and when they played it. Each time the user logs in, the updated receipt plays. Receipts are updated until the user discards them. You can cancel Auto-receipt if the FCOS contains either feature bit 021 (Make and request receipt) or 025 (Give and request receipt).

Requires feature bits:

- 020 (Make messages)
- 032 (Make to user distribution list) and/or 033 (Give to user distribution list)
- 040 (Receive messages from other users) and 044 (Receive user dist list messages) in the recipient mailbox

037 Not Used

038 Attach Original Message to Answer

Attaches the original message to the answer. The server plays the answer first, then all attached messages in reverse order. This can help users track questions and answers in a “conversation” because an answer is always accompanied by the original message, but it uses extra disk space. If a user gives an answer from this conversation to another mailbox, that answer includes the original message and all accumulated answers.

Requires feature bit 029 (Answer messages).

039 Notification Tone When New Msg Arrives

Notifies the user of any new message that arrives while the user is logged in. When the user presses a key after finishing any transaction, the user hears a beep.

Feature bit 047 (Notification prompt when new msg arrives) overrides this.

040 Receive Messages from Other Users

Allows a user to receive messages from other users. If you use bitmapped GCOS, the mailboxes must have a GCOS with at least one matching group.

041 Receive Messages from Outside Callers

Allows a mailbox to receive messages from outside callers.

Overrides feature bits:

- 068 (Define rotational mailbox)
- 121 (Define tree mailbox)

042 Not Used

043 Receive Message of the Day

Allows the user to receive the message of the day, an announcement from the attendant’s mailbox. The message plays automatically, immediately after a user logs in, and does not play again after it plays twice.

The first play is a hard play (the user must hear it); the second play is a soft play (if the user enters a command, the rest of the message is ignored).

044 Receive User Dist List Messages

Allows a mailbox to be added to the distribution lists of other users, and to receive messages from these distribution lists.

Requires feature bit 040 (Receive messages from other users) in the recipient mailbox.

045 Receive Master Dist List Messages

Allows a mailbox included in a master distribution list to receive user messages that are addressed to the master distribution list. Mailboxes with feature bits 034 (Make to master distribution list) or 035 (Give to master distribution list) can make or give messages to mailboxes with this feature.

Requires feature bit 040 (Receive messages from other users) in the recipient mailbox.

046 Announce Receipt Count at Login

Allows users to hear, when they log in, how many receipts are in the mailbox. Receipts are kept until users delete them. Otherwise, users can play receipts but do not hear how many receipts they have when they log in.

Requires feature bit 050 (Play messages).

047 Notification Prompt When New Msg Arrives

Plays a prompt that tells the user, who has completed a transaction in the mailbox, how many new messages have arrived since the previous transaction.

Overrides feature bit 039 (Notification tone when new msg arrives).

048 No Auto-timestamp of Unplayed Msgs

The server will not play time stamps for previously unplayed messages, and the user will not know when messages were actually received. Use this when the user has a voice pager with limited time. To hear the time stamp, the user presses T while the message plays, or T-1 if the FCOS includes feature bit 204 (Message skip, forward and backward). The user cannot play the time stamp if the FCOS includes feature bit 144 (Skip forward to next message). When a user replays a message, the time stamp plays if feature bit 049 (No auto-time stamp of played msgs) is not in the FCOS.

Requires feature bit 050 (Play messages).

049 No Auto-timestamp of Played Msgs

The server will not play time stamps for previously played messages, and the user will not know when messages were actually received. However, if that user gives a message to a mailbox without this feature bit, the time stamp plays for the recipient. To hear the time stamp, the user presses T while the message plays, or T-1 if the FCOS includes feature bit 204 (Message skip, forward and backward). The user cannot play the time stamp if the FCOS includes feature bit 144 (Skip forward to next message).

Requires feature bits:

- 050 (Play messages)
- 053 (Keep messages)

26.27.1 Feature Bits 050 to 099

050 Play Messages (Master Feature Bit)

Allows the user to play all messages received by the mailbox. The ability to receive messages is controlled by feature bits in the Receive Messages category. The Keep/Discard category also requires this feature.

051 Do Not Switch Language for Outside Callers

Plays prompts for the outside caller in the language of the caller's mailbox. For example, with this, an outside caller hears prompts in Spanish if a call from a mailbox set to Spanish reaches a chain mailbox set to English. Otherwise, the prompts play in the language of the called mailbox. Languages are set in the line group and the mailbox LCOS.

Mailbox LCOS language settings take priority over Line Group language settings so callers may receive prompts in an unexpected language when they reach the mailbox level. (For example, callers to a multilingual system select English prompts but connect to a mailbox with a French LCOS setting. Even though they have selected English, the prompts at the mailbox level will be in French.) If you want callers to continue to be prompted in their selected language, assign this feature bit to the FCOS of the user mailbox.

052 Auto-play Unplayed Messages

The server automatically plays the next unplayed message in the queue after the user keeps or discards the current message.

Note: Feature bit 089 (Auto-play all msgs, new and saved) overrides this. See Logout Interaction with Auto-play for more information. With feature bit 215 (Don't auto-play first msg, w/auto-play), a mailbox does not automatically play the first message and the user can perform other functions in the mailbox. If the user presses P to play the first unplayed or saved message, all subsequent unplayed messages then play.

Requires feature bit 050 (Play messages).

You cannot use this with feature bit 227 (Undelete last message with * key).

053 Keep Messages (master Feature Bit)

Allows the user to save messages by pressing K for keep. NuPoint Voice plays the "message kept" prompt and stores the message in the played messages queue. Include this in any mailbox that can receive messages.

Requires feature bit 050 (Play messages).

054 Auto-keep Messages

WARNING - To prevent a system malfunction, never put feature bits 054 and 056 in the same FCOS.

The server automatically keeps a message after it has been played, then plays a prompt that the message has been kept. If the FCOS includes feature bit 055 (Discard messages), the user has a few seconds to manually keep or delete the message before it is kept.

Requires feature bits:

- 050 (Play messages)
- 053 (Keep messages)

055 Discard Messages (Master Feature Bit)

Allows the user to delete a message by pressing D for discard. Include this in any mailbox that can receive messages. If a user can receive messages but cannot discard them, messages can be deleted only by automatic or manual purge them. (The LCOS assigned to a mailbox determines the timing of automatic purges.)

Requires feature bit 050 (Play messages).

056 Auto-discard Messages

WARNING - To prevent a system malfunction, never put feature bits 054 and 056 in the same FCOS.

The server automatically discards a message after it plays. If feature bit 053 (Keep messages) is included, the user has a few seconds to manually keep or delete the message before it is discarded. Use care when assigning this feature bit. If a user is disconnected while a message plays, that message is considered played and is discarded.

Requires feature bits:

- 050 (Play messages)
- 055 (Discard messages) You cannot use this with feature bit 227 (Undelete last message with * key).

057 Play Saved Messages in FIFO Order

Plays kept messages in first-in-first-out (FIFO) order so that earlier saved messages play first. Otherwise, saved messages play in last-in-first-out (LIFO) order.

Requires feature bits:

- 050 (Play messages)
- 053 (Keep messages)

058 Play Unplayed Messages in FIFO Order

Plays unplayed messages in first-in-first-out (FIFO) order so that earlier unplayed messages play first. Otherwise, unplayed messages play in last-infirst- out (LIFO) order.

Requires feature bit 050 (Play messages).

059 Play Unplayed Messages First

Plays new messages first. Otherwise, the server plays kept messages, then plays new messages.

Requires feature bits:

- 050 (Play messages)
- 053 (Keep messages)

060 Ignore DTMFs During Greeting

If the user enters a command while the mailbox greeting plays, the server will finish playing the greeting before processing the command. This effectively makes the greeting hard-play. In a Greeting-Only mailbox, if the FCOS also contains feature bit 066 (Login during greeting in greet-only mbx), the user must log in (press the * (star) key or 0) before entering a mailbox number or while the greeting is playing; otherwise, the server hangs up. The server does not prompt for the passcode until after the greeting plays.

Do not use this with feature bit 164 (Skip/pause during greeting in Greeting-only mailbox).

061 Wait to Record (Time-out = # Key)

Allows a user who presses M for make or G for give to either wait to start recording or press the # (pound) key to avoid the delay. This applies also to multiple make or give. For example, if the user wants to make or give a message to mailboxes 100, 101, and 102, the user can enter either this sequence, 100101102#, or enter a mailbox number and wait for the prompt to enter another mailbox number. After entering the last mailbox number, the user can wait to start recording or press the # (pound) key. If the user presses M to make a message but does not enter a mailbox number, the user hears a prompt to enter the mailbox number.

Use this when the users have phone calling cards because the # (pound) key signals some long distance providers to end the call and place another.

Requires either of these feature bits:

- 022 (Make to multiple destinations)
- 026 (Give to multiple destinations)

062 Hang Up Immediately After Greeting

The server plays the greeting, then immediately hangs up. No prompt plays before disconnect, and outside callers cannot record messages. Use this for Greeting-Only mailboxes, where no other interaction between the caller and the server is desired.

If the FCOS contains feature bit 066 (Login during greeting in greet-only mbx), the user must log in (press the * (star) key or 0) before entering a mailbox number or while the greeting plays; otherwise, the server hangs up. If the FCOS contains feature bits 060 (Ignore DTMFs during greeting) and 066 (Login during greeting in greet-only mbx), the server does not prompt for a passcode until the greeting plays.

Do not use this with these feature bits:

- 063 (Call mailbox attendant after greeting)
- 064 (Call mailbox user ext after greeting)
- 065 (Play system time after greeting)

063 Call Mailbox Attendant After Greeting

The server plays the mailbox greeting, then automatically transfers the call to the mailbox attendant's extension. The caller does not hear a prompt that the call is being transferred to the attendant. If no attendant's extension number is defined in the mailbox data file, the server transfers the call to the system attendant. If neither attendant is configured, the server tells the caller that no attendant is available, and the server hangs up.

The server does not supervise the transfer, so the caller may fail to reach the attendant and be disconnected.

If the FCOS contains feature bit 066 (Login during greeting in greet-only mbx) in a Greeting-Only mailbox, the user must log in (press the * (star) key or 0) before entering a mailbox number or while the greeting plays; otherwise, the server continues with the transfer.

Do not use this with these feature bits:

- 062 (Hang up immediately after greeting)
- 064 (Call mailbox user ext after greeting)

064 Call Mailbox User Ext After Greeting

The server plays the mailbox greeting, then automatically transfers the call to the mailbox extension. The server does not supervise the transfer, so the caller may fail to reach the extension and be disconnected. If no extension number is defined in the mailbox, the server tells the caller that the transfer failed, then hangs up.

If the FCOS contains feature bit 066 (Login during greeting in greet-only mbx) in a Greeting-Only mailbox, the user must log in (press the * (star) key or 0) before entering a mailbox number or while the greeting plays; otherwise, the server continues with the transfer

Do not use this with these feature bits:

- 062 (Hang up immediately after greeting)
- 063 (Call mailbox attendant after greeting)

065 Play System Time After Greeting

The server plays the greeting, then the system time. This feature bit is required with a TCOS.

066 Login During Greeting in Greet-only Mbx

Allows a user to press the * (star) key or 0 to log in to a Greeting-Only mailbox while the greeting plays. It also works in mailboxes that can receive messages. Otherwise, a user must press * and enter the mailbox number to log in.

067 Not Used

068 Define Rotational Mailbox

Allows the caller to hear the greeting of the called mailbox, then the greeting of a mailbox in distribution list 1 of the called mailbox. The server cycles through each of the mailboxes in the distribution list, either on a call-by-call basis or by time.

Any mailbox with this feature bit must also have distribution list 01, which controls cycling callers through up to 190 child mailboxes. For example, the mailbox 100 distribution list 01 has mailboxes 101, 102, and 103. On a call-by-call basis, the first caller hears the greetings for mailboxes 100 and 101. The second caller hears the greetings for mailboxes 100 and 102. The third caller hears the greetings for mailboxes 100 and 103. The fourth caller hears the greetings for mailboxes 100 and 101.

On a time basis, such as one hour, for the first hour callers hear the greetings for mailboxes 100 and 101; for the second hour, for mailboxes 100 and 102; for the third hour, for mailboxes 100 and 103; for the fourth hour, for mailboxes 100 and 101.

For details on rotational mailboxes, see FCOS 17: Rotational Mailboxes, in this chapter, or chapter 6.

Feature bit 041 (Receive messages from outside callers) overrides this and disables the mailbox's rotation.

069 Passcode Required for Mobile DID

Used with the DID NuPoint Voice application. If the Mobile DID option is configured for a DID group, users must always enter their passcodes when logging in. Otherwise, users who call in from their own mobile phones need no passcode, even if one is programmed into the mailbox.

070 User Options Menu (Master Feature Bit)

Allows the user to press U in the Main menu to reach the user options.

Required to use any combination of the User Options features. For a list of all feature bits that require 070, see Category 14, User Option feature bits.

071 Record or Change Mailbox Name

Allows the user to record and change the mailbox name.

The user logs in and presses U to reach the User Options menu, then N to record a name. The server announces this recorded name any time one user makes a message for, or gives a message to another user. NP Receptionist uses this for certain operations. The maximum recorded length of the name is controlled in the LCOS assigned to the mailbox. For details, see chapter 8.

Requires feature bit 070 (User Options Menu).

072 Record or Change Mailbox Greeting

Allows the user to record or change a personal mailbox greeting, which plays to outside callers who reach the mailbox. The user logs in and presses U to reach the User Options menu, then G to record the greeting. The maximum recorded length of the greeting is controlled in the LCOS assigned to the mailbox.

Requires feature bit 070 (User Options Menu).

073 Enter and Change Mailbox Passcode

Allows the user to set or change the mailbox passcode. The user logs in,presses U to reach the User Options menu, then presses P to change the passcode. Passcodes defined by users cannot appear on the console. Also, users cannot clear passcodes, or delete them entirely, unless the FCOS includes feature bit 125 (Clear user passcode).

Requires feature bit 070 (User Options Menu).

See also feature bit 093 (Deny change of passcode in first tutorial).

074 Create or Modify User Distribution List

Allows the user to create or modify a distribution list. A distribution list allows the user to make one message and send it to multiple mailboxes. An individual mailbox can store up to 99 lists, with a up to 65,535 recipient mailboxes per list. To create or modify a distribution list, the user presses U to reach the User Options menu, then presses L for lists.

Otherwise, only system administrators can create and change distribution lists from the console.

Requires feature bits:

- 032 (Make to user distribution list) and/or 033 (Give to user distribution list)
- 070 (User Options Menu)

Feature bits 032, 033, 070, and 074 alone do not allow all distribution lists to be modified; you must also allow change rights in the mailbox configuration.

Note: Tree mailboxes do not require either feature bit 032 or 033.

075 Audit Receipt Message

Allows the user to press A to audit (play) a message for which a receipt was requested. When users play a receipt, they may want to listen to the original message.

The Cut-through Paging optional feature does not require this feature bit.

Requires feature bit 050 (Play Messages).

076 Play Urgent Messages in FIFO Order

Plays urgent messages in first-in-first-out (FIFO) order so that earlier urgent messages play first. Otherwise, urgent messages play in last-in-first-out (LIFO) order.

Requires feature bits:

- 050 (Play messages)
- 088 (Receive urgent messages)

077 Change Pager Schedule

Allows the user to schedule the mailbox paging function if the mailbox

message waiting type is 5 (Pagers/Message Delivery). The user can

schedule when the server places a pager call to indicate unplayed messages

in the mailbox, such as for only during work hours, not during off hours.

Requires:

- Feature bit 070 (User Options Menu)
- Message waiting type 1 or 2 defined as 5 (Pagers/Message Delivery) in a mailbox
- A configured pager port

078 Activate User Tutorial

Allows users to activate the user tutorial. The user logs in, presses U to reach the User Options menu, then T for tutorial, which plays immediately. The tutorial is a series of instructions that guide users through setting passcodes, recording greetings, and recording their names. The system administrator can record a site tutorial, a greeting that plays after the NuPoint Voice tutorial, in the system attendant's mailbox. Otherwise, the tutorial plays only when a new user first logs in or when the administrator activates it from the console.

Use this feature bit for mailbox demonstrations.

If the FCOS does not include feature bit 073 (Enter and change mailbox passcode), the tutorial asks for a passcode only the first time it runs on a new mailbox. This feature bit also interacts with feature bit 093 (Deny change of passcode in first tutorial).

Requires feature bit 070 (User Options Menu).

079 Set Msg Wait #1 for Urgent Msgs Only

Activates the message waiting type 1 for urgent messages, only, and not for other unplayed messages.

Requires:

- Feature bits 040 (Receive messages from other users) and/or 041 (Receive messages from outside callers)
- Feature bit 088 (Receive urgent messages)
- Message waiting type 1 defined for the mailbox.

080 Set Msg Wait #2 for Urgent Msgs Only

Activates the message waiting type 2 for urgent messages, only, and not for other unplayed messages.

Requires:

- Feature bits 040 (Receive messages from other users) and/or 041 (Receive messages from outside callers)
- Feature bit 088 (Receive urgent messages)
- Message waiting type 2 defined in the mailbox

081 Only One Correct Passcode for Login

Requires a user who has entered an incorrect passcode to enter the correct passcode only one more time. Without this feature bit, the server requires a user to enter the passcode twice after an incorrect entry. As a security measure, the server tells a user that it did not get the user's passcode after the first of the two correct entries. (NuPoint Voice limits users to three tries.) Including this feature bit increases vulnerability to hackers and other unauthorized callers. This feature bit is included in FCOS 14 (MiCollab) by default.

082 Soft Play (Interrupt) Message Count

Allows the user to interrupt the "number-of-messages" prompt by pressing a command key, then immediately begin using the mailbox.

083 Soft Play (Interrupt) Most Prompts

Many NuPoint Voice Prompts are soft-play; that is, users can interrupt them by pressing a command key, but others are hard-play. This allows users to soft-play the Prompts listed in the following table..

Because callers reach the administrator's mailbox when they call the system directly, you can let callers use soft-play prompts by including this in the administrator's mailbox.

Table: Prompts that Soft-Play Only with Feature Bit 083	
Prompt	Application Used In
I'm sorry, but I don't understand what you pressed; plea se try again.	Paging, Message Delivery, NP WakeUp, NuPoint Voice
That is not a valid mailbox number; please try again.	NP Receptionist, NuPoint Voice, Hotel guest application
That is not a valid passcode; please try again.	Hotel guest application, NuPoint Voice
I'm sorry; I did not get your passcode. Please try again.	NuPoint Voice
Mailbox [number] has [x] unplayed messages, [y] urgent messages. OR Mailbox [number] has no messages.	Hotel guest application (guest mailbox reached from check-out mailbox)
I don't understand that command.	Hotel guest application, Main Menu, NuPoint Voice
Press P to enter your new passcode.	User Options
Enter 4 to [max. passcode length] digits for your passco de.	User Options
If you do not wish to have a passcode, enter 4 zeros.	User Options
I'm sorry; that is not a user option.	User Options
You cannot have a message for this mailbox. Please try again.	NuPoint Voice

084 Give Receipt Message with Comments

Requires the user to record additional comments when giving a message attached to a receipt.

Requires feature bits:

- 086 (Give receipt message)
- 040 (Receive messages from other users) in the recipient mailbox

Feature bit 075 (Audit receipt message) is recommended.

085 Give Receipt Message to Multiple Dests

Allows the user to give a message attached to a receipt to up to 200 destinations. If allowed, any of the destinations can be distribution lists, networked mailboxes, or off-system numbers.

Requires feature bits:

- 024 (Give messages)
- 086 (Give receipt message)
- 040 (Receive messages from other users) in the recipient mailbox

Feature bit 075 (Audit receipt message) is recommended.

086 Give Receipt Message (Master Feature Bit)

Allows users to re-send a message that originally had a receipt. When users play a receipt, they can press G to give the original message that was originally sent with a receipt. The receipt portion of the original message is not sent.

Feature bit 040 (Receive messages from other users) must be in the recipient mailbox.

087 Make and Mark Urgent

Allows the user to make a message and mark it urgent. The user presses M to make a message, then records a message. To mark the message urgent, the user presses M to reach the Message Addressing menu, then presses U for urgent. (To cancel urgent, the user presses U again.) To send the message, the user presses X until the server responds “message sent.” If you include feature bit 203 (Walk-away fax) in the FCOS, you must train the users and callers to press 8 twice to mark a fax urgent. The server plays urgent messages first only if the recipient’s FCOS includes

feature bit 088 (Receive urgent messages). Otherwise, the message plays with all other unplayed messages in the order received.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) in the recipient mailbox

088 Receive Urgent Messages

Plays an urgent message a separate queue of urgent messages before playing any other unplayed messages. Otherwise, any urgent message plays as a regular unplayed message with other unplayed messages in the order that the urgent message was received.

089 Auto-play All Messages (New and Saved)

The server automatically plays the next message, either played or unplayed, after the user keeps or discards the current message. If the FCOS does not include feature bit 054 (Auto-keep messages) ,the message stays in the unplayed queue if the user hangs up before keeping or discarding it.

With feature bit 215 (Don't auto-play first msg, w/auto-play), a mailbox does not automatically play the first message and the user can perform other functions in the mailbox. When the user presses P to play the first unplayed or saved message, all subsequent messages then play.

Do not use this with feature bit 227 (Undelete last message with * key).

Requires feature bits:

- 050 (Play messages)
- 053 (Keep Messages)

Overrides feature bit 052 (Auto-play unplayed messages). For more information, see Logout Interaction with Auto-Play.

090 Check In Other Mailboxes

Allows a desk clerk or TAS operator to record a name and assign a passcode to each guest mailbox. Although you only need one check-in mailbox per server, you can create one for each employee's telephone station.

A guest mailbox must have:

- Feature bit 008 (Mailbox can be checked in/out)
- The same GCOS as the check-in mailbox

091 Check Out Other Mailboxes

Allows a desk clerk or TAS operator to clear the name, greeting, passcode, and messages from each guest mailbox. Although you only need one checkout mailbox per server, you may want to create one for each employee's telephone station.

A guest mailbox must have:

- Feature bit 008 (Mailbox can be checked in/out)
- The same GCOS as the check-out mailbox

092 User will be in Dial-by-Name Database

Includes the mailbox owner's name in the two Dial-by-Name databases. The databases are identical but their format is different, with one listing users by last name and the other by first name. The server searches these databases for entries to match a caller's input. For example, if a caller is prompted to dial by last name, when the caller begins typing letters the system will search through the database that lists users by last name. If the caller is prompted to dial by first name, the system will search through the database that lists users by first name.

In addition, modify this information:

- Set one digit in the dialing plan to A or the optional star prefix; if you do not set the dialing plan, you can create a phonebook, but cannot use Dial-by-Name
- Set the line group parameters (Last Name First flag, Exact Match Break, Number of Names Threshold)
- Include the name of the mailbox owner when defining the mailbox, such as “Smith Jim”

Note: Do not use punctuation characters such as “-” or “,”.

093 Deny Change of Passcode in First Tutorial

Prevents the mailbox owner from changing the passcode during the first time through the tutorial. Include feature bit 078 (Activate user tutorial) and exclude 073 (Enter and change mailbox passcode), to disable the Prompt for a new passcode in the tutorial.

The server still Prompts the mailbox owner for the passcode when logging in.

Note: This feature bit only works with NuPoint UM Standalone deployments. It is inoperable with NuPoint UM on MiCollab .

094 Change Message Delivery Options

Allows the user to schedule the message delivery function if the mailbox message waiting type is 5 (Pagers/Message Delivery). The user can schedule when the server places a message delivery call to indicate unplayed messages in the mailbox, such as for only during work hours, and not during off hours.

Requires:

- Feature bit 070 (User Options Menu)
- Message waiting type 1 or 2 defined as 5 (pager) in the mailbox
- Message delivery set to Yes in the mailbox configuration
- A configured pager port

095 Mark Message for Future Delivery

Allows the user to make a message for another mailbox, mark it for future delivery, and audit future delivery messages. Future delivery dates can be up to one year from when the message is marked. The auditing function allows the mailbox owner to listen to messages sent, but not yet delivered. The key sequence is U for User Options, C for Call Schedule Options, then F for Future Delivery Audit.

The user presses M and records a message. To mark the message for future delivery, the user presses M to reach the Message Addressing menu, then presses F for future delivery. The user hears Prompts for month of delivery (1 through 12), then day (1 through 31), time, and a.m. or p.m. (A or P). To cancel future delivery during the date and time input, press the * (star) key. To cancel future delivery after entering the date and time, press the F key at any time before exiting the Message-Addressing menu. To send the message, the user presses X until the server announces that the message has been sent.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) in the recipient mailbox
- 070 (User Options Menu) to allow Audit Future Delivery

Note: In addition, set the LCOS parameter “Max days - future delivery” for the absolute number of days for future delivery.

096 Make Messages Before Keep/Discard

Allows a user to make a new message while another message plays or after it has played without first keeping or discarding that message. Otherwise, the user (while playing a message) must first keep or discard the message before pressing M to make a new message.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) in the recipient mailbox

097 Do Not Say "I will ring <name>" in AR

Used with NP Receptionist optional feature software. When a caller enters an extension, NP Receptionist says only, “Please hold.” If call screening is included, NP Receptionist asks the caller’s name. Otherwise, NP Receptionist asks the caller to hold and says, “I will ring [recipient’s name].”

098 Say "Press 0" to Caller Before Beep

The caller hears this prompt, “You may start your message now. Press 0 (zero) to return to the attendant” and a beep. If the caller presses 0, the server transfers the call to the system attendant’s extension, or if that number is not configured, to the system attendant’s mailbox. If neither is configured, the “Press zero. . .” portion of the prompt does not play.

NP Receptionist Usage -- With NP Receptionist, this feature bit works the same way unless you include feature bit 003 (Return to Welcome prompt), which plays the Receptionist greeting after the caller presses 0.

99 Speech Navigation

Allows users to manage their messages and reach the operator by with spoken commands. The Speech Navigation license defines the total number of users that may use the feature. The licenses are automatically assigned to low-numbered mailboxes first, so if you have purchased three licenses and your system has three mailboxes, 1234, 1235, 1236, then only 1234 and 1235 will be licensed to use Speech Navigation. You can, however, manually reassign a user license by disabling Speech Navigation on one mailbox and enabling it on another.

099 NP Talk with Talkover

This feature is used with OneTalk optional feature software, which allows for commands through voice. This feature bit gives the user the ability to speak voice commands while the server is playing a prompt or message.

Notes:

- At the beginning of a call, the server does a calibration of the line. If it is too noisy, then Talkover will not be allowed even if bit 099 is set.
- Do not include this bit in the same FCOS with bit 100.

26.27.2 Feature Bits 100 to 149

100 Disable Talkover

This feature is used with OneTalk optional feature software, which allows for commands through voice. This feature bit disables the Talkover feature. As a result, the user cannot give spoken commands while the server is playing prompts or messages.

Note:
Do not include this bit in the same FCOS with bit 099 unless you want to disable Talkover.

101 - 109 Deny Login on Line Group <1 - 9>

Allows the system administrator to deny users access to mailboxes through certain line groups. The line group number is the feature bit number minus 100: 101 = line group 1, 109 = line group 9, and so on.

For example, if line group 7 consists of “800” numbers meant only for customers’ messages, add feature bit 107 to all mailbox FCOS to prevent mailbox owners (employees) from calling on these lines to log in to their mailboxes.

110 Make/Give to Telephone Number

Allows a mailbox owner to make or give a message to a telephone number outside the mailbox system; known as “call placement.” To use this, the mailbox owner specifies the number by dialing the call placement digit (set in the dialing plan) and then the telephone number, instead of specifying a mailbox while making or giving a message.

The server Prompts the mailbox owner to record the name of the recipient. Modify these parameters:

- Set the dialing plan digit for call placement messaging to T or the optional star prefix.
- Set LCOS definitions for call placement in the More Limits Parameters menu.
- Set the Call Placement Access Index Code, also known as a predial string, in the user’s mailbox. The server inserts these digits before the call placement number when dialing out on the pager port.
- Configure an outdial (pager) port.

Requires feature bits:

- 020 (Make messages)
- 024 (Give messages)
- 040 (Receive messages from other users).

111 - 119 Deny Message Receipt on Line Group <1 - 9>

Allows the system administrator to deny callers access to mailboxes through certain line groups. The line group number is the feature number minus 110: 111 = line group 1, 119 = line group 9, and so on.

For example, if line group 7 consists of “800” numbers meant only for a company’s sales or service force to retrieve messages, adding FCOS feature bit 117 to all FCOS prevents customers from calling in on these lines to leave messages.

As another example, if company A (using line group 1) and company B (using line group 2) share a PBX, company B’s system administrator can assign feature bit 111 (Deny message receipt from line group 1) to every FCOS to ensure that callers do not use company A’s lines to reach company B’s mailboxes.

120 Default to First Child of Tree Mailbox

Applies to tree mailboxes. When a time out occurs, causes the server to default to the first mailbox in distribution list 01. For details about tree mailboxes, see FCOS 15 (Tree), chapter 6, and feature bit 121 (Define tree mailbox).

With this, the server routes callers who do not enter a digit promptly after the tree mailbox greeting to the first child mailbox in the tree mailbox distribution list. Otherwise, the server routes those callers to the attendant’s mailbox. Use this feature for calls from rotary telephones.

Requires feature bit 121 (Define tree mailbox).

Overridden by feature bit 186 (Default to last child of tree mailbox).

121 Define Tree Mailbox (Master Feature Bit)

The tree mailbox routes callers to “child” mailboxes or “members” of the tree mailbox distribution list 01. When a caller reaches this mailbox, the greeting plays, then the server waits for DTMF input to route the call to the next mailbox.

For details about tree mailboxes, see FCOS 15 (Tree) and Tree Mailbox.

Requires feature bits:

- 070 (User Options Menu)
- 072 (Record or change mailbox greeting)

Feature bit 041 (Receive messages from outside callers) overrides this and disables the mailbox��s tree function.

Tree Mailboxes and NP Receptionist -- If the administrator’s mailbox is a tree, callers can press the # key to exit from the tree structure any time during the greeting. NP Receptionist then prompts the caller to enter an extension number and transfers the call to that number. If the administrator’s mailbox is not a tree, and if, for example, a caller presses the # key, reaches the administrator’s mailbox, and enters mailbox number 3530, the call will transfer to extension 3530. If that number does not answer and the caller presses 3531 during the mailbox greeting, the call will transfer to 3531, and so forth. This feature is also called “pound (#) dial around.” It does not work if the caller dials a DID number and forwards to a NuPoint Voice line group. The call must either originate from a line group programmed to use NP Receptionist, or the call must be call forwarded to such a line group.

The server does not announce the “pound (#) dial around” feature; the user’s greeting must refer to the option.

Do not use this with feature bit 187 (Receptionist call-transfer tree mailbox).

122 Define Broadcast Mailbox (Master Feature Bit)

When a message is made for a mailbox with this, it is deposited in the mailboxes of all members of distribution list 01. When the recipients play the message, the server announces the name that is recorded in the sender's mailbox (or the sender's mailbox number if no name is recorded). If feature bit 123 (Announce broadcast mailbox name) is in the FCOS, the server announces the broadcast mailbox name. Do not use with feature bit 291 (Enable Record A Call).

- Overrides feature bit 134 (Broadcast message waiting status).
- Requires feature bit 040 (Receive messages from other users) and/or044 (Receive user dist list messages)

123 Announce Broadcast Mailbox Name

Used with broadcast mailboxes. The server announces the name that is recorded in the broadcast mailbox. Otherwise, the server announces the sender's name (or the sender's mailbox number if no name is recorded).

Requires feature bits:

- 040 (Receive messages from other users) and/or 044 (Receive user dist list messages)
- 070 (User Options Menu)
- 071 (Record or change mailbox name)
- 122 (Define broadcast mailbox)

124 Change Paging Phone Number

Allows the mailbox owner to use a pushbutton telephone to change the paging telephone number. This does not affect the post-pager dial string, which is programmed in the mailbox.

Requires:

- Feature bit 070 (User Options Menu)
- Message waiting type 1 or 2 defined as 5 (pager) in the mailbox
- A configured pager port

Note:

- Do not confuse this feature bit with feature bit 143 (Change message delivery phone number).
- This feature bit only works with NuPoint UM Standalone deployments. It is inoperable with NuPoint UM on MiCollab.

125 Clear User Passcode

Allows users to eliminate their passcodes if they do not want to enter a passcode when they log in. Otherwise, users can change the passcodes, but not remove it. For security reasons, be careful when you use this feature bit. The user logs in, presses U to reach the User Options Menu, then presses P to change the passcode. The user enters four zeros, 0000, at the prompt to clear the passcode. This also applies during the tutorial.

Requires feature bits:

- 070 (User Options Menu)
- 073 (Enter and change mailbox passcode)

126 Make/Give to Mailbox with Empty GCOS

Allows one-way communication to a mailbox that has a GCOS with no groups entered or has GCOS 2 (Self). The recipient mailbox cannot answer the message, even if the FCOS contains feature bit 029 (Answer messages). Service bureau operators or hotel staff mailboxes can use this to send messages to customers.

Requires feature bits:

- 020 (Make messages)
- 040 (Receive messages from other users) in the recipient mailbox

127 Deny Receipt of Messages Before Tutorial Run

Prevents a mailbox from receiving messages before the mailbox owner plays the tutorial and sets up the mailbox.

Requires feature bits:

- 040 (Receive messages from other users) and/or 041 (Receive messages from outside callers)
- 070 (User Options Menu)

128 Family Head

129 Host Mailbox

130 Passcode Cannot be Same as Mailbox

Prohibits a user from assigning a passcode that is the same as the mailbox number. This security feature helps prevent hackers from breaking in to the system.

Requires feature bits:

- 070 (User Options Menu)
- 073 (Enter and change mailbox passcode)

Note:
This feature bit only works with NuPoint UM Standalone deployments. It is inoperable with NuPoint UM on MiCollab .

131 Don't Say Limits of Liability Statement

This feature bit is only used with VMUIF, a custom user interface, and with ISO UI, a user interface based on ISO/IEC International Standard 13714.

132 Bad Passcode Lockout if Over Limit

Each mailbox tracks bad passcode attempts within a specified time limit. If the count reaches the limit, the mailbox owner hears “I’m sorry. You cannot reach your mailbox at this time. Good-bye.” The system administrator must clear the mailbox either at the console or by phone.

Otherwise, the mailbox owner hears, “Warning! There have been excessive bad passcodes entered for your mailbox.” The bad passcode count is automatically cleared after the time limit. You can modify the time limit and bad passcode attempts in the NuPoint Voice application.

133 Don't say: "You may start your msg now"

Before an outside caller leaves a message, the server prompts the caller to start the message. This feature bit omits that prompt. Use this when line usage time is an issue, or if callers know what to do at the beep.

Requires feature bits:

- 004 (Outside caller functions)
- 041 (Receive messages from outside callers)

134 Broadcast Message Waiting Status

Sets the server to broadcast the message waiting, rather than the message itself, to distribution list 01.

Requires feature bits:

- 040 (Receive messages from other users) and/or 044 (Receive user dist list messages)
- 070 (User Options Menu)
- 074 (Create or modify user distribution list)

Feature bit 122 (Define broadcast mailbox) overrides this.

135 Define Template Mailbox (NP Forms)

Used with the NP Forms optional feature. The mailbox plays the greetings stored in its child mailboxes, sequentially, and records a message after each greeting.

136 Don't say: "End of message"

Omits the “End of Message” prompt that occurs after a message plays. Use this when line usage time is an issue.

Requires feature bit 050 (Play messages).

137 Caller Must Enter Access Code

Requires that callers enter a valid access code (“authorization code” in NP Receptionist) before they can leave messages. Codes can include up to ten digits, any of the numeric keys on a pushbutton phone. A mailbox owner can require that callers enter a specific mailbox number plus the passcode in order to leave a message.

The mailbox owner or system administrator creates this access code when setting up the mailbox.

See also feature bit 160 (Caller must enter line group access code), which requires an access code before playing the greeting.

138 Don't say: "Message complete"

Omits the “Message complete” prompt after recording of a message. Use this when line usage time is an issue.

Requires feature bit 020 (Make messages).

139 Template: Assume Last Greet Box FCOS

Used with the NP Forms optional feature. For more information, see the NP Forms guide.

Requires feature bit 135 (Define template mailbox).

140 Say Full Date When Playing Messages

Announces the full date (time, day, date, month, and year) before playing all messages. Otherwise, when a mailbox user plays a message, the delivery date is shortened as much as possible. If the message was delivered the same day, only the time plays; if it came the same week, only the day of week plays; and so on.

Requires feature bit 050 (Play messages).

Do not include feature bits 048 (No auto-time stamp of unplayed msgs) or 049 (No auto-time stamp of played msgs) in the FCOS.

Note:
Using this feature bit can significantly increase how long users are connected to the server, increasing line usage time.

141 Define Chain Mailbox in NP Receptionist

Works with NP Receptionist Chain mailboxes route calls to an extension even if the chain mailbox has no greeting. In addition, NP Receptionist can route a call from a chain mailbox to an extension that the caller enters.

142 Must Run Tutorial from Own Phone (SMDI)

Used for Centrex and Unified integrations. Requires that the user play the tutorial from the telephone assigned to the mailbox, rather than any telephone. Use this where users are assigned default passcodes because it prevents “stealing” mailbox access by dialing in and changing the passcode.

Requires feature bits:

- 070 (User Options Menu)
- 073 (Enter and change mailbox passcode)
- 093 (Deny change of passcode in first tutorial)

143 Change Message Delivery Phone Number

Allows the mailbox owner to use a pushbutton phone to change the message delivery telephone number. Mailbox owners can use this when they expect a call and are at a different telephone number than the message delivery number currently programmed in the mailbox.

This feature bit requires:

- Feature bit 070 (User Options Menu)
- Feature bit 094 (Change Message Delivery Options)
- Message-waiting type 1 or 2 defined as 5 (pager) in the mailbox
- A configured pager port

144 Skip Forward to Next Message

Allows a user to skip forward from the current message to the “top” of the next message by pressing the T key without first keeping, giving, or discarding. When a user skips a message, the server treats the message as unplayed. The next time the user logs in, the server includes skipped messages in the count of unplayed messages.

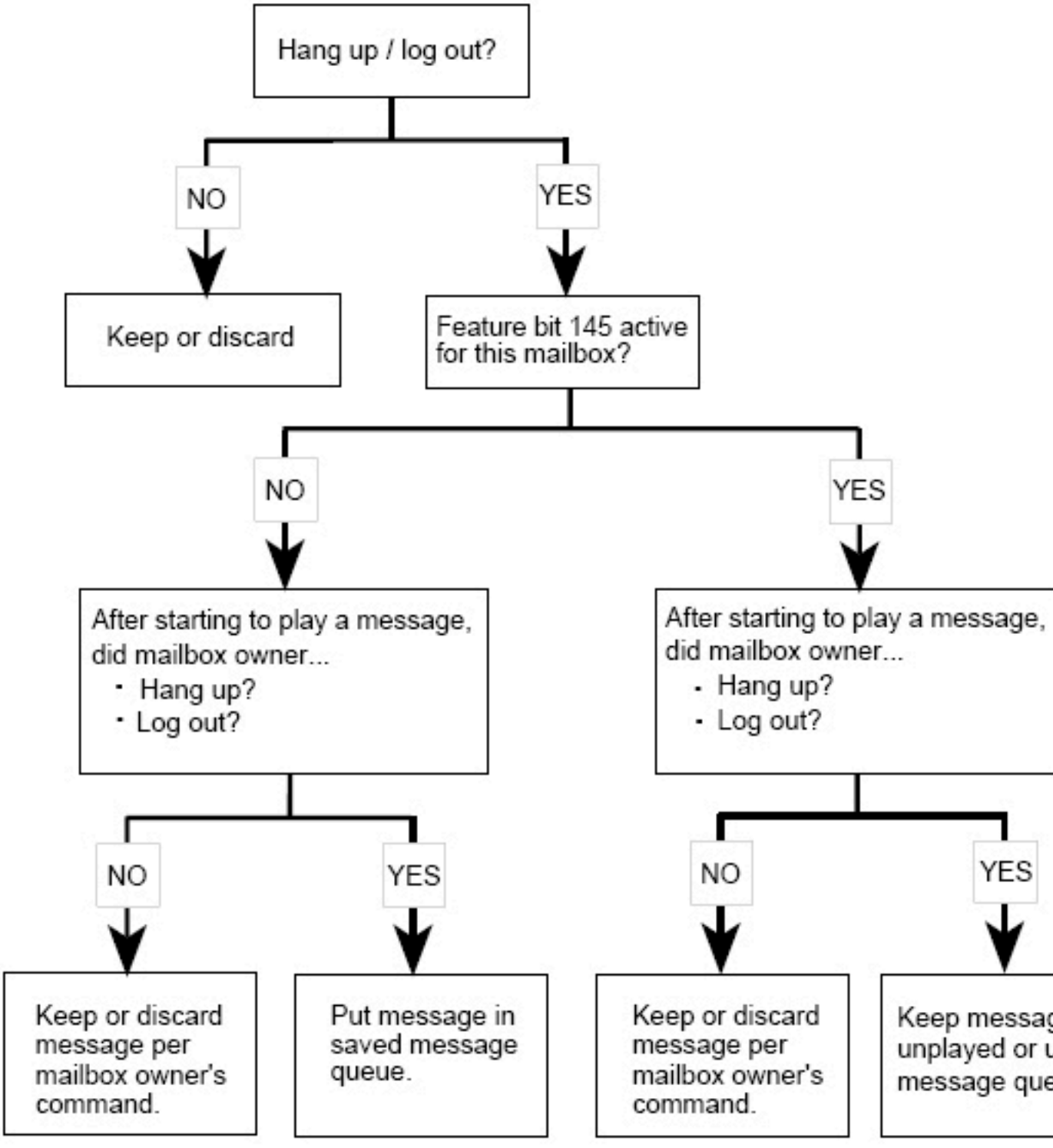
This feature bit:

- is overridden by feature bit 204 (Message Skip, Forward and Backward).
- conflicts with feature bits 048 (No Auto-timestamp of Unplayed msgs) and 049 (No Auto-timestamp of Played Msgs).

145 Message Stays in Original Queue on Hangup

Determines how the server classifies a message if a mailbox owner does not either press K to keep it or press D to discard it. The message stays in the original (unplayed or urgent) queue if the mailbox owner hangs up or logs out after starting to play it. See below:

Decision Process for Unplayed Messages



Otherwise, a message moves to the saved queue when the mailbox owner hangs up or logs out while playing it.

If a mailbox owner has feature bit 089 (Auto-play all msgs, new and saved) but not feature bit 054 (Auto-keep messages), and hangs up before keeping or discarding a message, it always stays the unplayed queue.

Feature bit 144 (Skip Forward to Next Message) overrides this feature bit. If a mailbox owner has feature bit 144 and uses it to skip forward to a new message, then hangs up before keeping or discarding the message, both messages (skipped and played) will stay in the unplayed queue. This occurs even if feature bit 145 is disabled.

See also feature bit 147 (Send receipt after full play) for information on how 145 and 147 interact.

146 Don't say: "NuPoint Voice storage is full"

Suppresses a warning that the system issues if the voice storage is 80% full, encouraging mailbox owners to delete unneeded messages. The warning is sent in two formats:

- An audible prompt played when the user logs in to his or her mailbox.
- An email message sent to the user's Standard or Advanced UM address (programmed in the mailbox parameters).

Use this when the site policy does not allow mailbox owners to receive audible or email system warnings.

147 Send Receipt After Full Play

Sends a receipt for a message after a user plays the entire message, even if the user does not press K to keep it or D to discard it. If the FCOS includes feature bit 145 (Message stays in original queue), the message stays in the unplayed queue; without 145, it moves to the saved queue.

If the user skips past the message, hangs up, or logs out before it finishes playing, and the FCOS includes feature bit 145, the server does not send the receipt and the message stays in the unplayed queue.

If the user skips past the message, hangs up, or logs out before it finishes playing, and the FCOS does not include feature bit 145, the server sends the receipt and the message moves to the saved queue.

148 Change NP Wakeup Phone Number

Allows a user to use a pushbutton telephone to change the phone number for NP WakeUp. An LCOS, "NP WakeUp--Phone Length", sets the length of the phone number.

Requires:

- Feature bit 015 (Change wakeup options)|
- Feature bit 070 (User Options Menu)
- NP WakeUp optional feature
- A configured outdial or pager port

149 Login to Template Thru Rotational Mailbox

Used with the NP Forms optional feature.

Requires feature bit 135 (Define template mailbox, NP Forms).

26.27.3 Feature Bits 150 to 199

150 (ISO) Simple Message Delivery

This feature bit is only used with ISO UI, a user interface based on ISO/IEC International Standard 13714. When this bit is on, the receiver gets a future delivery message without an option menu. When this bit is off, the receiver gets a future delivery message with an option menu.

151 Deny 333 Access for Mobile DID

Used only with the DID NuPoint Voice application. Requires mailbox owners to log into their mailboxes only from the mobile phone, not from a “land line.”

The “333” refers to an internal code for land line access. Configure the DID line group for the Mobile DID option.

152 Deny Login Within Tree

Prohibits callers from logging in from a tree mailbox or any of its child mailboxes. Use this to restrict mailboxes to information retrieval only.

Requires feature bit 121 (Define tree mailbox).

153 Don't Jump to New Message from Saved Queue

Allows the user to continue playing saved messages after a new message arrives, without losing place. After the Prompt for the new message, the user can either play all saved messages, then hear the new message, or, if the FCOS includes feature bit 204 (Message skip, forward and backward), skip forward or backward to the new message.

Otherwise, the server immediately plays any new message that arrives while a user is playing saved messages.

Requires feature bits:

- 039 (Notification tone when new msg arrives) or 047 (Notification prompt when new msg arrives)
- 050 (Play messages)
- 053 (Keep messages)

154 Announce Text (Email) Message Count

Plays the Prompts that announce text messages, such as email, messages, or faxes at a hotel front desk.

Feature bit 217 (Announce text msgs without count) overrides this.

155 Payphone User/Recipient Interface

This feature bit is reserved for future use.

156 Deny Login After Greeting

Allows a mailbox owner to log in only before or while the greeting plays, not afterward.

157 Repeat Message for Answering Machine

Used with call placement. If the called party does not press a key, the message plays twice to allow an answering machine to receive the message. Otherwise, the message does not play because the server waits for DTMF input and a timeout.

Requires:

- Feature bit 110 (Make/give to telephone number)
- A mailbox configured for call placement
- Outdial (paging) port

158 Continue Sending Message (* Key)

Allows the mailbox owner to press the * (star) key to continue giving, sending, or answering a message. After making, giving, or answering a message, the mailbox owner hears a Prompt to press the * (star) key to add an additional mailbox. If the FCOS includes feature bits 022 (Make to multiple destinations) and 026 (Give to multiple destinations) the mailbox owner can enter more than one mailbox number.

Also allows a user to send the most recently made message to additional mailboxes, unless the user skips to the next message.

Requires at least one of these feature bits:

- 020 (Make messages)
- 024 (Give messages)
- 029 (Answer messages)

159 Say "Press 0 to return to NP Receptionist"

Plays a Prompt, “Press zero to return to automated receptionist,” after the caller leaves a message, then presses the # (pound) key to return to the Receptionist menu.

Requires the NP Receptionist optional feature.

160 Caller Must Enter Line Group Access Code

Requires an outside caller to enter an access code to continue. Otherwise, the server hangs up.

Use this for the administrator’s mailbox, for a line group that has 800 (toll free) service, or for a modem. This function is required by law in some countries.

See also feature bit 137 (Caller must enter access code), which requires callers to enter an access code to leave a message in the mailbox.

161 Conditional Greetings

Allows the mailbox owner to use separate, personal or system greetings for each forwarding condition: Busy, Forward, or Ring No Answer.

Requires:

- Feature bit 070 (User Options Menu)
- Call forwarding information from the PBX

162 General Greetings

Allows the mailbox owner to choose the general system greetings for all call types. The system greeting is the default greeting used when a user has not recorded a personal greeting. When used with feature bit 161, allows four general greetings: Primary, Busy, Call Forward, and Ring No Answer.

Requires feature bit 070 (User Options Menu).

163 Don't Play Message Count

Suppresses the message count prompt (“You have no messages in your mailbox”) to allow callers to enter DTMF digits rather than voice messages. To use this function, create a new FCOS based on FCOS 10. Delete feature bits 4, 20, and 41; add feature bits 133, 138, 163, 171, and 213.

Used with the Cut-Through Paging optional feature. Do not use this for mailboxes that receive messages.

164 Skip/Pause During Greeting in Greeting-only Mailbox

Allows a caller to press the # (pound) key to skip forward (fast forward), press the * (star) key to skip backward (rewind), press 1 to pause, or press 7 to restart while listening to a greeting. This is similar to skipping and pausing when playing messages (see feature bits 006 and 007). Use this for long greetings so callers can verify the information without having to call the mailbox again.

To log in to this mailbox, you must use the * (star) key and mailbox number sequence, not the mailbox number and * (star) key sequence.

Requires:

- Feature bit 062 (Hang up immediately after greeting)
- Greeting-Only mailbox.

Dial-by-Name overrides this because it hard-plays the mailbox greeting.

Overrides feature bit 060 (Ignore DTMFs during greeting).

165 Pound Key (#) Login

Allows a user to log in by dialing in from any server port, pressing the # (pound) key, and entering the mailbox number.

Overrides Dial an Extension and Email.

166 AMIS Analog Networking

Used with the AMIS Analog Networking optional feature. For details, see the AMIS Analog Guide.

167 (ISO) SMS Short Text Option Enabled

This feature bit enables a short text message option in the ISO SMS main menu. If this bit is on, bit 12 must also be on.

Related bits: 12, 214, 269, 278 and 284.

168 Message Wait 1, Pager Requeue

If a message arrives during a time period when paging is not scheduled, queues the server to page at the start of the next scheduled paging period for schedule one (Message Waiting type 1). Otherwise, the server does not page unless a message arrives during the scheduled paging period.

Applies to both paging and message delivery.

169 Message Wait 2, Pager Requeue

If a message arrives during a time period when paging is not scheduled, queues the server to page at the start of the next scheduled paging period for schedule two (Message Waiting type 2). Otherwise, the server does not page unless a message arrives during the scheduled paging period.

Applies to both paging and message delivery.

170 Transfer to Email System

Prompts an outside caller to transfer into the Email system. Do not include this feature bit unless your system is part of an Email system.

Requires feature bits:

- 040 (Outside caller functions)
- 005 (Play Outside Caller Menu prompts)
- 176 (Say “Press pound [#] for more options” to callers)

171 Cut-through Paging

Activates either of two types of Cut-through Paging for the mailbox. A Caller can leave either a telephone number or a message, but not both. You can use this with feature bit 173 (Receive cut-through page notify receipt).

Requires:

- Feature bit 070 (User Options Menu)
- Cut-though Paging optional feature
- Message waiting type 5 defined in the mailbox

172 Cut-through Paging and Messaging

Activates either of two types of Cut-through Paging for the mailbox. A Caller can leave either a telephone number, a message, or both. You can use this with feature bit 173.

If the FCOS includes feature bit 004 (Outside caller functions), the caller must press i, the feature activation key, to activate Cut-through Paging. Otherwise, the caller can enter the telephone number without pressing i.

If the FCOS does not include feature bit 005 (Play Outside Caller Menu prompts), the caller does not hear the function prompts. Feature bit 005 requires feature bit 004.

Requires:

- Feature bit 070 (User Options Menu)
- Cut-though Paging optional feature
- Message waiting type 5 defined in the mailbox

173 Receive Cut-through page Notify Receipt

Works with the Cut-through Paging optional feature to generate receipts for all paging attempts. You can use this with feature bit 171 or 172.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 075 (Audit receipt message)
- Feature bit 171 (Cut-through Paging) or 172 (Cut-though Paging and messaging)
- Cut-through Paging optional feature
- Message waiting type 5 defined in the mailbox

174 Define Broadcast Greeting Mailbox

Allows a mailbox to send recorded greetings to a list of other mailboxes, like a broadcast mailbox sends messages it receives to other mailboxes. Use distribution list 09 for the broadcast greeting mailbox list.

Requires these feature bits in mailboxes that receive the broadcast greeting:

- 161 (Conditional greetings) for multiple mailbox greetings
- 162 (General greetings) for multiple mailbox greetings
- 175 (Receive broadcast greeting)

A broadcast greeting mailbox can also be a tree mailbox or a broadcast message mailbox. Use distribution list 01 for the tree or message broadcast feature. Use distribution list 09 for the greeting broadcast.

Can be used with feature bit 178 (Define broadcast name mailbox). Both use the same distribution list 09.

175 Receive Broadcast Greeting

Allows a mailbox to receive the greeting from a broadcast greeting mailbox. For information on the broadcast greeting mailbox, see feature bit 174 (Define broadcast greeting mailbox).

Requires feature bits to change multiple mailbox greetings:

- 161 (Conditional greetings)
- 162 (General greetings)

176 Say: "Press pound [#] for more options" to Callers

Plays Prompts for outside callers if more options, such as Dial an Extension or transferring to Email. The user hears, “Press the pound [#] key for more options.” If the user presses the # (pound) key, the server then plays, “Press 1 to dial an extension, 2 to transfer to Email,” if both optional features are available. If only one option is installed, pressing the # (pound) key initiates that option.

Requires feature bits:

- 004 (Outside caller functions)
- 005 (Play Outside Caller Menu prompts)
- 170 (Transfer to Email System) for the prompt to include Email.

177 (ISO) Reminder Calls

This feature bit is only used with ISO UI, a user interface based on ISO/IEC International Standard 13714. This feature bit allows mailbox users to create reminder calls.

178 Define Broadcast Name Mailbox

Broadcasts all recorded names that are created or modified to a list of mailboxes, like a broadcast mailbox sends a message to other mailboxes. Use distribution list 09 for the broadcast name mailbox list.

Mailboxes that receive the broadcast name must include feature bit 179 (Receive broadcast name).

- A broadcast name mailbox can also be a tree mailbox or a broadcast message mailbox. Use distribution list 01 for the tree or broadcast message feature. Use distribution list 09 to broadcast the name.

Can be used with feature bit 174 (Define broadcast greeting mailbox). Both use the same distribution list 09.

179 Receive Broadcast Name

Allows a mailbox to receive a recorded name from a broadcast name mailbox. For information on the broadcast name mailbox, see feature bit 178 (Define broadcast name mailbox).

180 Record Personal Wakeup Message

This feature bit is used with VMUIF, a custom interface. It allows the mailbox owner to record a personal message for the next wakeup call, which is used instead of the normal wakeup message. This feature bit requires the Auto Wakeup optional feature.

181 Paging over msgdel, mwi 1 over mwi 2

Sets the selection order for pagers:

- If either message waiting type 1 or message waiting type 2 is a pager, selects the pager instead of message delivery
- If both types are for pagers, selects message waiting type 1

Use this when paging schedules overlap.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 077 (Change pager schedule)
- Message waiting type 1 or 2 defined as 5 (pager) in the mailbox
- A configured pager port

182 Use pri/alt as Week/Weekend for mwi 1

Changes the operation of the primary and alternate message waiting type 1 (MWI 1). Uses primary message waiting type 1 for weekday messages and uses the alternate for weekend messages. Use this for paging or message delivery if the telephone numbers differ for weekday and weekend. The server assumes that weekends are Saturday and Sunday, independent of the day/night configuration.

Otherwise, the server tries the primary message waiting type until all tries are exhausted, and tries the alternate.

Requires that message waiting type 1 be configured for the mailbox.

183 Use pri/alt as Week/Weekend for mwi 2

Changes the operation of the primary and alternate message waiting type 2 (MWI 2). Uses primary message waiting type 2 for weekday messages and uses the alternate for weekend messages. Use this for paging or message delivery if the telephone numbers differ for weekday and weekend. The server assumes that weekends are Saturday and Sunday, independent of the day/night configuration.

Otherwise, the server tries the primary message waiting type until all tries are exhausted, and tries the alternate.

Requires that message waiting type 2 be configured for the mailbox.

184 Append Mailbox Number to Transfer

Used when transferring to another system, such as Email, from the NuPoint Unified Messaging server. Allows NuPoint Voice to append the mailbox number to the end of the Email transfer string to inform the other system of the mailbox number when transferring the call transfer. Configure the transfer number in the online option for an Email string.

185 Receive Wakeup Call Notification Receipt

Use this in the hotel/motel environment to give users a receipt for any wakeup calls that were not delivered because of a Busy or Ring No Answer.

Requires:

- Feature bit 070 (User Options Menu)

- Feature bit 015 (Change Wakeup Options)
- NP WakeUp optional feature

186 Default to Last Child of Tree Mailbox

When a time out occurs, causes the server to default to the last mailbox in distribution list 01.

Requires feature bit 121 (Define Tree Mailbox).

Overrides feature bit 120 (Default to First Child of Tree Mailbox).

187 NP Receptionist Call-transfer Tree Mailbox

Used with the NP Receptionist optional feature. Allows a call to be transferred to the first child mailbox on a Ring No-Answer, and to the second child mailbox on a Busy. Record greetings for the tree mailbox and its child mailboxes. Use this to track statistics for extensions in high traffic conditions.

Do not use with feature bit 121 (Define tree mailbox).

188 Append # to End of Cut-thru Page Number

Used with the cut-through paging optional feature. Allows a caller to enter a number, then press the # (pound) key to indicate that the number is complete. Otherwise, the server waits for the time out set in the LCOS before sending the page.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 171 (Cut-through Paging) or 172 (Cut-though Paging and messaging)
- Cut-through Paging optional feature
- Message waiting type 5 set up in the mailbox

189 Rotate on Full Mailbox

Allows a caller to leave a message even if the original mailbox is full by routing the message to the first available mailbox in distribution list 01 of the full mailbox. When logging in to the primary mailbox, the mailbox owner hears “Your overflow mailbox has messages.” The mailbox owner must log into the child mailbox(es) to retrieve overflow messages.

Otherwise, when a mailbox reaches the maximum number of messages allowed by its LCOS, the caller hears “I’m sorry, mailbox for [mailbox owner] is full” and the caller cannot leave a message.

Use this to override the server limit for maximum messages per mailbox. For example, to set a limit of 250 messages for a mailbox owner, set the limits to 200 (the maximum) for the parent mailbox and to 50 for the child mailbox.

190 Receive Fax Messages

Allows a mailbox to receive fax messages with voice comments. Callers hear a Prompt to leave a voice message and to press L to leave a fax with the voice message. A caller can ignore the voice message prompt and press L to only leave a fax.

Requires:

- Feature bits 040 (Receive Messages from Other Users) or 041 (Receive Messages from Outside Callers)
- NuPoint Fax optional feature

191 Make Fax Messages

Allows a mailbox owner to press L to make a fax message. The fax message can include voice comments; both are delivered to the recipient.

Requires:

- Feature bit 020 (Make messages)
- NuPoint Fax optional feature

192 Give Fax Messages

Allows a mailbox owner to forward a received fax, with voice comments, to another user or an outside line. Another fax is not considered a comment.

Requires:

- Feature bit 024 (Give Messages)
- Feature bit 190 (Receive Fax Messages)
- NuPoint Fax optional feature

193 Deliver Fax to Default Number

Allows a user to listen to the voice comments, then deliver the fax to a personal (default) fax telephone number. The system administrator can set this to a specific fax machine during configuration. In the mailbox, the user can set the default fax number by pressing U (User Options), F (Fax), then D (Default Fax Number), and enter the number. This requires feature bit 070 (User Options Menu).

Requires:

- Feature bit 190 (Receive Fax Messages)
- Feature bit 110 is required to send a fax to an external machine. It is not required to send internal faxes.
- NuPoint Fax optional feature

194 Deliver Fax Online

Allows the user to call from a fax telephone to retrieve a stored fax message. The user must first listen to any voice comments.

Requires:

- Feature bit 190 (Receive Fax Messages)
- NuPoint Fax optional feature

195 Specify Fax Delivery Number

Plays a Prompt, "Press i to input a number for this fax" that allows a user or caller to press i and enter a telephone number for the fax machine.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 190 (Receive Fax Messages)
- Feature bit 110 is required to send a fax to an external machine. It is not required to send internal faxes.
- NuPoint Fax optional feature

196 Change Default Fax Number

Allows a user to change the default fax phone number. Use this for people who travel between several offices so they can set the default number when arriving at an office.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 190 (Receive Fax Messages)
- Feature bit 193 (Deliver Fax to Default Number)
- NuPoint Fax optional feature

197 Fax-on-Demand for Greeting Only Mailbox

Used for fax publishing. Set up a Greeting-Only mailbox, and include this feature bit so callers can retrieve faxes from the mailbox. The feature bit 194 (Deliver fax online) function is included in this feature bit. To allow the user to input a different number for the fax, include feature bit 195 (Specify fax delivery number).

Requires:

- Feature bit 004 (Outside Caller Functions)
- Feature bit 005 (Play Outside Caller Menu prompts)
- Feature bit 190 (Receive Fax Messages)
- NuPoint Fax optional feature

198 Receive Fax Messages Only

Used for both fax mail and guaranteed fax. Callers do not hear a greeting or prompts, and the mailbox receives only faxes, not voice messages. A fax session starts as soon as the server answers the call.

Requires:

- Feature bit 190 (Receive Fax Messages)
- NuPoint Fax optional feature

199 Auto-receipt for Successful Fax Transmissions

Creates a time-stamped voicemail receipt when a user sends a fax transmission that succeeds. The receipt is placed in the sending user's mailbox.

Note that regardless of whether this feature is enabled:

- Failed fax transmissions always cause a voicemail receipt to be placed in the sending user's mailbox.
- If an Email Fax Confirmation address is configured, both failed and successful fax transmissions cause an email confirmation message to be sent to the user. The subject line of the email includes the following information: success/failure status, number of pages, and date and time of transmission attempt.

Requires:

- Feature bit 020 (Make Messages)
- Feature bit 070 (User Options Menu)
- Feature bit 095 (Mark Message for Future Delivery)
- Feature bit 190 (Receive Fax Messages)
- Feature bit 193 (Deliver Fax to Default Number) or Feature bit 195 (Specify Fax Delivery Number)
- NuPoint Fax optional feature

26.27.4 Feature Bits 200 to 249

200 Personal Fax Cover Page

Allows the user to enter a personal fax cover page that identifies the user as the recipient that will be attached to any faxes the user retrieves. In the system administrator's mailbox, the cover page becomes the company fax cover page, and is delivered with any faxes for users who do not have a personal cover page.

If there is no personal or company cover page, then the server does not auto-generate a default cover page.

Requires:

- Feature bit 190 (Receive fax messages)
- NuPoint Fax optional feature

201 Deny Trivial Passcode

Checks passcodes to prohibit sequential numbers, such as 1234, and a sequence of a single digit, such as 1111. (However, 21111 is allowed.)

Requires feature bits:

- 070 (User Options Menu)
- 073 (Enter and change passcode)

Note:
This feature bit only works with NuPoint UM Standalone deployments. It is inoperable with NuPoint UM on MiCollab .

202 Do Not Play Mailbox Name or Ext Number

Use this in the hotel/motel environment to suppress the name or extension number of a guest who leaves a message in another guest's mailbox. This keeps hotel guests' names and room numbers confidential.

Requires feature bit 020 (Make messages).

203 Walkaway Fax for Callers

Allows callers to dial a mailbox and send a fax without voice comments. If the server detects an incoming fax tone, it processes the incoming fax. Without a fax tone, the caller hears the normal mailbox greeting and prompts. If the mailbox includes feature bit 087 (Make and mark urgent), you must train the users and callers to press 8 twice if they wish to mark a fax urgent.

Requires the NuPoint Fax optional feature.

204 Message Skip, Forward and Backward

Allows the user to press two keys to skip forward to the next message or backward to the previous message:

T#	Skip forward
T*	Skip backward
TI	Replay the message time stamp
TO	User Options

Pressing T without pressing another key within two seconds causes a skip forward. To use this function with NuPoint Fax, these key combinations apply:

T	Fax Transmittal options
T#	Skip forward
TT	Skip forward
T*	Skip backward
TI	Replay the message time stamp
TO	User Options

Overrides feature bits 048 (No auto-time stamp of unplayed messages), 049 (No auto-time stamp of played messages), and 144 (Skip forward to next message).

205 Do Not Use Text Count for Message Waiting

Sets the server to ignore the text count for the message waiting indicator, even if the text count is one or more.

206 Discard Fax Message After Delivery

Automatically deletes a fax after sending it. Used in guaranteed fax to prevent res-ending the same fax.

Requires the NuPoint Fax optional feature. For more information, see the NuPoint Fax Manual.

Feature bit 237 (Automatically deliver fax to default number) overrides this.

207 Fax Verify (Sending System Not Self)

Used with guaranteed fax mailboxes that can call a system port. It prevents an outgoing call to its own mailbox number.

Requires the NuPoint Fax optional feature.

208 Play Reorder Tone After CTP or Greet-only

Plays a reorder tone (fast busy signal) after a caller enters a number for cut-through paging, or hears the greeting on a Greeting-Only mailbox to encourage callers to hang up.

Requires feature bit 171 (Cut-through Paging) or 172 (Cut-through Paging and messaging) or a Greeting-Only mailbox.

209 Tone Only Pager Mailbox Interface

Used for special mailboxes that use tones rather than greetings to simulate a paging terminal; intended for DID lines only.

When a caller reaches the mailbox, the server immediately generates a page, according to the schedule set in the mailbox. Callers cannot leave messages. Overrides all feature bits in the Receive Message category.

Requires:

- Message waiting type 1 or 2 defined as 5 (pager) in the mailbox
- A configured pager port

210 Numeric Display Pager Mailbox Interface

Used for special mailboxes that use tones rather than greetings to simulate a paging terminal; intended for DID lines only. When a caller reaches the mailbox and enters a number, the server immediately generates a page, according to the schedule set in the mailbox. Callers cannot leave messages. Overrides all feature bits in the Receive Message category.

Requires:

- Message waiting type 1 or 2 defined as 5 (pager) in the mailbox

- A configured pager port

211 Voice Pager Mailbox Interface

Used for special mailboxes that use tones rather than greetings to simulate a paging terminal; intended for DID lines only. When a caller leaves a voice message, the server immediately generates a page, according to the schedule set in the mailbox. Callers do not hear greetings or Prompts.

Requires:

- Message waiting type 1 or 2 defined as 5 (pager) in the mailbox
- A configured pager port

212 Send Page Upon Answer, Greet-only Mbx

When this feature bit is used with a Greeting-Only mailbox and the BBL Terminal Emulation optional feature, the mailbox can send out a page in accordance with its pager schedule as soon as a call is received, regardless of when the outside caller hangs up.

This feature bit requires:

- Message waiting type 1 or 2 defined as 5 (pager) in a mailbox owner's mailbox
- A pager port defined in the VoiceMemo configuration
- The BBL Terminal Emulation optional feature must be installed and enabled

213 Edit CTP Num with * Key if No Caller Menu

Used for cut-through paging. Allows callers to edit the cut-through page number no caller menu is activated. The caller can press the * (star) key to delete the cut-through page number and enter a new one. The caller then hears: "The number you have entered is [nnnnnn]. Press star to delete this number and enter another. You can press X or hang up to send your page."

Requires feature bit 171 (Cut-through Paging) or 172 (Cut-through Paging and messaging).

Do not include feature bit 005 (Play Outside Caller Menu prompts).

214 (ISO) SMS Voice Messaging Option Enabled

This feature bit enables a voice message option in ISO SMS main menu. If this bit is on, bit 12 must also be on.

Related bits: 12, 167, 269, 278 and 284.

215 Don't Auto-play First Msg (w/auto-play)

Used with feature bits 052 (Auto-play unplayed messages) or 089 (Auto-play all msgs, new and saved), to not automatically play the first message and allow the user to perform other functions in the mailbox. After the user presses P to play the first unplayed or saved message, all subsequent messages then auto-play according to feature bit 052 or 089.

Requires feature bits:

- 050 (Play messages)
- 052 (Auto-play unplayed messages) or 089 (Auto play all msgs, new and saved)

216 Play Receipts After Urgent Messages

Plays urgent messages, then receipts, and then unplayed (non-urgent) messages. Otherwise, unplayed messages play before receipts.

Requires feature bits:

- 050 (Play messages)
- 088 (Receive urgent messages); without feature bit 088, receipts play before all unplayed messages

217 Announce Text Msgs without Count

Alerts a mailbox owner when the text counter is greater than zero, but does not give a count. Use this for integrations that cannot give a text message count to the server, but can indicate the presence of one or more messages.

Overrides feature bit 154 (Announce text (Email) message count).

218 Passcode NOT Needed on Direct Calls

Allows users to log in to their mailboxes from their own telephones without entering a passcode. The integration must provide the telephone number.

219 Login with 0 Using Cut-thru paging

Allows a caller to press 0 to log in to a cut-through paging mailbox; the server sends all other input to the pager display.

Requires feature bit 171 (Cut-through Paging) or 172 (Cut-through Paging and messaging).

220 No Dial Ext or Email if Unplayed Msgs

Disables the user transfer to Dial an Extension or Email if there are unplayed messages in the queue. After the user plays all unplayed messages, the transfer is allowed.

Requires either NP Receptionist or the Email interface optional feature, which requires feature bit 170 (Transfer to Email system).

221 Deny Caller Transfer to Email

Prevents an outside caller transfer to Email if the Email interface is installed.

Do not use feature bit 176 (Say “Press pound [#] for more options” to callers) with this, unless the system has Dial-an-Extension for outside callers.

222 Deny Nesting of Distribution Lists

Prevents mailbox owners from nesting distribution lists. Otherwise, a distribution list number can be a member of another distribution list.

Requires feature bits:

- 070 (User Options Menu)
- 074 (Create or modify user distribution list)

223 Delay Requested Receipt for 24 Hours

Causes the server to wait 24 hours before delivering receipts so that a mailbox owner can use receipts as “ticklers” to follow up calls. The receipt arrives 24 hours after the user sends the message and indicates whether or not the recipient played the message.

Requires feature bits:

- 020 (Make messages)
- 021 (Make and request receipt)
- 050 (Play messages)

Note:
Does not delay automatic (forced) receipts.

224 Auto-transfer to Task Before Greeting

Transfers all outside callers to Email or another phone number. Used with the Email interface, which requires feature bit 170 (Transfer to Email System).

225 Auto-transfer to Task Upon Login

Transfers the mailbox user to Email or another phone number when logging in. Used with the Email interface, which requires feature bit 170 (Transfer to Email System).

226 Auto-transfer to Task After Unplayed Msgs

Transfers the mailbox user to Email or another phone number after the user plays all unplayed messages, but before playing receipts and played messages; therefore the user does not hear Prompts for these. Used with the Email interface.

Requires feature bit 170 (Transfer to Email System).

227 Undelete last Message with * Key

Allows a mailbox owner to undelete a message after deleting it. After pressing D to delete a message, the user can immediately press the * (star) key to retrieve the message. This does not work if the user presses any other key immediately after pressing D.

You can use this with other feature bits that use the * (star) key, such as 144 (Skip forward to next message) or 158 (Continue sending message, * key), because they use the star (*) key in a different

context. However, you cannot use this with feature bits 052 (Auto-play unplayed messages), 056 (Autodiscard messages), or 089 (Auto-play all msgs, new and saved).

Requires feature bits:

- 050 (Play messages)
- 055 (Discard messages)

228 Set Msg Wait #3 for Urgent Msgs Only

Activates message waiting type 3 for urgent messages only, and not for other unplayed messages.

Requires:

- Feature bit 040 (Receive messages from other users) and/or 041 (Receive messages from outside callers)
- Feature bit 088 (Receive urgent messages)
- Message waiting type 3 defined for the mailbox

229 Play Names of Lists 1 Children

Used with a shared extension mailbox to play the name of each child mailbox defined in distribution list 01. You can specify up to 190 child mailboxes.

For details on shared extension mailboxes, see the Shared Extension Suggested Additional FCOS and FCOS 15 (Tree).

230 Deny Change of Fax Cover Page Options

Prevents a user from changing a fax cover page through the User Options menu. A user can use a default company cover page, or a personal cover page that the system administrator entered through the server console.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 190 (Receive fax messages)
- NuPoint Fax optional feature

231 Passcode Broadcast Mailbox

Broadcasts the passcode to a list of mailboxes, like a broadcast mailbox sends a message to other mailboxes. Use distribution list 09 for the broadcast passcode mailbox list. Typically used in a network environment such as NP Net.

Mailboxes that receive the passcode must include feature bit 232 (Allow receipt of passcode broadcasts).

A broadcast passcode mailbox can also be a tree mailbox or a broadcast message mailbox. Use distribution list 01 for the tree or broadcast message feature. Use distribution list 09 to broadcast the passcode.

Can be used with feature bit 174 (Define broadcast greeting mailbox) or 178 (Define broadcast name mailbox). Both use the same distribution list 09.

232 Allow Receipt of Passcode Broadcasts

Allows a mailbox to receive a passcode from a passcode broadcast mailbox. For information on the broadcast passcode mailbox, see feature bit 231 (Passcode broadcast mailbox) for more information.

233 Not Used

234 Check Message Wait Status of Children

Used with a shared extension mailbox to check the message waiting status of all child mailboxes defined in distribution llist 01, up to 190. For details on shared extension mailboxes, see the Suggested Additional FCOS, Shared Extension, and FCOS 15 (Tree).

When a child mailbox broadcasts its message waiting status to the shared extension mailbox, this causes the parent mailbox to check all other child mailboxes for messages before turning off the message waiting indicator. Otherwise, if two child mailboxes receive new messages, and one user retrieves the message, the message waiting indicator turns off, even though the other child mailbox still has a message waiting.

Child mailboxes require:

- Feature bit 134 (Broadcast message waiting status)
- Distribution list 01 with parent mailbox as only member
- Feature bit 229 (Play names of list 1 children)

The parent mailbox requires:

- Feature bit 070 (User Options Menu)
- Feature bit 072 (Record or change mailbox greeting)
- Feature bit 121 (Define tree mailbox)
- Configured message waiting indicator

235 Display FROM Field on Fax Cover Page

Adds the “From” field to the default fax cover page to show who sent the fax.

Requires:

- Feature bit 190 (Receive fax messages)
- **NuPoint Fax** optional feature

236 Display Promotional Messages on Fax Cover Page

Adds a promotional message field to the default fax cover page.

Requires:

- Feature bit 190 (Receive fax messages)

- NuPoint Fax optional feature

237 Automatically Delivers Fax Message to Default Number

Allows the user to automatically send faxes to a default fax number when they arrive in the mailbox to make it easier for users who regularly use the same fax machine to retrieve their faxes. The fax or voice/fax message automatically moves to the saved queue without turning on the message waiting indicator. The user can set this in the User Options menu.

Requires:

- 070 (User Options Menu)
- 190 (Receive fax messages)
- NuPoint Fax optional feature

Overrides feature bit 206 (Discard fax message after delivery). Use 206 for guaranteed fax mailboxes only.

238 End-of-session Multiple Fax Delivery Number

Enables the server to make only one outbound call for all faxes sent to the same number during a mailbox session. This is invisible to users and saves on outbound fax calls.

Requires:

- Feature bit 191 (Make fax messages)
- NuPoint Fax optional feature

239 Retrieve All Unplayed Faxes Through User Option

Groups multiple unplayed faxes in a mailbox for a single delivery to the fax machine rather than sending each fax to the fax machine individually. The user can select this option in the User Options menu.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 190 (Receive fax messages)
- A default fax number
- NuPoint Fax optional feature

240 Receive Fax on Voice Recording Timeout

Allows a caller to dial a mailbox from a manually operated fax machine, press start, and walk away, or, if adding voice comments, to skip pressing L to send the fax.

Requires:

- Feature bit 070 (User Options Menu)
- Feature bit 190 (Receive fax messages)
- NuPoint Fax optional feature

241 Suppress Broadcast Forced Receipt Number

If a name, greeting, or passcode cannot be broadcast from a Broadcast mailbox to a recipient's mailbox, this logs a message in the system log file and prevents the server from creating forced receipts in a recipient's mailbox.

242 Say Variable Passcode Prompts for Business Guest Mailboxes Number

Used for guest mailboxes in a business environment. Causes the server to prompt the mailbox owner (usually the administrator) to enter a passcode within a set range of digits. Passcodes can be changed for guest mailboxes even without feature bit 073 (Allow to change passcode). Other feature bits, such as 130 (Passcode cannot be same as mailbox), 201 (Passcode not simple series), or 125 (Allow user to clear passcode) affect which passcodes can be used.

This feature bit is not recommended for a hotel/motel environment.

243 (ISO) Transfer to API on Main Menu Key 4

This bit enables menu option key '4' on the Main Menu. This option key can be used for the following prompts:

- "To hear a NewsMemo category, press 4"
- "To erase this message, press 4"
- "Pressing 4 to hear a NewsMemo lets you review a story for a NewsMemo category"

244 (ISO) Transfer to API on Main Menu Key 5

245 (ISO) Transfer to API on Personal Options Menu Key 6

246 (ISO) Transfer to API on Personal Options Menu Key 7

247 Don't Play Any Prompt to Fax Call Placement Recipient

Suppresses prompts to a call placement recipient for a fax message. Use this when broadcasting a fax message to multiple telephone numbers.

Requires:

- Feature bit 020 (Make messages)
- Feature bit 110 (Make/give to telephone number)
- Feature bit 191 (Send fax messages)
- NuPoint Fax optional feature

248 (ISO) Deny Transfer to API for Guest Mailboxes

249 Allow Transfer to Help Desk During Tutorial

26.27.5 Feature Bits 250 to 306

250 Allow NP PWG View Login

Allows a user to log in to NP View. Requires the NP View optional feature. For more information, see the NP View Administrator's Guide.

251 Allow NP PWG View Telephone Playback/Record

Allows a user to use a telephone to play and record NP View messages.

Requires:

- Feature bit 250 (Allow NP View login)
- NP View optional feature; for more information, see the NP View Administrator's Guide Feature bit 259 (Restrict NP View user to play only faxes) overrides this.

252 Allow NP PWG View Client to Change Mailbox ID

Allows a user to change the ASCII name of the mailbox during an NP View session. This affects the mailbox name in NP View, Dial-by-Name, and Mailbox Maintenance.

Requires:

- Feature bit 250 (Allow NP View login)
- NP View optional feature; for more information, see the NP View Administrator's Guide

253 Not Used

254 Turn on Mailbox Message Trace

Enables a utility that traces, or tracks, activity for the mailbox and stores it in a record that you can retrieve through the Mailbox Maintenance menu. Use this feature bit only to troubleshoot a specific mailbox.

255 Delete Mailbox if No Unplayed Messages

Used with the NP OnDemand optional feature to allow users to have temporary mailboxes that are created only when a message arrives for them. This deletes the temporary mailbox after the user plays the message or when the unplayed message reaches the retention limit set in the LCOS. Deleting occurs at midnight, when Automatic Purge runs.

Requires:

- Feature bit 041 (Receive messages from outside callers)
- Feature bit 050 (Play messages)
- Mailbox on Demand optional feature; for more information, see the NP OnDemand Manual

Feature bit 218 (Passcode not needed on direct calls) is recommended.

256 Enable Fixed Greet "Press 1 or wait" for Walkaway Fax

Plays a fixed greeting, ”r;Press 1 or wait,” for walkaway fax that sets a mailbox to expect calls from fax machines rather than from live callers.

Requires:

- Feature bit 203 (Walkaway fax for callers)
- NuPoint Fax optional feature; for more information, see the NuPoint Fax Manual

257 Prevent NP PWG View User Voice Playback/Record

For security purposes, prevents users from playing or recording voice messages on their PCs. Users can view faxes and see the list of messages, but they must use a telephone, not speakers, to hear voice messages. Do not include feature bit 251 (Allow NP View telephone playback/record) unless you include feature bit 259 (Restrict NP View client to play only faxes). Here are the possible combinations of the three feature bits:

251	257	259	Result
In	Out	Out	Users can play/record with sound card or with Call-Me/Meet-Me
In	In	Out	Users can play/record with Call-Me/Meet-Me only
Out	Out	Out	Users can play/record with sound card only
Out	In	In	Users cannot play/record voice messages; users can only Make, View, and Save fax messages

Requires:

- Feature bit 250 (Allow NP View login)
- NP View optional feature; for more information, see the NP View Administrator’s Guide

258 Prevent NP PWG View Client from Using Local Storage

By default, NP View saves on the server. For security purposes, this prevents users from saving messages to local folders.

Requires:

- Feature bit 250 (Allow NP View login)
- NP View optional feature; for more information, see the NP View Administrator’s Guide

259 Restrict NP PWG View Client to Play Only Faxes

Allows users to view, make, and save faxes, but not to view, make, and play voice messages. Do not use with feature bit 251 (Allow NP View telephone playback/record).

Requires:

- Feature bit 250 (Allow NP View login)
- NP View optional feature; for more information, see the NP View Administrator's Guide

260 Allow NP PWG View Client to have Caller ID Lookup

If Caller ID information is available from the switch, allows the user to use the local database for phone number-to-caller name look-up. Use this with feature bit 262 (Store caller line ID as a phone number).

To determine if Caller ID is available, contact your telecommunications representative.

Requires:

- Feature bit 250 (Allow NP View login)
- NP View optional feature; for more information, see the NP View Administrator's Guide

261 Allow NP PWG View WEB Access to Messages

262 Store Caller Line ID as a Phone Number

Allows users to receive CLI information in the NP View Inbox as a phone number rather than as a mailbox, which is the default. The caller's phone number appears in the "Mailbox#" field and the caller's name appears in the "Caller" field.

This feature bit requires:

- Feature bit 250 (Allow NP View login)
- Feature bit 260 (Allow NP View user to have Caller ID lookup)
- NP View optional feature. For more information, see the NP View Administrator's Guide.

263 Store Caller Line ID as a Phone or Mailbox Number

Allows users to receive CLI information in the NP View Inbox "Mailbox#" field as either a mailbox or a phone number associated with the message. The user hears that mailbox or phone number when retrieving the message by telephone. If the caller's phone number matches the dial plan and a mailbox number, the mailbox number is associated with the message. Otherwise, the phone number is associated with the message.

264 Play Outside Caller User Interface for CLI Capture

Allows an outside caller to enter a callback number manually, from the keypad, to be captured as the CLI callback number.

265 Enable NP RapidDial Features

Enables the NP RapidDial optional feature in the mailbox. For details, see the NP RapidDial Manual.

266 Enable SMSC for Callback Numbers

267 Enable SMSC for Short Text Messages

268 Enable SMSC Receipts

269 (ISO) SMS Allow Urgent Deliver

270 Enable Dial-Back Feature

Allows users to dial back a caller who leaves a voice mail. Used in conjunction with feature bits

263 (Store Caller Line Id as a phone or mailbox number), 264 (Play outside caller user interface (with FCOS bit 280)), and 280 (Enable CLI outside caller interface (with FCOS bit 264)) to enable the Dial-back feature.

271 Send SMSC Cancel VMNs for ML_OFF

272 Send SMSC Cancel CBNs for ML_OFF

273 Send MWN Via SS7 Information Directives

274 Not Used

275 Enable SMSC Customized Text Messages

276 Press 0 for More Billing Info

Allows the user to check billing information from the mailbox. After the user listens to an unplayed message, the Prompt includes ”r;Press 0 for billing information.” Pressing 0 transfers the user to a greeting-only mailbox that plays billing information specific to that user, then returns the user to the main menu.

Note: For information about using this to collect billing information, see the Call Detail Recorder Manual. To set this up, reach the Mailbox Maintenance screen for the mailbox, then enter a greeting-only mailbox number in the ”r;Attend DN” field. Do not use ”r;H” or ”r;S+” in the transfer string. Users cannot press 0 to transfer to the attendant.

Requires a greeting-only mailbox.

277 Send Mail Waiting Notice After Mbox Deletes

278 (ISO) SMS Callback Number Enabled

279 Enable TollSaver for Outsider Leaving Message

280 Enable CLI Outside Caller Interface

Must be used with feature bit 264 to activate the CLI outside caller interface for the mailbox. Allows an outside caller to enter a callback number manually, from the keypad, to be captured as the CLI callback number.

281 Enable NP Boomerang Manual Callback Number Option 'N'

282 Enable Call Screening in MBOD for Callers and Users

Enables the user to screen calls by prompting outside callers to state their names before leaving a message. The user hears the caller's name before playing the message.

Requires:

- Feature bit 133 (Don't say: "You may start your message now.")
- NP OnDemand optional feature

283 Say Number of Unplayed Messages on Last Logout

Allows users to hear the number of messages left unplayed.

284 Provide Callback Number Delivery Options

Captures the caller line ID number.

Requires NP Boomerang or CLI optional features.

285 Enable Speech to Text

Allows users to access transcription of voice mail messages to text. Can be used alone or in conjunction with the following bits to provide specific features:

- For automatic transcription, UM Advanced users also require feature bit 295; UM Standard users require bit 304.
- To provide transcription request link in UM email messages, feature bit 289 OR 295 (and a UM Advanced license)
- Features bit 290 to view and/or save a text transcription of a voice mail message in the Web View

286 To Allow Mailbox to Accept Calls without Charge

287 Enable Enhanced Auto Wakeup

Allows users to reach the wakeup menu directly from Main menu, rather than through the User Options menu. For details, see the NP WakeUp Guide.

Requires the NP WakeUp optional feature.

Do not use with feature bit 015 (Change wakeup options).

288 Enable TUI Emulation

Provides a telephone user interface (TUI) that emulates the first level of the Octel/Avia voice mail system. This feature can be employed by customers who have migrated to the NuPoint Unified Messaging platform from a competitive system and wish to continue using well-known TUI commands for common functions.

289 Enable UM - SMTP

Allows Unified Messaging users to have their voice mail messages forwarded to their email address via SMTP forwarding.

290 Enable UM - Web View

Allows Unified Messaging users to access their voice mail messages from a Web browser or email client. To use their email client, the client must be configured for Web access.

291 Enable RAC (Record A Call)

Enables soft keys on the user's phone, to allow the user to save phone conversations to their NuPoint mailbox.

Do not use with feature bit 122 (Define Broadcast Mailbox).

292 Enable NP Call Director

Allows the current mailbox to create a personal call flow to direct callers.

293 Disable the <Save> <Reply> and <Forward> Buttons on the UM Standard Web View Web Pages

Removes the save, reply, and forward buttons from the Unified Messaging user's Web View interface so that the user cannot manipulate their voice mail messages.

294 Enable the Mitel Embedded Player on the UM Standard Web View Web Pages

Enables a secure, embedded applet that will play voice mail messages through the user's PC speakers. Does not create temporary files on the user's PC.

295 Enable Advanced UM

Enables Advanced UM options for users who also have the Standard UM option. Allows users to access messages from the Web View in an email client or Web browser. Also allows users to access messages from the TUI. (E-mail can be accessed through the TUI via Text-to-Speech functionality.)

Requirements:

- Each Advanced UM user must have a mailbox configured with an Email Alias (Microsoft) , Full Name (Lotus), or UM Email Address (Google). All required fields must be completed; if they are left blank or misconfigured, the user will not be found and a service interruption may occur.
- If a password changes in the client, it must also be changed in the mailbox.
- Licenses must be purchased for all Advanced UM users.

296 Enable Text-to-Speech Playback

Requires feature bit 295.

297 Enable Extended Absence Greeting

An Extended Absence Greeting (EAG) tells callers that the person they are calling is away for an extended period of time. Callers do not have the option to skip the greeting. At the end of the greeting, callers can leave a message, transfer to the line-group attendant, or end the call.

Note: The Extended Absence Greeting supports only Mnemonic and UK English prompts.

You must assign FCOS 297 (Enable Extended Absence Greeting) to a mailbox to allow the user to record and enable an EAG. You can also assign 298 (Disable message delivery when Extended Absence Greeting is enabled). For information on how users record and enable an EAG greeting for their mailbox, refer to the NuPoint Unified Messaging *Messaging User Guide*.

EAG is included in the base software and can be enabled for any NuPoint Unified Messaging user.

298 Disable message delivery when Extended Absence Greeting is enabled

Prevents callers from leaving a message for the mailbox user when that user has an Extended Absence Greeting enabled. Callers can transfer to the line-group attendant for further options, or they can end the call.

Requires feature bit 297.

Note: This bit has a conflict with feature bit 133: Don't say: "You may start your msg now". If the mailbox user has also enabled feature bit 133, then messages are not prevented from being left.

299 Allow choice of unplayed or saved messages during playback

Provides mailbox users with the choice to play unplayed or saved messages first.

300 Enable secure tutorial

Prevents the mailbox PIN from being played back to the user for confirmation during the tutorial. Instead, the user is required to confirm the passcode by entering it twice.

301 Text-To-Speech playback new messages only

When a user employs the Text-to-Speech feature to listen to email messages, only new messages will be played. Messages that have already been read will not be played.

Requires feature bit 296.

301 Enable "Press # when you are finished recording" prompt to make, forward, or answer a message for a mailbox

Enables the prompt to inform users to press the pound key (#) when they are finished recording a voice message. This prompt applies to mailbox-to-mailbox messaging and to messages recorded after being forwarded to a user's mailbox.

302 Enable Alternate MWI for Skipped Messages

Enables users to skip a new message (if bit 204 is enabled), have it remain in the unplayed queue (if bit 145 is enabled) and when the user logs out have the MWI lamp turn off. The user is still able to log in at any time and listen to the skipped messages that were still marked as unplayed and are announced as such.

303 Disable Web View Downloads

FCOS 303 is used to disable downloading of the Outlook Client Plug-in (OCP) installation or Fax Printer installation executables from the Web View interface (Downloads page). The OCP installation is enabled

by default when FCOS 295 (Advanced UM) is enabled. The new FCOS 303 must be set in order to disable downloads from the Web View.

304 Enable UM Standard

Allows Unified Messaging users with the Standard UM option to access their voice mail messages from any email client. This feature bit enables the configuration of three email addresses for the user.

305 Do not Play Back the Message Caller ID

The server will not play the caller ID (CLID) during message playback. Instead of hearing a time stamp and CLID, users will only hear a time stamp before the message is played. This feature bit is intended for users who receive many messages or who have a limited amount of time to listen to messages. Requires feature bit 050 (Play messages).

306 Play Back Caller ID After ID

By default, the caller ID (CLID) of the person who has left the message is played prior to the message. Enabling this feature bit will cause the CLID to be played after message playback. While the CLID is playing, the user can skip ahead to the voice message menu by pressing any key. Requires feature bit 050 (Play messages).

Notes:

- If feature bit 305 is enabled, feature bit 306 is disabled and the CLID will *not* be played.
- This feature only applies to voice messages, not FAX messages. If feature bit 306 is enabled and you use the TUI to retrieve a fax message, the sender's CLID will *not* be played.

26.28 Other Classes of Service - Overview

A class of service differentiates privileges and functions for mailboxes. The previous section discusses the Features Class of Service (FCOS), which controls the features in mailboxes. This section discusses three other classes of service:

- **Limits Class of Service (LCOS)** controls time and storage parameters within mailboxes, such as the number of messages the mailbox can store, as well as the set of Prompts
- **Group Class of Service (GCOS)** manages communication between mailboxes
- **Restriction Class of Service (RCOS)** controls the outdial applications, such as Call Placement, message delivery, and pages, and limits these telephone calls by either area code or prefix.

The two remaining classes of service are described in detail outside of this section:

- A **Network Class of Service (NCOS)** controls network access for users; see the NP Net application section.
- A **Tenant Class of Service (TCOS)** manages mailbox interaction between user communities; see "ESMDI Integration" in the *NuPoint Unified Messaging Optional Integrations Guide* for more information.

26.28.1 Limits Class of Service - Overview

The Limits Class of Service (LCOS) consists of a set of limits parameters configured to a value of your choice. As the administrator, an LCOS is the best resource available to you to control the use of disk storage.

The LCOS assigned to a mailbox's configuration controls the time and storage parameters associated with that mailbox. For example, the LCOS can control message-length and the total number of messages stored in a mailbox. You can also modify an LCOS to specify alternate language prompts.

Be aware that certain options interact within and between these Classes of Service; some options require other options, and some combinations of options conflict. In particular, the LCOS can affect how the FCOS functions. For example, if you allow a mailbox owner to make messages and then assign an LCOS that has a user message length of 0 seconds, the user cannot record a message.

Pre-Programmed LCOS

LCOS 1 is pre-programmed. You can copy this LCOS and customize it as required. The LCOS parameters and their default settings for LCOS 1 are listed in LCOS Limits Parameters and Defaults. Up to 640 LCOS can be configured in this system; each can have different limits for all parameters in the Limits Parameters Menu.

LCOS for the Administrator or Attendant Mailbox

For best results, assign the default LCOS (LCOS 1) to both the administrator's and the attendant's mailboxes. LCOS 1, with the appropriate FCOS and GCOS, supports the special functions for these mailboxes.

Selecting Alternate Language Prompts

The default language for all line groups is English; all languages other than English are optional features.

You can modify a line group or LCOS so that users receive prompts in an alternate language. In addition, you can specify a second alternate language for line groups. This enables users to select between multiple languages (for example, English and French) when they call into the Message Center or NuPoint Receptionist application.

Before you can specify alternate languages for a line group or an LCOS, you must install the alternate-language prompt software.

If your server is running more than one language at the line group level (one or two per line group) and you want to control the line groups that callers reach, specify a prompts language for each LCOS. This process ensures that callers hear mailbox prompts in the correct language.

26.28.2 LCOS Parameters and Default Values (Web Console)

LCOS 1 is pre-configured; it contains the default values for all parameters. All mailboxes are assigned LCOS 1 by default, unless otherwise configured by the system administrator.

Limits Values - Web Console Layout

General Limits	U	Def u	Min	Max	Notes
Greeting length	Minutes	2u	0	60	Sets the maximum time for recording a personal greeting. When the user reaches this limit or the server detects silence, the server stops recording and announces that the recording is complete. If no limit is set, the limit is the available storage capacity. Can also be disabled.

General Limits	U	Default	Min	Max	Notes
Username length	Seconds	2	0	248	Sets the maximum time for recording the mailbox name. When the user reaches this limit or the server detects silence, the server stops recording and announces that the recording is complete. If no limit is set, the limit is the available storage capacity. This name is announced when the user makes or gives a message; also used by NP

General Limits	U	Default	Min	Max	Notes
Message count		200		200	Sets the maximum number of messages in a single mailbox. When the user's mailbox is 80% full, the system will warn the user to "delete any unnecessary messages" as follows: • An audible prompt will be played when the user logs in to his or her mailbox. • An email message will be sent to the user's

General Limits	U	Du	Mi	Ma	Notes
User message length	Minutes	5	0	60	Sets the maximum time, in minutes, that another user can make, give or answer a message for this mailbox. When the user reaches this limit or the server detects silence, the server stops recording and announces that the recording is complete.

General Limits	U	Du	Mi	Ma	Notes
Caller message length	Minutes	5	0	60	Sets the maximum time, in minutes, that a caller can leave a message for this mailbox. When the caller reaches this limit or the server detects silence, the server stops recording and announces that the recording is complete.

General Limits	U	Default	Min	Max	Notes
Maximum login time	Minutes	0 (unlimited)		50	Sets how long, in minutes, a user can remain logged in to the mailbox in a single session. At the end of this time, the server automatically logs the user out.
Maximum attachments per page		100		100	Limits the number of messages that the user can attach when making or giving a message.

General Limits	U	Default	Min	Max	Notes
Future delivery message count		99	1	99	Sets the maximum number of messages that can be stored in a mailbox's future delivery queue. Enter 0 to disable.
Future delivery maximum days	Days	60	1	365	Sets the maximum delay, in days, to deliver a message in the future. Enter 0 to disable.

General Limits	U	Default	Min	Max	Notes
Minimum message length	Seconds	0 (unlimited)	0	5	Sets the shortest time for a message to be considered valid. Shorter messages are not delivered.
Minimum recipients count		65536	65535		Sets the minimum number of recipients needed to activate a receipt summary. The system then plays receipts in this order: for undelivered messages, unplayed messages, then played messages. 0 = the maximum (65535)

General Limits	U	Du	Mn	Mn	Notes
Maximum recipients count		65	63	65535	Sets the total number of possible recipients of a message in any combination of mailboxes, distribution lists, and nested distribution lists. If the number of recipients exceeds this limit (*n*), the system sends the message to only the first (*n*) recipients. 0 = the maximum (65535)
Passcode Expiry Period	Days	0	0	365	Enter 0 to disable.

General Limits	U	D u	M n	M n	Notes
Wake UP Limits	Un	Default	Minimum	Maximum	Notes
Phone length	Number of Digits		1	24	Sets the maximum number of digits a user can enter for a wakeup call phone number.
Maximum days	Days	0 (unlimited)	0 (unlimited)	365	Limits the time in the future that a user can schedule a wakeup call.
Billing Limits	Un	Default	Minimum	Maximum	Notes
Maximum pages per billing		0 (unlimited)	0 (unlimited)	999	Sets the maximum number of times a user can be paged during one billing cycle.

General Limits	U	D u	M n	M n	Notes
Maximum wake-up per billing		5	0 (unlimited)	99	Sets the maximum number of wakeup calls a user can schedule during one billing cycle.
Minimum billed number length	Number of Digits	0	0	25	Sets the minimum number of digits in a dial string to activate billing for outdials.
Call Placement Limits	Un	Default	Minimum	Maximum	Notes

General Limits	U	Default	Min	Max	Notes
RNA retry limit	Retries	5	1	255	Sets how many times the server tries to deliver a call placement message after a Ring No Answer call.
RNA retry interval	Minutes	5	1	255	Sets how long the server waits between tries to deliver a call placement message after a Ring No Answer call.

General Limits	U	D u	M n	M n	Notes
Busy retry limit	Retries	5	1	255	Sets how many times the server tries to deliver a call placement message after a Busy call.
Busy retry interval	Minutes	5	1	255	Sets how long the server waits between tries to deliver a call placement message after a Busy call.
Message phone length	Number of Digits	10	1	25	Sets the maximum number of digits a user can enter for a call placement phone number.

General Limits	U	D u	M n	M n	Notes
Recipient count		1	90	198	Sets maximum number telephone numbers you can enter at any one time, for a single message. This includes both call placement, and AMIS messages
Maximum message length	Minutes	5	0 (unlimited)	60	Sets how long a message can be for a call placement phone number.
Distribution List Limits	Un	Default	Minimum	Maximum	Notes

General Limits	U	D u	M n	M n	Notes
Maximum members per list		200	(unlimited)	65535	Sets the total number of possible recipients of a message in any combination of mail boxes, distribution lists, and nested distribution lists. If the number of recipients exceeds this limit (n), the system sends the message to only the first (n) recipients.
Maximum number of lists		990	(unlimited)	999	Sets the maximum number of distribution lists allowed in a mailbox.

General Limits	U	Default	Minimum	Maximum	Notes
Fax Limits	Units	Default	Minimum	Maximum	Notes
Maximum number of digits	Digits	11	1	25	Sets the maximum phone number for fax delivery.
Fax message count		100	1	199	This is the maximum number of fax messages that can be stored in the mailbox at anytime.

General Limits	U	D u	M n	M n	Notes
CNG tone detection length	Seconds	0 (unlimited)			This parameter SHOULD be 0! Starting with the NuPoint Messaging architecture, CNG can be detected during greet and even record. Consequently, an incoming walkaway fax will be taken through the user's greet or during record if missed during the greet period. This provides an effective dual use mailbox (message or fax). The parameter has been

General Limits	U	D u	M n	M n	Notes
Fax delivery retry limit	Retries	5	1	255	This is the maximum number of unsuccessful attempts of fax delivery.
Fax delivery retry interval	Minutes	5	1	255	This is the number of minutes that the system waits between fax delivery tries.
ISO User Interface Limits	Units	Default	Minimum	Maximum	Notes
Maximum family members or guests		0 (unlimited)			Not used.
Reminder calls maximum days	Days	0 (unlimited)			

General Limits	U	Default	Minimum	Maximum	Notes
Maximum reminder calls per billing		0 (unlimited)			
Maximum destinations per reminder		0 (unlimited)			
Language	Un	Default	Min	Max	Notes
Language		Default	N/A	N/A	Only installed languages can be assigned. Select a language from the drop-down list.
Message Age Limits	Un	Default	Min	Max	Notes

General Limits	U	D u	M n	M n	Notes
Played messages retention	Ho	672	1	8760	Sets how long a played message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.
Unplayed messages retention	Ho	336	1	8760	Sets how long an unplayed message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.

General Limits	U	D u	M n	M n	Notes
Urgent messages retention	Hours	336	8760		Sets how long a played or unplayed urgent message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.

General Limits	U	Default	Min	Max	Notes
Cut-thru paging receipt retention	Hours	672	1	8760	Sets how long a receipt for a cut-through paging message can remain in a mailbox before it is deleted by automatic purging. For more information, see the Cut-Through Paging. 0 means unlimited.

General Limits	U	D u	M n	M n	Notes
Receipt retention	Hours	672	8760		Sets how long a receipt for a message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.
Played fax retention	Hours	672	8760		Sets how long a played Fax message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.

General Limits	U	D u	M n	M n	Notes
Unplayed fax retention	Hours	36	8	760	Sets how long an unplayed Fax message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.
Urgent fax retention	Hours	36	8	760	Sets how long a played or unplayed urgent Fax message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.

General Limits	U	Du	Mn	Mn	Notes
Fax receipt retention	Hours	672	8760		Sets how long a receipt for a Fax message can remain in a mailbox before it is deleted by automatic purging. 0 means unlimited.

General Limits	U	D u	M n	M n	Notes
Absolute message retention	Hours	0	8	8760	Sets how long a message stays in the mailbox if the user does not delete it. **Note**: If you set this to less than the values for the Played and Unplayed message retention parameters, it overrides them. If this is set to 0 (the default), it is ignored. 0 means unlimited.
MWI Limits	Un	De ult	Mi mu	Ma mu	Notes

General Limits	U	Default	Min	Max	Notes
Paging Phone Length	Digits	11	1	24	Sets the maximum number of digits a user can enter for a pager phone number.
Message delivery phone length	Digits	11	1	24	Sets the maximum number of digits a user can enter to for a message delivery phone number.
MWI message length	Minutes	0 (unlimited)	0	5	Sets the shortest time for a message that will activate message waiting or paging for the mailbox.
Network Limits	Units	Default	Minimum	Maximum	Notes

General Limits	U	Du	Mn	Mn	Notes
Network queue message count		99	1	99	Limits how many messages a user can make or give for remote delivery. For more information, see NP Net.
Maximum attachment per network message		1	9	1	Limits the number of messages that the user can attach when making or giving a message in a network environment. For more information, see the NP Net and VPIM optional features.

General Limits	U	D u	M n	M n	Notes
Maximum hours to wait for reply from NIB	Hours				Not used.
Outdial Applications Limits	Und	Default	Min	Max	Notes
Minimum billed number length	Digits	0	0	25	Sets the minimum number of digits in a dial string to activate billing for outdial.
Call Director Template	Und	Default	Min	Max	Notes

General Limits	U	D u	M n	M n	Notes
Template		No T empl ate	N/ A	N/ A	Only existing templates can be assigned. Select a template from the drop-down list.
Unified Messaging Limits	Un	De ult	Mi mu	Ma mu	Maximum

General Limits	U	D u	M n	M n	Notes
Unified Messaging Limits		Yes			For Standard Unified Messaging users. By default, the system forwards voice mail messages to email clients as audio attachments, links to audio files, links to messages in Web View, or text notifications. To save hard drive space you can limit notifications to text format only. Setting unified messaging limits (selecting "No" for "Allow All SMTP Delivery Options"

26.28.3 Create a New LCOS from a Copy

Creating a new LCOS consists of assigning:

- a number (we recommend that you use consecutive numbering to conserve database space)
- a name (a descriptive name, up to 15 alphanumeric characters, for example, "ForContractors")
- the required limits (for example, you might set the Mailbox passcode expiry parameter for all contractors to 90 days)
- the prompt language, if other than the default English

Use the LCOS worksheet to organize the information you need. (See a sample worksheet.)

To create a new LCOS based on an existing LCOS:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(L) Limits COS**.
2. Select **(C) Choose Limits COS to Modify** and enter the **number** of the new LCOS you want to create (1-640), or just press **Enter** if the displayed LCOS is correct.
3. Select **(N) Name Selected LCOS** and enter a descriptive **name** for the LCOS, from 1 through 15 characters.
4. Select **(K) Copy LCOS** and enter the ***n*** **umber** of the existing LCOS you want to copy (1-640).
5. Select the required parameters menu in which you want to make changes. (For example, to change the Passcode Expiry parameter, select **(L) Set Limits for selected LCOS**; to change a message retention parameter, select **(D) Set Mailbox & Message Age Limits**.) See LCOS Parameters and Default Values for the menu location of parameters.
6. Select the parameters you want to change and enter the new values.
7. You can verify your entries by selecting the "Show" menu option for the various parameters menus (for example, **(T) Show More LCOS States**, or **(Y) Show Message Age Limits**.)
8. After confirming that modifications are correct, save the modified limits by exiting the LCOS menu.

26.28.4 LCOS Parameters and Default Values (Text Console)

LCOS 1 is pre-configured; it contains the default values for all parameters. All mailboxes are assigned LCOS 1 by default, unless otherwise configured by the system administrator.

The tables below provide a quick reference to all the limits parameters, with default values.

Limits Parameters Menu	Default Value
(G) Greeting length	2.0 (minutes)
(N) User name length	2 (seconds)
(M) Message count	200*
(B) Messages per billing	0 (no limit)
(L) User message length	5.0 (minutes)
(C) Caller message length	5.0 (minutes)
(E) End of message warning time	0 (seconds)

Limits Parameters Menu	Default Value
(T) Maximum login time	0 (no limit)
(O) Maximum NP View Inactivity Timeout	59 (minutes)
(W) Network queue message count	99
(S) Maximum attachments per message	199
(I) Maximum attachments per network message	199
(D) Message delivery login delay	5 (seconds)
(P) Mailbox passcode expiry	0=disabled (days)

More Limits Parameters Menu	Default Value
(A) NP WakeUp - phone length	11 (digits)
(B) Paging - phone length	11 (digits)
(C) Message delivery - phone length	11 (digits)
(D) Future delivery - message count	99
(E) Max days - future delivery	60 (days)
(F) Max family member or guest	0 (not used)
(G) Message waiting indicator - message length	0 (no minimum)
(H) Minimum message length	0 (no minimum)
(I) Maximum pages per billing	0 (no limit)
(J) Maximum wakeups per billing	0 (no limit)
(K) Maximum outstanding wakeup calls	0 (not used)
(L) Callback number length	11 (digits)

Even More Limits Parameters Menu	Default Value
(A) Max days - NP WakeUp	0 (no limit)
(B) Max days - reminder call	0 (not used)
(C) Max reminder calls per billing	0 (not used)
(D) Max destinations per reminder call	0 (not used)
(E) Max members per distribution list	200
(F) Max recipients count	190 (per message)
(G) Max number of distribution lists	99 (lists)
(H) Min number of recipients for receipt summary	0 (no recipients)
(I) Minimum billed number length	0 (digits)
(J) Max hours to wait for reply from NIB	0 (not used)

Call Placement Menu	Default Value
(A) Ring No Answer (RNA) retry limit	5 (retries)
(B) RNA retry interval	5(minutes)
(C) Busy retry limit	5(retries)
(D) Busy retry interval	5(minutes)
(E) Message phone length	11 (digits)

(F) Recipient count	190
(G) Maximum message length	5 (minutes)

Fax Limits Parameters Menu	Default Value
(A) Maximum Number of digits for telephone number	11 (digits)
(B) Fax Message count	199 (quantity)
(C) Pre-greet silence interval to improve walkaway CNG detection	0 (seconds)
(D) Fax delivery retry frequency	5
(E) Fax delivery retry interval	5 (minutes)

Message Retention Limit Menu	Default Value
(M) Message retention	0 (no limit)
(P) Played message retention	672 (hours)
(U) Unplayed message retention	336 (hours)
(R) Urgent message retention	336 (hours)
(S) Cut-through paging receipt retention	672 (hours)
(T) Receipt retention	672 (hours)
(A) Played Fax Message Retention	672 (hours)
(B) Unplayed Fax Message Retention	336 (hours)
(C) Urgent Fax Message Retention	336 (hours)
(D) Fax Receipt Retention	672 (hours)
(E) Absolute message retention	0 (no limit)

Prompt Language Selection Menu	Default Value
(D) Use default	
Other Prompt set options are listed according to the opt ional features installed.	

*For systems that upgrade to release 4.1 or later from a pre-4.1 release, this LCOS parameter carries forward a default of 73 messages.

26.28.5 Assign an LCOS to a Mailbox

Note: Before a custom LCOS can take effect, you must define it.

To assign an LCOS to a mailbox configuration:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** and enter the *n*umber of the new mailbox you want to configure.

   OR
3. Select **(M) Modify Mailboxes** and enter a mailbox number to modify an existing mailbox.

4. Press **Enter** until the **Limits Class of Service** or **New LCOS** prompt appears and then enter the number of the LCOS that will govern this mailbox. (If you are modifying a mailbox, the LCOS you just entered replaces the existing LCOS.)
5. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number. At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.28.6 View LCOS Information

You can view LCOS information through the System Configuration Menu or the Reports Menu.

To display all defined LCOS and the limits parameters that comprise them:

Using the System Configuration Menu

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(L) Limits COS**.
2. To view limits parameters in defined LCOS, select an option (for example, (T) Show More LCOS States), and then enter the number of the LCOS(s) you want to view (1-640) in one of the formats shown here:
3. A single LCOS **number**, for example 3
4. A range of FCOS **numbers**, for example 2-4
5. A series of FCOS **numbers**, for example, 2,4,5,12
6. **A** for a summary of all FCOS
7. **E** for a summary of even-numbered FCOS
8. **O** for a summary of odd-numbered FCOS
9. **L** for a summary of the lower half of FCOS
10. **U** for a summary of the upper half of FCOS
11. The server displays a list of all defined LCOS that shows the values set for general limits parameters contained in them.

```
LCOS to show (? for help)= 1

Max Netq Max User Callr Name Greet Max Msg Net MsgDl 1View

# Name Msgs Msgs Bill Len Len Len Len Log Sib Sib Delay Tmout

-------------------------------------------------------------------------

1 Default 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59
```

12. To view any other limits parameters, select from the following list and enter the LCOS number you want to view:
13. (U) Show Call Placement LCOS States
14. (W) Show NuPoint Fax LCOS states
15. (Y) Show Message Age Limits for Selected LCOS
16. (Z) Show Language for Selected LCOS

Using the Reports Menu

1. From the Main Menu, select **(R) Reports Menu**.
2. Select **(E) LCOS**.
3. At the output routing prompt, select one of the following:
4. **C** to send the report to the console without pausing
5. **P** to send the report to the console, pausing as the screen fills,
6. **F** to send the report to a file on the server,
7. **A** to append the report to an existing file on the server, or
8. **X** to exit report output options (no report).

```
              LIMITS
CLASS OF SERVICE
```

Wed Oct 28 13:47:08 20XX

Max Netq Max User Callr Name Greet Max Msg Net MsgDl 1View

Name Msgs Msgs Bill Len Len Len Len Log Sib Sib Delay Tmout

---

1 Default 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

2 NYNEX-Basic 200 99 0 2.0 2.0 2 2.0 0 199 199 5 59

3 NYNEX-Advanced 200 99 0 2.0 2.0 2 2.0 0 199 199 5 59

4 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

26.29 Group Class of Service - Overview

Group Class of Service (GCOS) provides a way to manage communication between mailboxes for a particular set of users. For example, if two departments need to communicate with a supervisor but not with each other, the GCOS of the supervisor needs only to contain the group numbers of the two departments. Each department's GCOS will contain only the group number of the supervisor.

GCOS usage is essential to the operation of the system, and especially for large systems with many mailbox owners, or owners who have multiple mailboxes.

NuPoint Unified Messaging supplies a default GCOS (GCOS1) that includes all groups and so allows communications between all mailboxes. You can create your own custom GCOS as required to a maximum of 32,000.

There are two types of GCOS: bitmapped and affinity.

Bitmapped GCOS

This GCOS must be defined as containing a number (up to 128) of groups. Two users can exchange messages if their GCOS has any group number in common. Bitmapped GCOS can have several groups defined, or none, allowing for a range of complexity in message exchange. Although bitmapped GCOS are more complex than Affinity, they are also much more flexible.

Bitmapped GCOS are numbered from 1-64.

Affinity GCOS

This GCOS is not defined - all mailboxes with the same Affinity GCOS can communicate with each other (but not with anyone else). Affinity GCOS works well when mailboxes require communication within particular groups but not across groups. Easier to use than bitmapped GCOS, they are also less flexible.

Affinity GCOS are numbered 65 - 32,267

Which Type of GCOS Should I Use?

When choosing GCOS, consider the following factors:

- To allow all mailboxes to exchange messages, assign the Default GCOS 1, which contains all 128 groups.
- Mailboxes with bitmapped GCOS and those with affinity group GCOS cannot interact.
- If you assign GCOS 1 to one mailbox and GCOS 65 to another, these mailboxes cannot exchange messages. If you mix the two types, one mailbox cannot communicate with another.
- Every mailbox that shares the same group in a bitmapped GCOS or shares the same affinity GCOS can exchange messages (even if the shared group is in a different GCOS).
- Bitmapped GCOS are useful when you need to develop complex relationships.
- Although mailbox owners may be in the same Dial-by-Name database, they can only reach others in the database who share the same GCOS group (in a bitmapped GCOS) or affinity group.

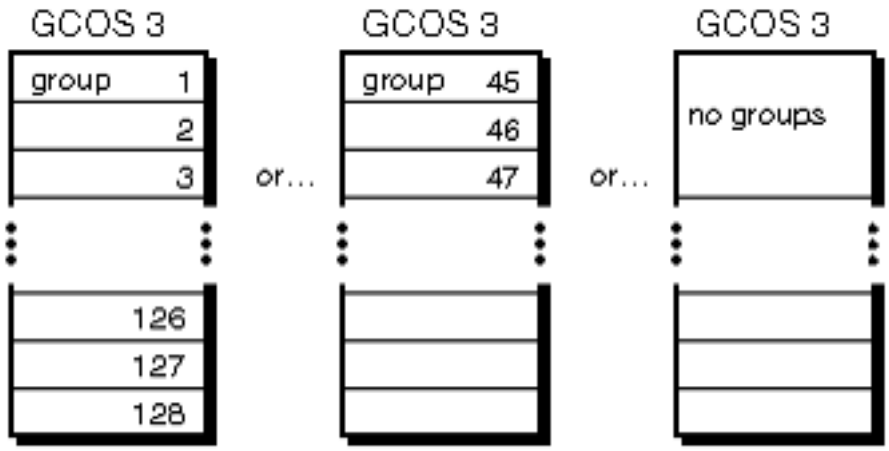
26.29.1 How a GCOS Works

There are two types of GCOS: bitmapped GCOS and affinity GCOS. Bitmapped GCOS are GCOS 1 through 64. Affinity group GCOS are GCOS 65 through 32,000. The two types work very differently, though you can mix both types in one system.

Bitmapped GCOS

A bitmapped GCOS is a collection of groups. A group is nothing more than a number from 1 through 128. Two users can exchange messages if their bitmapped GCOS have any of the same groups. To allow all users to communicate with each other, use the default GCOS 1. It contains all groups.

Figure 2 shows three possible ways to set up the same bitmapped GCOS. As the illustration shows, a bitmapped GCOS can have many groups, a few groups, or no groups defined.



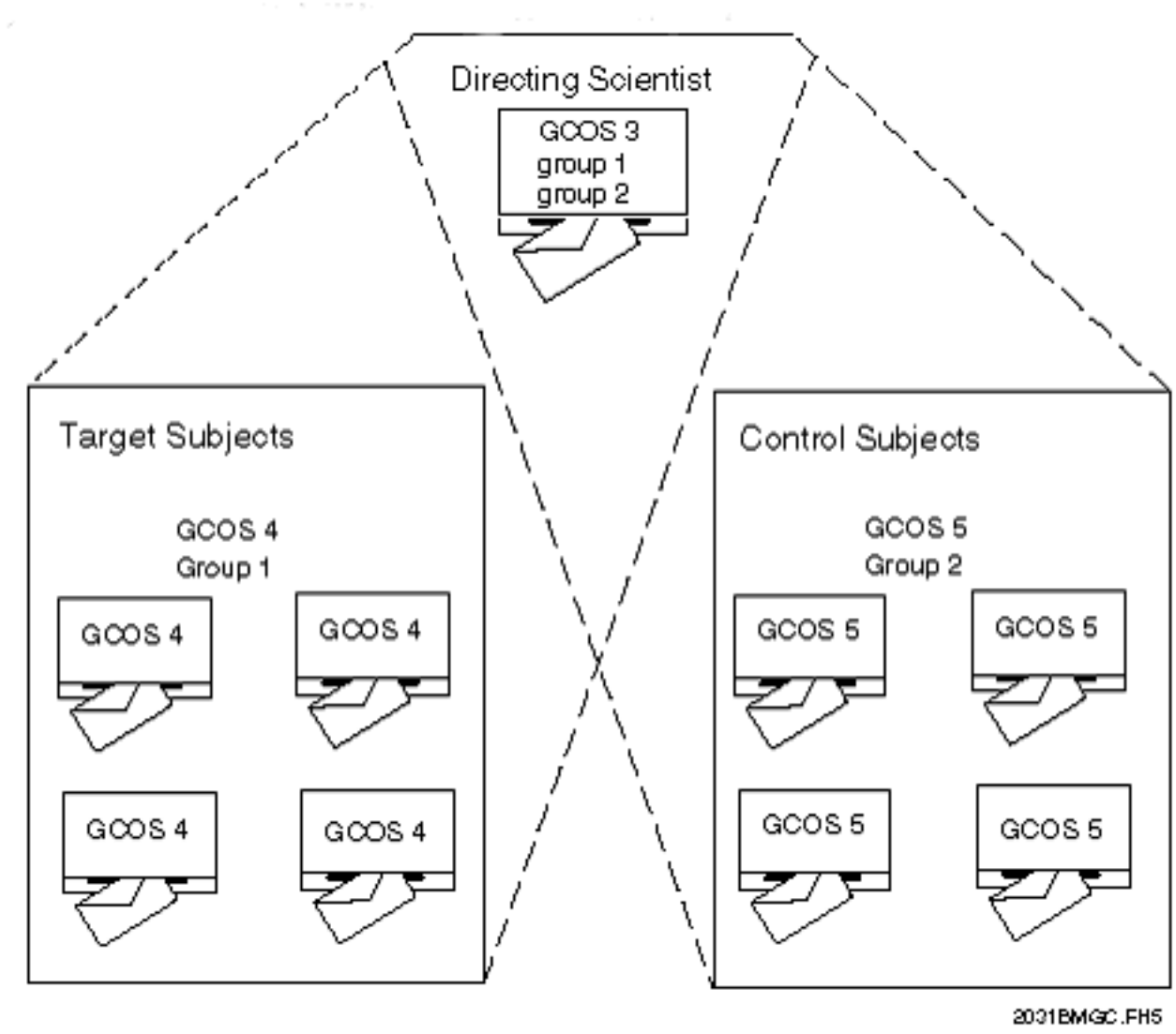
You can enable message exchange ranging from simple to complex, depending on which groups you include or exclude in bitmapped GCOS and which bitmapped GCOS you assign to mailboxes.

As an example, suppose that a scientist directs an experiment using target subjects and control subjects. The target subjects and control subjects do not communicate with each other, but both must communicate with the scientist. The scientist communicates with every subject. Using bitmapped GCOS, you can put the target subjects in a GCOS with one group, the control subjects in another GCOS with a different group, and the scientist in a third GCOS, with both groups.

For example:

Tenant	GCOS	Groups in GCOS
Directing scientist	3	1, 2
Target subjects	4	1
Control subjects	5	2

The following diagram illustrates this message exchange scheme:

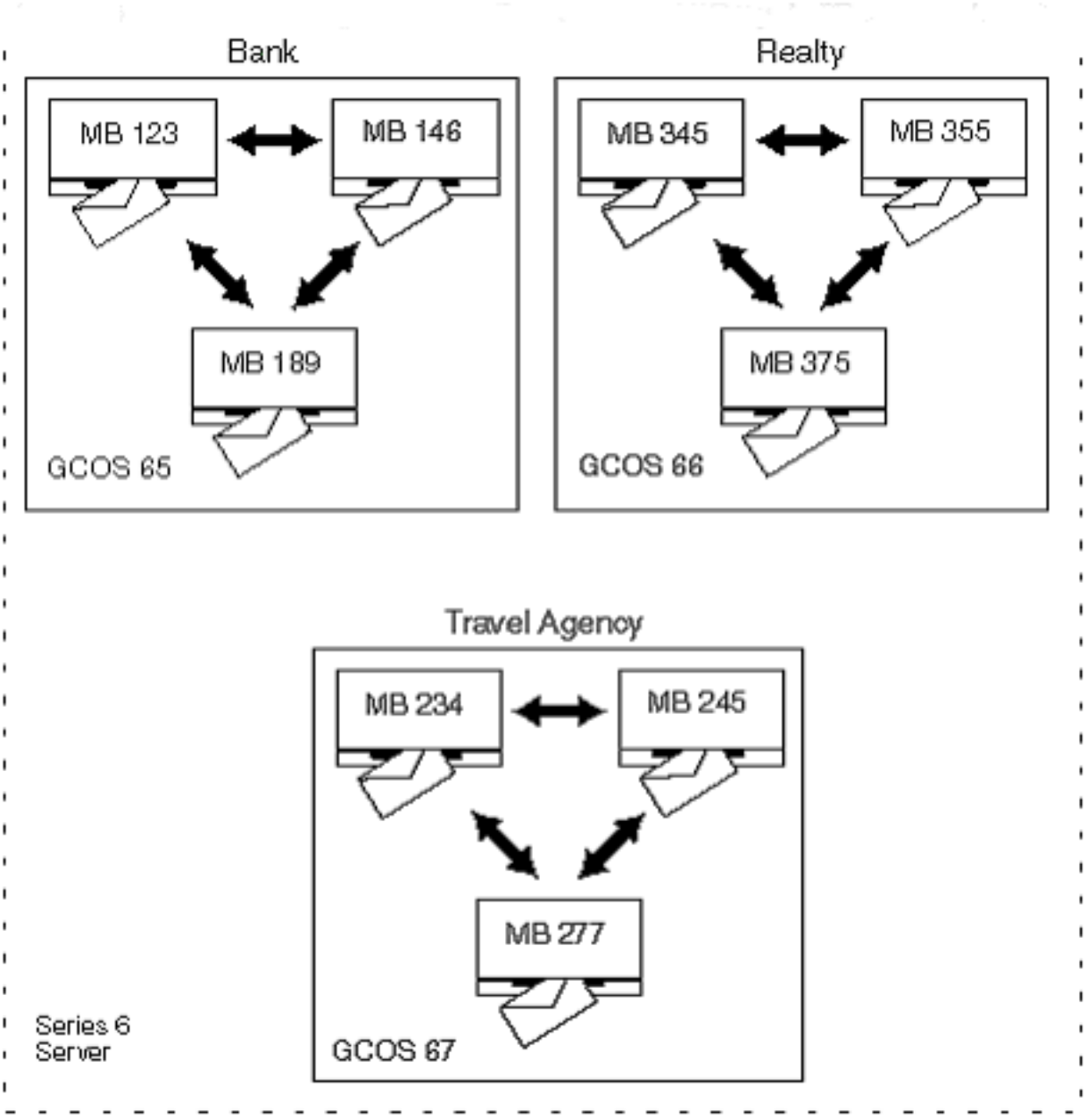


Bitmapped GCOS work well when the mailboxes in your system have different communication needs. Some mailboxes require universal communication, while others must be tightly restricted. This is the more flexible, more complex of the two methods. If you want to use a bitmapped GCOS other than default GCOS 1, you must define it before assigning it to mailboxes.

Affinity Group GCOS

Affinity group GCOS work well when mailboxes require communication within particular groups, but not across groups. This is the simpler of the two methods; all mailboxes that have the same affinity group GCOS can communicate with each other but cannot communicate with anyone else. Affinity group GCOS are never defined in the system; you simply assign one, numbered from 65 through 32,000, to mailboxes.

The example shows how affinity groups can create several communication groups within a single system.



Guidelines for Deciding Which Type of GCOS to use

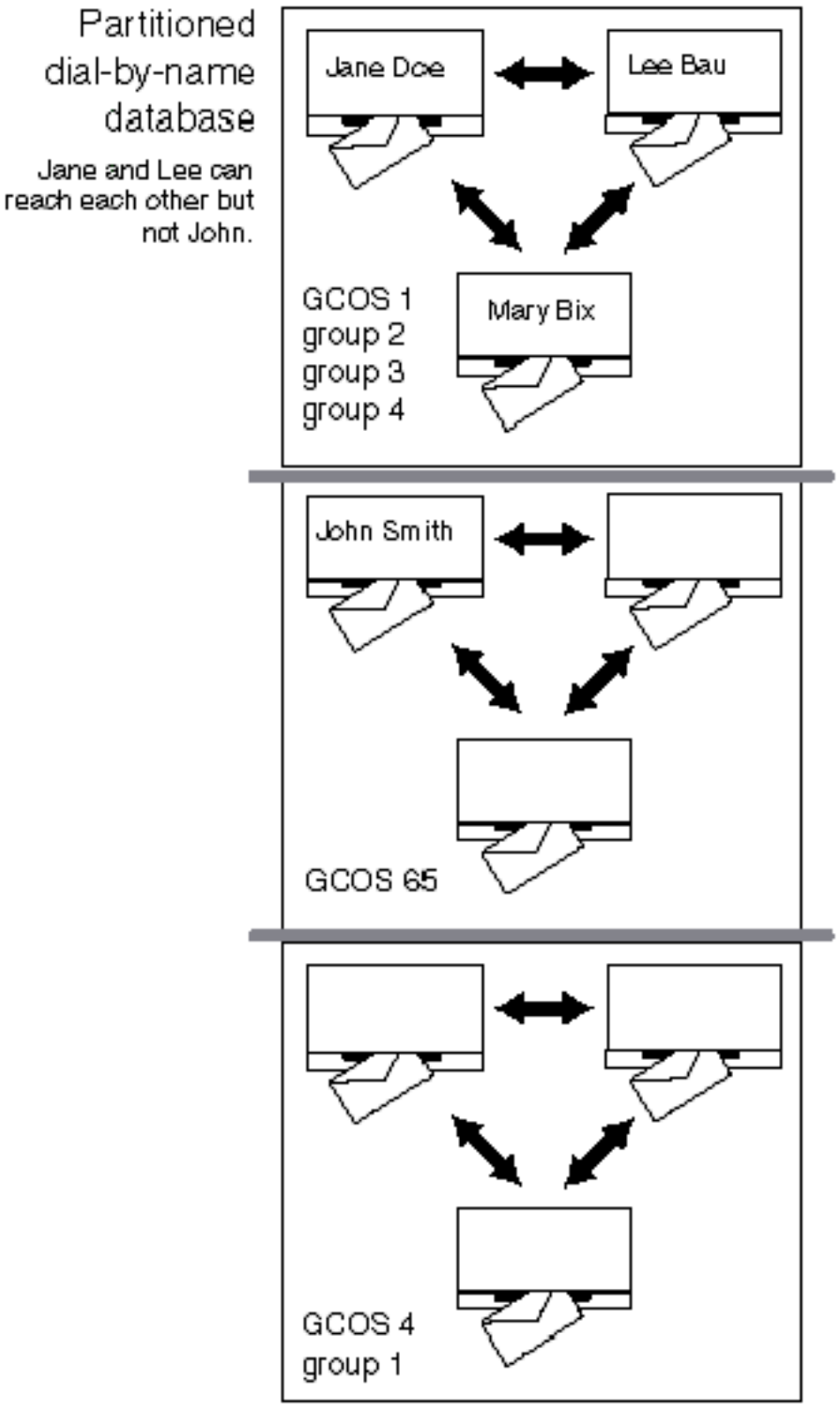
When deciding which type of GCOS to use, consider the following factors:

- If you want all mailboxes to be able to exchange messages, just assign GCOS 1, a bitmapped GCOS that contains all 128 groups.
- You can mix the two GCOS types, but mailboxes with bitmapped GCOS (numbered 1-64) cannot interact with mailboxes that have affinity group GCOS (numbered 65-32000), and no single mailbox can communicate with all the mailboxes. If you assign the bitmapped GCOS 1 to one mailbox and the affinity GCOS 65 to another, those two mailboxes cannot exchange messages.
- With bitmapped GCOS, every mailbox that shares the same group can exchange messages, even if the shared group is in a different bitmapped GCOS.

- Bitmapped GCOS are useful when you need to develop complex relationships. The communication links required for the arrangement shown below, for example, are possible only with a bitmapped GCOS.

Dial-by-Name Considerations

Even though mailbox owners may all be in the same Dial-by-Name database, they can only reach others in the database if they share either the same affinity group or if their bitmapped GCOS have any of the same groups. For example, Jane Doe, Lee Bau, and John Smith are all in the Dial-by-Name database, but Jane's mailbox and Lee's mailbox are configured with GCOS 1, a bitmapped GCOS, and John's mailbox is configured with GCOS 65, an affinity group GCOS. Jane and Lee can reach each other but not John. This grouping, sometimes called "Partitioned Dial-by-Name," is illustrated in the figure below.



Jane and Lee can be in different bitmapped GCOS but can still communicate if both GCOS include each of their group numbers.

Interaction Between FCOS and GCOS

Interaction between mailboxes is limited by the GCOS and FCOS that are assigned to them. If, for example, an FCOS allows a user to make confidential messages (feature bit 023), other users within the same GCOS must be able to receive messages from other users (feature bit 040), and to play messages (050). Otherwise, the make confidential message feature is useless.

Recommendations for GCOS Flexibility

By default, GCOS 1 has all 128 groups defined, giving a mailbox with this GCOS the maximum flexibility in exchanging messages. It is recommended that you do not alter this GCOS.

It is also recommended that you create GCOS 2, but define no groups for it. This “empty” GCOS is useful in restricting the capabilities of a mailbox. It is also used to enable one-way communication, as described in One-Way Communication Using an Empty GCOS.

26.29.2 One-Way Communication Using an Empty GCOS

You can prevent contact between users, but you can also allow them to receive certain kinds of messages, using an empty GCOS. For example, you probably want to notify all users before a system shutdown. The empty GCOS is one that is assigned a name and number but no groups.

To enable this one-way communication, the originating (or sending) mailbox must have an FCOS that allows it to make messages and also allows the mailbox owner to make or give (messages) to a mailbox with an empty GCOS. The FCOS feature bits to accomplish this are:

- 020 (Make messages)
- 126 (Make/give to mailbox with empty GCOS)

The receiving mailbox must also have an FCOS that allows it to receive messages from other users (FCOS bit 040). These features enable a user to make a message, as well as give messages from other users, to the mailbox with the empty GCOS.

For example, suppose the local phone company notifies an answering service that maintenance on buried phone cables will disrupt service for two hours next week. If all customers have mailboxes with the FCOS and empty GCOS just described, and if the system administrator’s mailbox has the same FCOS, then the system administrator can use one-way communication to notify users in advance of the system shut down.

To use an empty GCOS and feature bits to enable one-way communication from one set of mailboxes to another:

1. Customize an FCOS to assign to the **originating** mailbox (the mailbox that sends the one-way messages), that includes the following feature bits:
   - **020** (Make messages)
   - **126** (Make/give to mailbox with empty GCOS)
2. Customize the FCOS assigned to the **receiving** mailbox to include feature bit **040** (Receive messages from other users).
3. Assign an empty GCOS to the receiving mailbox.

26.29.3 Managing GCOS

GCOS is mainly used when a single NuPoint Unified Messaging system serves more than one company and you want to prevent people belonging to different companies from sending messages to each other.

You can:

- List GCOS
- Add a GCOS
- Edit a GCOS
- Delete a GCOS
- Assign a New GCOS to a Mailbox
- See a Description of GCOS fields

Listing GCOS

To display a list of all GCOS in the system

- In the navigation tree, click Class of Service, and then click Group COS.

Add a GCOS

1. In the navigation tree, click Class of Service, and then click Group COS. The Group COS list is displayed.
2. Click Add. The Add GCOS form is displayed.
3. Do one of the following:

   - Copy an existing GCOS by selecting one from the list and clicking the **Copy from** button. The parameters of that GCOS will be copied into your new GCOS, which you can then edit as required. The Next Available GCOS number is automatically applied.

     OR
   - Chose to manually select all limits for the new GCOS
4. In the **Number** field, enter a **number** for this COS, or click **Next Available** to automatically assign the next number.
5. In the **Name** field, enter a **name** (up to 15 alphanumeric characters) for this GCOS.
6. From the Groups listing, select all groups that will be included in this GCOS.
7. To save the GCOS and return to the Group COS list, click Save.

Edit a GCOS

1. In the navigation tree, click Class of Service, and then click Group COS. The Group COS list is displayed.
2. Select the GCOS you want to modify and then click **Edit**.
3. Select or clear group check boxes as required.
4. To save the GCOS and return to the Group COS list, click Save.

Delete a GCOS

Deleting a GCOS that is in use by mailboxes will cause all of those mailboxes to be assigned the default (1) GCOS. A warning message is displayed to allow you to cancel the operation. If you are deleting the default GCOS, the mailboxes assigned to it will be assigned to the next available GCOS. You cannot delete the last remaining GCOS in the system; therefore, you cannot select all GCOS for deletion.

Note: At any time during the deletion of a GCOS (but before you confirm the deletion), you can click the Cancel button to discard your changes and return to the Group COS list.

To delete one or multiple GCOS

1. In the Group COS list, select one or multiple GCOS, and then click Delete. The system will prompt you to confirm the deletion.
2. To confirm the deletion, click Yesfor a single deletion or Yes to allfor a range.

   OR

   To reject the deletion, click No.

Assign a New GCOS to a Mailbox

- Follow the procedure to edit a mailbox and when instructed to edit mailbox parameters, enter the new GCOS on the Class of Service tab.

GCOS Fields Description

Field	Description	Values
Number	*Required field. Determines the number of the new GCOS. You can manually enter a number from 1-64 as long as it is not already assigned to a GCOS. You can also click the "Use next available number" link to have the system assign the next available number to the GCOS.	Enter a number in the range of 1-64. The number must not be already used for an existing GCOS. Or click the "Use next available number" link.

Field	Description	Values
Name	*Required field. This is the name of the GCOS. (**Note**: You can create unnamed GCOS using the Text console but they are not supported in the Web console. If you encounter an unnamed GCOS, use the Text console to name it.)	Maximum 15 alphanumeric characte rs.
(Group numbers)	Select the groups (by number) that y ou want to include in the GCOS. Mail boxes that are assigned this GCOS will be members of the groups that you select here. There are 128 grou ps.	Select any combination of groups fr om 1 to 128.

26.29.4 Define a Bitmapped GCOS

Defining a new GCOS consists of assigning:

- a number (of the new GCOS you are defining, or an existing GCOS you are modifying. We recommend that you do NOT modify the default GCOS1.) Bitmapped GCOS are numbered 1-64. Affinity GCOS are numbered 65-32267.
- a name (a descriptive name up to 15 alphanumeric characters. Not required for Affinity GCOS.)
- the required groups (all groups to include in this GCOS. Affinity GCOS does not contain groups.)

To define a bitmapped GCOS: (You can use this procedure to define a new GCOS or to modify an existing GCOS.)

1. Complete a GCOS Worksheet. (See a sample worksheet.)
2. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(G) Group COS**.
3. Select **(C) Current GCOS** and enter the **number** (1-64) of the bitmapped GCOS you are defining.
4. Select **(N) Name GCOS** and enter a descriptive **name for the new** GCOS.

5. Select **(A) Add Group** and then enter the one- to three-digit **numbers** of all groups that comprise this GCOS in one of the following formats:

   - A single group, for example, 3
   - A range of groups, for example, 1-128
   - A series of groups, for example, 3,4,6,7
   - **L** to specify the lower half (1-64)
   - **U** to specify the upper half (65-128)
   - **A** to specify all group numbers
   - **E** to specify even group numbers
   - **O** to specify odd group numbers

   You can mix types of entries, so you can specify all the bits necessary in one attempt. For example, this entry is valid: 1,3,4-19,U. Do not enter spaces after commas, and do not end the entry with a comma.
6. If necessary, you can delete groups from the GCOS by selecting (D) Delete Group and entering the group **number(s)** to delete. Use the same format as for adding groups.
7. To verify that the information you have entered matches your worksheet, select (S) Show GCOS and enter the GCOS number.
8. When you are finished defining the GCOS, save it by exiting from the Group Class of Service Menu.
9. Copy the number of this defined GCOS from your GCOS worksheet to the appropriate mailbox worksheet.

26.29.5 Modify a Bitmapped GCOS Group

This procedure describes how to modify a bitmapped GCOS by adding or deleting groups.

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(G) Group COS**.
2. Select **(C) Current GCOS** and then enter the **n umber** of the bitmapped GCOS (1-64) you want to modify, or press **Enter** if the displayed GCOS is correct.
3. At the **Enter GCOS name** prompt, enter a descriptive name for the GCOS (up to 15 characters), or press **Enter** if the displayed name is correct.
4. Select **(A) Add Group** or **(D) Delete Group**, as required, and then enter the Group **number(s)** to add or delete (1-128) in one of the following formats:

   - A single group, for example 7
   - A continuous range of groups, for example 2-7
   - A series of groups, for example 1,2,6,7
   - You can mix types of entries, so you can specify all the groups necessary in one attempt. For example, this entry is valid: 1-4,8,9,12. Do not enter spaces after commas, and do not end the entry with a comma.

26.29.6 Assign a GCOS to a Mailbox

Before you can assign a bitmapped GCOS, you must define its parameters.

To assign a bitmapped or affinity group GCOS to a mailbox configuration.

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** and enter the *n*umber of the new mailbox you want to configure.

   OR
3. Select **(M) Modify Mailboxes** and enter a mailbox number to modify an existing mailbox.
4. Press **Enter** until the **Group Class of Service** or **New GCOS** prompt appears and then enter **number** of the bitmapped GCOS (1-64) or affinity group GCOS (65-32,000) that governs this mailbox. (If you are modifying a mailbox, the GCOS you just entered replaces the existing GCOS.)
5. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.29.7 View GCOS Information

You can view GCOS information through the System Configuration Menu or the Reports Menu.

Using the System Configuration Menu

To display a li*st* of defined bitmapped GCOS:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(G) Group COS**.
2. Select **(S) Show GCOS** and then enter *t*he number(s) of the GCOS(s) you want to view in any of these formats:

   - A single GCOS **number**, for example 3
   - A range of GCOS **numbers**, for example 3-6
   - A series of GCOS **numbers**, for example, 3,4,5,12
   - **E** for a summary of even-numbered GCOS
   - **O** for a summary of odd-numbered GCOS
   - **L** for a summary of the lower half of GCOS (1-32)
   - **U** for a summary of the upper half of GCOS (33-64)
   - **A** for a summary of all GCOS

```
GCOS to show (? for help) = 1,2

GCOS: Default GCOS 1 : 1

001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019 020

021 022 023 024 025 026 027 028 029 030 031 032 033 034 035 036 037 038 039 040

041 042 043 044 045 046 047 048 049 050 051 052 053 054 055 056 057 058 059 060

061 062 063 064 065 066 067 068 069 070 071 072 073 074 075 076 077 078 079 080

081 082 083 084 085 086 087 088 089 090 091 092 093 094 095 096 097 098 099 100

101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120

121 122 123 124 125 126 127 128

GCOS: Contractors : 2

001 007 009 013 041 056 099
```

Using the Reports Menu

1. From the Main Menu, select **(R) Reports Menu**.
2. Select **(G) GCOS**.
3. At the output routing prompt, select one of the following:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills,
   - **F** to send the report to a file on the server,
   - **A** to append the report to an existing file on the server, or
   - **X** to exit report output options (no report).

GROUP CLASS OF SERVICE

Thu Oct 29 09:15:23 2009

GCOS: Default GCOS 1 : 1

001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019 020

021 022 023 024 025 026 027 028 029 030 031 032 033 034 035 036 037 038 039 040

041 042 043 044 045 046 047 048 049 050 051 052 053 054 055 056 057 058 059 060

061 062 063 064 065 066 067 068 069 070 071 072 073 074 075 076 077 078 079 080

081 082 083 084 085 086 087 088 089 090 091 092 093 094 095 096 097 098 099 100

101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120

121 122 123 124 125 126 127 128

GCOS: Contractors : 2

001 007 009 013 041 056 099

26.30 Restriction Class of Service - Overview

The Restriction Class of Service (RCOS) acts to restrict system outdials. Restrictions can be programmed by number of digits to dial (for example, a limit of 7 digits effectively restricts long-distance calling), by screening for certain area codes and Central Office codes, using NPA/NXX screening.

NPA/NXX Screening

NPA (or Numbering Plan Area) is the 3 digit code in a telephone number that represents the area. (For example, one area code for Ottawa is 613.) The NXX digits represent the Central Office or exchange that is assigned to the CO that serves this telephone number. (For example, the NXX digits for the CO that serves Mitel are 592.)



26.30.1 Managing RCOS

You can

- List RCOS
- Add an RCOS
- Edit an RCOS
- Delete an RCOS
- Assign a New RCOS to a Mailbox
- See a list of RCOS Fields Description

List RCOS

To display a list of all RCOS on the system

- In the navigation tree, click Class of Service and then click Restriction COS.

Add an RCOS

1. In the navigation tree, click Class of Service and then click Restriction COS. The Restriction COS list is displayed.
2. Click Add. The Add RCOS form is displayed.
3. Do one of the following:

   - Copy an existing RCOS by selecting one from the list and clicking the **Copy from** button. The parameters of that RCOS will be copied into your new RCOS, which you can then edit as required. The Next Available RCOS number is automatically applied.

     OR
   - Chose to manually select all limits for the new RCOS
4. In the **Number** field, enter a **number** (1-64) for this RCOS, or click **Next Available** to automatically assign the next number.
5. In the **Name** field, enter a **name** (up to 15 alphanumeric characters) for this RCOS.
6. In the drop-down list, select any of the RCOS properties and configure the parameters that are associated with the properties (see RCOS Fields Description).
7. To save the RCOS and return to the Restriction COS list, click Save.

Edit an RCOS

You can edit any RCOS data except for the RCOS number.

1. In the navigation tree, click Class of Service and then click Restriction COS. The Restriction COS list is displayed.
2. Select an RCOS to modify, and click Edit. The Edit RCOS form is displayed.
3. Modify RCOS data as required. For information about the RCOS data fields, see RCOS Fields Description.
4. To save the RCOS and return to the Restriction COS list, click Save.

Delete an RCOS

Deleting an RCOS that is in use by mailboxes causes all of those mailboxes to be assigned the default (1) RCOS. A warning message is displayed to allow you to cancel the operation. If you are deleting the default RCOS, the mailboxes assigned to it will be assigned to the next available RCOS. You cannot delete the last remaining RCOS in the system; therefore, you cannot select all RCOS for deletion.

To delete one or multiple RCOS:

1. In the Restriction COS list, select one or multiple RCOS, and then click Delete. The system will prompt you to confirm the deletion.
2. To confirm the deletion, Yesfor a single deletion or Yes to allfor a range.

   OR

   To reject the deletion, click No.

Assign a New RCOS to a Mailbox

- Follow the procedure to edit a mailbox and when instructed to edit mailbox parameters, enter the new RCOS on the Class of Service tab.

RCOS Fields Description

Fields	Description	Values
Number	*Required field. Determines the number of the new RCOS. You can manually enter a number from 1-64 as long as it is not already assigned to an RCOS. You can also click the Next Available button to have the system assign the next available number to the RCOS.	Enter a number in the range of 1-64. The number must not be already used for an existing RCOS. Or click the Next Available button.

Fields	Description	Values
Name	*Required field. This is the name of the RCOS. (**Note**: You can create unnamed LCOS using the Text console but they are not supported in the Web console. If you encounter an unnamed LCOS, use the Text console to name it.)	Maximum of 15 alphanumeric characters.
(RCOS properties drop-down list)	RCOS properties are organized in to four categories. You select a category from the drop-down list to modify the limits that are associated with this category, as displayed in the following figures.	Select one of the following four categories: • Absorption Table This table can contain up to 16 entries of up to 10 digits each. NPA must be a 3-digit number. • Exact Match Table This table can contain up to 100 25-digit entries. • System-wide RCOS settings Enter the starting and ending digit position for NPA and NXX • NPA/NXX The NPA table can contain all 999 possible 3-digit numbers (except "000"). Each 3-digit string can only be added once it is in the NPA table. For each NPA entry, you can define up to 999 NXX entries, using a similar table. Selecting an NPA in the NPA table will automatically fill the NXX table with the corresponding NXX entries. The NPA and NXX starting and ending digit positions must be digits from 0-25.

26.30.2 Configure an RCOS

You must configure the RCOS System-wide parameters before you can use an RCOS.

To configure an RCOS:

1. Complete an RCOS Worksheet. (Blank worksheets are here.)
2. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(M) Restriction COS**.
3. Select **(A) Select RCOS** and enter the **n umber** (1 through 64) of the RCOS group to be modified.
4. Select **(M) Modify Selected RCOS**.
5. Select **(N) Name of Selected RCOS** and enter a descriptive **name** (up to 15 characters)
6. Select **(H) Home NPA** and enter the **n umber** of the NPA (1- to 3-digit number representing area code).
7. Select **(C) Check Numbers Which Do Not Have Absorb Digits** and enter **Y** to continue screening the numbers, or **N** to skip screening and allow call placement unconditionally.
8. Select **(M) Modify Digit Absorption Table** if you need to specify digits to be absorbed. (Refer to your RCOS worksheet.)
9. Select **(A) Add a number** and enter the number to be absorbed in one of the following formats:

   - a single pattern (for example 91)
   - a series of patterns separated by commas (for example, 91,1,102880). Do not enter spaces after the commas and do not end the entry with a comma.
10. Press **Enter** to exit the add menu and then press **(X)** to exit the Absorb menu.
11. In the Modify RCOS menu, select **(A) Set Exact Match Numbers to Allow/Disallow** if you want to set up an Exact Match database:
12. Enter **A** to allow these numbers or **D** to disallow them.
13. Select **(E) Modify Exact Match Table**.
14. Select **(A) Add a number** and enter the **number** to be matched against. Number patterns can be entered in the following formats:

    - A single pattern, for example, 5551212,
    - A series of patterns, for example, 911,411. Do not enter spaces after commas and do not end the entry with a comma.
    - Press **Enter** to exit the add menu and then press **(X)** to exit the **Exact Match** menu.
15. In the Modify RCOS menu, select **(S) Set NPA Screening to Allow/Disallow** if you want to set up an NPA Database.
16. Enter **A** to allow these numbers, or **D** to disallow them.
17. Select **(T) Modify NPA/NXX Table**.
18. Select **(P) Select NPA** and enter the **number** of the NPA to add.
19. Select **(A) Add NPA**. The system confirms the addition.
20. Select (**N) Add NXX** if you want to set up an NXX Database.
21. Select **(B) Set NXX Screening to Allow/Disallow** and enter **A** to allow these numbers, or **D** to disallow them.
22. Select **(X)** to exit the NPA/NXX menu.
23. You can verify your changes using the instructions to View RCOS Information.
24. Exit the Restriction Class of Service Menu to make the changes take effect.
25. Copy the number of this RCOS from your RCOS Worksheet to the appropriate mailbox worksheet.

26.30.3 Set RCOS System-Wide Parameters

To enter the starting and ending NPA (area code) and NXX (three-digit prefix) digit positions:

1. Complete an RCOS worksheet.
2. • From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(M) Restriction COS**, and then **(D) Define System Wide Parameters.**
3. • Count an example dial string your server can use to locate the starting and ending digit positions for the NPA (area code) and the NXX (three-digit prefix). For example, the settings for a North American ten-digit phone number are:
   - The starting NPA digit position is 10
   - The ending NPA digit position is 8
   - The starting NXX digit position is 7
   - The ending NXX digit position is 5
4. Select **(A) Starting Digit Position of NPA** and enter the **n umber** of the digit position at the start of the NPA.
5. Select (**B) Ending Digit Position of NPA** and enter the **n umber** of the digit position at the end of the NPA.
6. Select **(C) Starting Digit Position of NXX** and enter the **n umber** of the digit position at the start of the NXX.
7. Select **(D) Ending Digit Position of NXX a**nd enter the **n umber** of the digit position at the end of the NXX.
8. Exit the RCOS menu to save your settings.

26.30.4 Modify the Absorption Table

To add or remove dial strings from the absorption table:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(M)Restriction COS**, **(M) Modify selected RCOS**, and then **(M) Modify Digit Absorption table**.
2. Select **(A) Add a number** and enter the number to be absorbed, (OR select **(R) Remove a number** to remove one) in one of the following formats:

   - a single pattern (for example 91)
   - a series of patterns separated by commas (for example, 91,1,102880). Do not enter spaces after the commas and do not end the entry with a comma.
3. To verify your changes, select **(S) Show Table**. The system displays your table.
4. Exit the RCOS Menu to save your changes.

26.30.5 Modify the Exact Match Table

To add or remove dial strings from the exact match table:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(M) Restriction COS**, **(M) Modify selected RCOS**, and then **(E) Modify Exact Match table**.

2. Select **(A) Add a number** and enter the **number** to be matched against (OR select **(R) Remove a number**to remove one). Number patterns can be entered in the following formats:

   - A single pattern, for example, 5551212,
   - A series of patterns, for example, 911,411. Do not enter spaces after commas and do not end the entry with a comma.
3. To verify your changes, select **(S) Show Table**. The system displays your table and options.
4. Exit the RCOS Menu to save your changes.

26.30.6 Modify NPA/NXX Tables

To make changes to the NPA (area code) and NXX (3-digit prefix) tables.

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(M) Restriction COS**, **(M) Modify selected RCOS**, and then **(T) Modify NPA/NXX Table**.
2. Select **(P) Select NPA** and enter the **number** of the NPA to add.

   - If you are creating the NPA, select **(A) Add NPA**.
   - If you are deleting the NPA, select **(R) Remove NPA**.
   - The system confirms the modification.
3. To create/modify an associated NXX table, if necessary, select **(N) Add NXX** and enter the **n umber(s)** of prefix(es) to be added. NXX numbers can be entered in the following formats:

   - A single pattern, for example 252
   - A series of patterns, for example 252,428,354. Do not enter spaces after commas and do not end the entry with a comma.
4. To remove prefixes that you no longer need screened, select **(D) Remove NXX** and enter the number(s) of prefix(es) to be removed.
5. Select **(B) Set NXX Screening to Allow/Disallow** and **A** for Allow, or **D** for disallow.
6. To verify your changes, select **(S) Show Table**. The system displays your table and options.
7. To add another NPA, repeat this process starting from step 2.
8. Exit the RCOS Menu to save your changes.

26.30.7 Assign an RCOS to a Mailbox

To assign an RCOS to a mailbox configuration:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** and enter the *n*umber of the new mailbox you want to configure.

OR

1. Select**(M) Modify Mailboxes**to modify an existing mailbox.

Note:
Prompts are almost the same for creating a new mailbox and modifying an existing one, except that "New" precedes a prompt when you select Modify Mailboxes.

2. Press **Enter** until the **Restriction Class of Service** or **New RCOS** prompt appears and then enter the **number** of the RCOS (1 through 64) configured for the outcall capabilities for this mailbox. If you are modifying a mailbox, the RCOS you just entered replaces the existing RCOS.

1. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number. At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.30.8 View RCOS Information

You have a choice of information levels to view:

- System-wide parameters, which includes a list of configured RCOS and their names
- Home NPA and screening settings for a specific RCOS
- Configuration of a specific RCOS
- Configuration of all RCOS

Viewing System-Wide Parameters

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(M) Restriction COS**.
2. Select **(P) Show System Wide Parameters**. The server displays a list of the defined RCOS with their names at the server maintenance console, followed by the system-wide parameters.

Viewing Home NPA and Screening Settings for a Selected RCOS

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(M) Restriction COS**.
2. Select **(A) Select RCOS** and enter the **n umber** (1 through 64) of the RCOS to view.
3. Select **(S) Show Selected RCOS**. The server displays the home NPA, whether numbers without digits to be absorbed are checked, whether exact match numbers are allowed, and whether NPA screening is allowed, for the selected RCOS.

Viewing the Configuration of a Specific RCOS

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(M) Restriction COS**.
2. Select **(A) Select RCOS** and enter the **n umber** (1 through 64) of the RCOS to view.

3. Select **(R) Report Selected RCOS**. The server displays the following information about the current RCOS:

   - Home NPA
   - Whether numbers without absorb digits are checked
   - Whether exact match numbers are allowed or disallowed
   - Whether NPA screening is allowed or disallowed
   - Digit absorption table
   - Exact match table
   - NPA/NXX table

Viewing the Configuration of All RCOS

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(M) Restriction COS**.
2. Select **(T) Report All RCOS**. The server displays a report of all the defined RCOS with all of their parameter settings.
3. If you are displaying it at the console, use the following commands to control scrolling:

   - To stop scrolling: Press **Ctrl-S**
   - To restart scrolling: Press **Ctrl-Q**

26.30.9 Sequence of NPA/NXX Screening

Without NPA/NXX call screening, the system restricts outdials only by the number of digits to be dialed. With NPA/NXX call screening, the system restricts the outdial capabilities for a mailbox by allowing calls to be made only to certain area codes or to certain prefixes within an area code.

The system prioritizes the screening process in the following manner:

1. Removes the absorption digits (numbers at the beginning of the dial string that allow access to outside lines) from the dialing string prior to the screening process. These numbers were entered in the Digit Absorption Table, one of the RCOS menus.
2. Compares the number called to the Exact Match Table, one of the RCOS menus, which specifies whether the number is allowed or disallowed. The first table shows the screening method.
3. Counts the remaining number of digits. If the dial string does not contain an NPA (area code), it adds the home NPA.
4. If the system does not receive an exact match for the dial string, it then continues with the NPA/NXX screening.
5. Passes the NPA to the NPA Table, one of the RCOS menus, and determines if the area code is allowed or disallowed. The second table shows the screening method.
6. If the NPA contains an NXX Table, another RCOS menu, the system disregards the selection of the allow or disallow status for the area code. The determination of whether to allow the call is based only on whether the prefix is allowed or disallowed in the NXX Table.
7. Screens the number with the NXX table. The third table shows the screening method.
8. Allows the number or notifies the mailbox owner that the number is not within the mailbox owner's calling area.

Exact Match Number Table		
Is the number in the table?	**If the table is to allow the call, the system...**	**If the table is to disallow the call, the system...**
Yes	Allows the call	Blocks the call
No	Blocks the call	Allows the call

NPA Table		
Is the NPA in the table?	If the table is to allow the call, the s ystem...	If the table is to disallow the call, the system...
Yes	Checks for NXX table. If no NXX tab le exists, places the call.	Blocks the call
No	Blocks the call	Checks NXX table. If no NXX table e xists, places the call.

NXX Table		
Is the NXX in the table?	**If the table is to allow the call, the system...**	**If the table is to disallow the call, the system...**
Yes	Allows the Call	Blocks the Call
No	Blocks the Call	Allows the Call

26.30.10 Screening Examples

Several configuration examples are offered here to show how the RCOS works. If you were to configure an RCOS as shown in the table, the system would process dial strings as shown in the following examples.

Example Configuration	
Parameter	**Value**
Home NPA	408
Starting digit position of NPA	10
Ending digit position of NPA	8
Starting digit position of NXX	7
Ending NXX digit position of NXX	5
Digits to be absorbed	9,1,91
Exact match table is set to disallow	5551212,411
NPA table is set to allow	408,415,510
NXX table for the NPA 408 is set to disallow	662,684,728

If a dial string is 914084283558, the system:

1. Removes the 91 in accordance with the absorption table.
2. Compares to the exact match table and finds no match.
3. Compares the NPA 408. Because the NPA 408 has an associated NXX table, it is used.
4. Places the call because the NXX table is a disallow table and does not contain the prefix 428.

If a dial string is 2551234, the system:

1. Compares to the exact match table.
2. Adds the home NPA.
3. Compares the NPA 408. Because the NPA 408 has an associated NXX table, it is used.
4. Places the call because the NXX table is a disallow table and does not contain the prefix 255.

If a dial string is 14154244567, the system:

1. Removes the 1 in accordance with the absorption table.
2. Compares to the exact match table.
3. Compares the NPA 415. Because the NPA 415 has an associated NXX table, it is used.
4. Blocks the call because the NXX table is a disallow table and contains the prefix 424.

If a dial string is 95551212, the system:

1. Removes the 9 in accordance with the absorption table.
2. Compares to the exact match table and blocks the call because the number matches and the table is a disallow table.

If a dial string is 15102265678, the system:

1. Removes the 1 in accordance with the absorption table.
2. Compares to the exact match table.
3. Compares the NPA 510. Places the call because the NPA 510 does not have an associated NXX table and the NPA table is set to allow.

As the preceding examples show, NPA/NXX call screening works well for domestic outdials. For restricting international outdials, the best method is to limit the number of digits that can be dialed to less than the length of an international telephone number. Do this with an LCOS that includes any of these limits parameters, as appropriate:

- NP WakeUp – Phone Length
- Maximum Number of Digits for Telephone Number
- Message Delivery – Phone Length
- Message Phone Length
- Paging – Phone Length

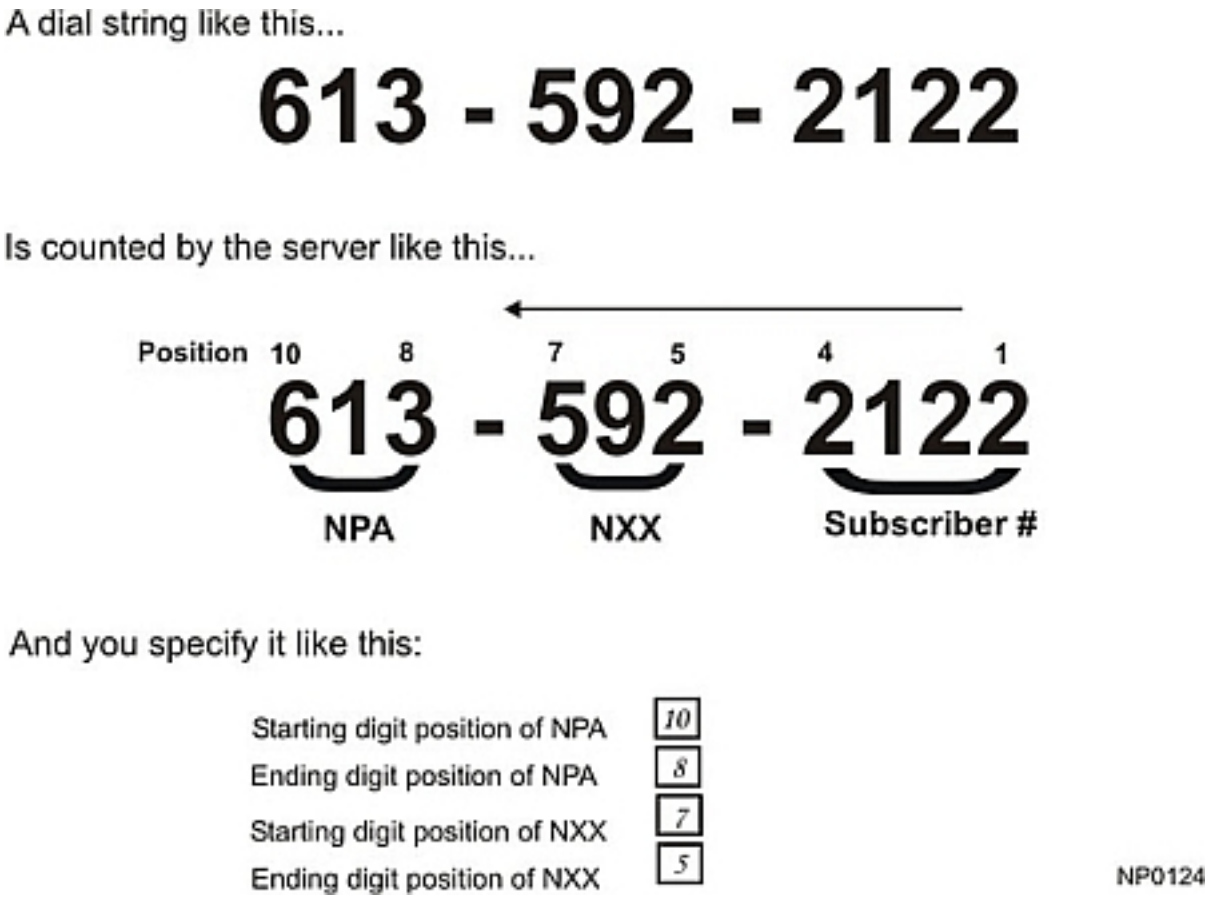
Then assign this LCOS to the desired mailboxes. Refer to the Limits Class of Service section for information about LCOS configuration.

26.30.11 RCOS Worksheet Configuration

Organize the data you need to configure an RCOS using an RCOS Worksheet. The worksheet will help you set the parameters in the RCOS menu. The areas of the worksheet are described in detail below.

To configure an RCOS using the RCOS worksheet:

1. Identify the RCOS with a number from 1 through 64 and enter this number in the “RCOS to modify” box of the worksheet.
2. You have the option of naming the RCOS to easily identify it; you can enter up to 15 characters in the “RCOS name” box on the worksheet.
3. In the **System Wide Parameters** section, you define the NPA/NXX starting and ending positions that will apply to all RCOS. Any change you make here will affect the entire system. When specifying digit positions, be aware that the system counts the positions from right to left as shown here:



4. In the RCOS-specific section, you will define parameters that provide the following calling capabilities:
5. Home NPA: Because a system can connect to foreign exchange trunks, you must specify the “local” NPA for each RCOS. If a dial string does not contain an NPA, this number is added for the screening process. The system can accept a number of up to three digits for the NPA.
6. Digits to be Absorbed: Many calls contain numbers at the beginning of the dial string that allow access to outside lines, international calling, or pager systems. You must remove these numbers before the actual screening process can begin. Numbers entered in the Absorption Table are removed from the dial string before the screening process occurs. If the dial string does not contain any digits to be absorbed, there is an option to skip the balance of the call screening process. This facilitates outdial placement to other mailboxes on the system. The system absorbs the longest matching string in the absorption table from the dial string starting from the first digit. The table capacity is 16 patterns, with a maximum of 10 digits per pattern.
7. Exact Match Numbers Database: You can enter numbers in the exact match database and specify if they are to be allowed or disallowed. The table capacity is 100 patterns, with a maximum of 25 digits per pattern. Entries to this database should include common numbers that you donotwant used for message addressing. Such numbers include 911, 411, 5551212, and 0.

8. NPA Database: The NPA database contains area codes that are screened. You can configure the database to either allow or disallow access to specific area codes. For example, you can restrict the mailbox to only the local NPA or restrict access to NPAs such as 900 numbers.

   It is possible to restrict outdial access to only one NPA by setting the NPA allow/disallow status to allow and creating an NPA table with only one NPA entry. Remember that if you want to set any outdial restrictions for the home NPA, you must enter that NPA in the table.
9. NXX Database: After you specify an NPA, the system asks if you want NXX screening for the specific NPA. You must also set the allow/disallow status for the NXX field. The NXX allow or disallow setting takes priority over the NPA setting. This is useful for restricting the use of an NPA to only specific NXXs. The setting for the NPA in this situation is not used in determining if the call is placed. Call placement is determined only by the NXX allow/disallow setting. The system treats the combined NPA/NXX (408/415 for example) in light of the NXX allow/disallow setting, regardless of the NPA setting.
10. See a Sample RCOS Worksheet.

Distribution Lists

If an RCOS is changed, it is possible for a distribution list created before the RCOS change to contain some restricted telephone numbers. A restriction check is performed before each outdialing sequence to avoid calls being placed to restricted telephone numbers. If a telephone number fails the check, a receipt is generated stating “The following telephone numbers are restricted: [number 1], [number 2], etc.” This receipt is always generated, regardless of a mailbox owner request for cancellation of a receipt.

26.30.12 Default FCOS

Several FCOS are pre-programmed in the default configuration. This section describes the default FCOS. Within the feature bit list for each default FCOS, master feature bits appear in bold type. You can select a default FCOS that matches your needs and assign it to a mailbox, or you can customize your own FCOS, using a default FCOS as a template.

We recommend that you preserve these default COS settings and customize FCOS when you require extra features.

Note:
Operations that involve interactions with other mailboxes (make, give, answer) are limited to those mailboxes with compatible Group Class of Service (GCOS).

FCOS 1: Unlimited

This FCOS contains most standard feature bits, except for the message-addressing options. The user can record name and greeting, change the passcode, and receive messages from other users and outside callers. The user can also play, keep, discard, answer, give messages and make new messages for other system users or for distribution lists, as well as create and modify distribution lists. Although this FCOS suits the needs of users with standard applications, do not think of it as truly “unlimited,” which implies that the mailbox is not restricted. It is, more accurately, the basic FCOS for a system.

Note:
New mailboxes have FCOS 1 assigned to them by default unless you specify another FCOS.

FCOS 1 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

020 Make messages

024 Give messages

028 Give with comments

029 Answer messages

032 Make a user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Give to master distribution list

040 Receive messages from other users

041 Receive messages form outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist. list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

098 Say “Press 0” to caller before beep

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

FCOS 2: Full Guest

This FCOS is used in the hotel/motel environment where no Property Management System (PMS) integration is available. It has fewer capabilities than FCOS 1 (Unlimited). However, some feature bits allow check-in and check-out mailboxes to reach this type of mailbox.

FCOS 2 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

008 Mailbox can be checked in/out

020 Make messages

024 Give messages

028 Give with comments

029 Answer messages

032 Make a user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Change to master distribution list

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist. list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

092 User will be in Dial-by-Name database

098 Say "Press 0" to caller before beep

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

161 Conditional greetings

FCOS 3: Restricted

This FCOS is used by hotels. Guests cannot enter or change their names, greetings, or passcodes; make, answer, or give messages; or create or use distribution lists. They can, however, keep and discard messages. Only the attendant can record names and greetings and assign passcodes. For a hotel or motel environment, a name and passcode are usually entered for this mailbox from a special check-in (see default FCOS 4) mailbox. Callers hear the greeting “Please leave a message for [name].”

A guest logs into the mailbox and hears the count of unplayed messages. Unplayed messages play automatically (that is, the guest hears the first message and all succeeding messages without having to press P to play). All messages are automatically kept, unless the guest presses D (to delete messages) within a few seconds.

FCOS 3 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

008 Mailbox can be checked in/out

009 Automatic logout if no message/receipt

010 (ISO) Enhanced Outcall Paging Options

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list **050 Play messages**

052 Auto-play unplayed messages **053 Keep messages**

054 Auto-keep messages **055 Discard messages**

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet only mailbox

FCOS 4: Check In

This FCOS is used by hotels for a check-in mailbox, a special mailbox that manipulates other mailboxes. In a check-in mailbox, the system prompts for the mailbox number to be checked in, then prompts the attendant to record a name and enter a passcode for the mailbox. Guest mailboxes controlled by FCOS 4 must contain feature bit 008 (Mailbox can be checked in/out). Guest mailboxes are therefore usually assigned default FCOS 2 (Full Guest) or default FCOS 3 (Restricted).

FCOS 4 contains the following bits:

001 Login to mailbox

004 Outside caller functions

005 Play Outside Caller Menu prompts

066 Login during greeting in greet only mailbox

070 User Options Menu

071 Record or change mailbox name

072 Record or change greeting

090 Check in other mailboxes

FCOS 5: Check Out

This FCOS is used by hotels for a check-out mailbox that is the counterpart of the check-in mailbox. In a check-out mailbox, the server prompts for the mailbox number to be checked out. The attendant can then choose to either keep or discard any messages left in the mailbox. Finally, the server purges the guest's name, greeting, and passcode, and follows the attendant's command about messages. The mailbox is then ready to be checked in for the next guest.

You must create a check-out mailbox to use the hotel check-in/check-out feature. Guest mailboxes controlled by FCOS 4 must contain feature bit 008 (Mailbox can be checked in/out). Guest mailboxes are therefore usually assigned default FCOS 2 (Full Guest) or default FCOS 3 (Restricted).

FCOS 5 contains the following bits:

001 Login to mailbox **004 Outside caller functions**

005 Play Outside Caller Menu prompts

066 Login during greeting in greet only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change greeting

091 Check out other mailboxes

FCOS 6: Greeting Only

When a caller reaches a Greeting-Only mailbox, the server plays the greeting and then hangs up. For example, a theater manager wants callers to hear an announcement of show times. The manager creates a mailbox with this FCOS, logs in to the mailbox, and records a greeting that announces show times. The mailbox owner can change the mailbox name, greeting, and passcode, but cannot create or use distribution lists. A Greeting-Only mailbox cannot accept messages. A Greeting-Only mailbox must have a greeting; otherwise, the server considers the mailbox invalid. To log into a Greeting-Only mailbox that does not have a greeting, press the * (star) key, then enter the mailbox number. You can remove feature bit 066 (Login during greeting in greet-only mbx) after you record a greeting for the mailbox.

FCOS 6 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

060 Ignore DTMFs during greeting

062 Hang up immediately after greeting

066 Login during greeting in greet only mbx **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

FCOS 7: <TUI Emulation>

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions005 Play outside caller menu prompts

006 Rewind and fast-forward during playback

007 Pause in record or play

016 Deny recycling with * key

018 Give and mark urgent

019 Answer and mark urgent

020 Make messages021 Make and request receipt

022 Make to multiple destinations

023 Make and mark confidential

024 Give messages025 Give and request receipt

026 Give to multiple destinations

027 Give and mark confidential

028 Give with comments

029 Answer messages

030 Answer and request receipt

031 Answer and mark confidential

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Give to master distribution list

038 Attach original message to answer

039 Notification tone when new msg arrives

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist list messages

045 Receive master dist list messages

047 Notification prompt when new msg arrives

050 Play messages 053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

066 Login during greeting in greet-only mbx

070 User options menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

078 Activate user tutorial

084 Give receipt message with comments

085 Give receipt message to multiple dests

086 Give receipt message

087 Make and mark urgent

088 Receive urgent messages

094 Change Message Delivery options

095 Mark message for Future Delivery

098 Say "Press 0" to caller before beep

125 Clear user passcode

126 Make/Give to mailbox with empty GCOS

144 Skip forward to next message

190 Receive fax messages

191 Make fax messages

192 Give fax messages

193 Deliver fax to default number

194 Deliver fax online

195 Specify fax delivery number

196 Change default fax number

204 Message Skip, forward and backward

288 Enable TUI Emulation

FCOS 8: Chain

Chain mailboxes play a greeting, then route calls to the mailbox selected by the caller. A chain mailbox cannot accept messages. Assign this chain FCOS to a mailbox and record a greeting for the mailbox. A chain mailbox prompts callers to enter a mailbox number or to wait. If callers enter a mailbox number, the chain mailbox routes the call to that mailbox. If callers wait (do not immediately enter a mailbox number), NuPoint Voice transfers the call to the attendant's mailbox or to the attendant, depending on the configuration. When a mailbox owner logs in to this type of mailbox, NuPoint Voice prompts, "Press U to change user options, X to exit." The mailbox owner can change the mailbox name, greeting, and passcode, but cannot make messages or create or use distribution lists. Chain mailbox is a default, unless the FCOS has one of these feature bits: 062 (Hang up immediately after greeting), one of the receive message feature bits, or any of the tree, rotational, or broadcast mailbox feature bits. If these feature bits are not included, the general greeting plays, which asks the caller for a mailbox number.

Note:
NP Receptionist and the Chain FCOS: NP Receptionist is an optional feature. The server prompts the caller to enter an extension number, then transfers the caller to that extension. If the caller does not enter an extension, the server transfers the call to the attendant's extension, if one is defined; otherwise NP Receptionist transfers the call to the attendant's mailbox. If you include feature bit 141 (Define chain mailbox in Receptionist), a chain mailbox routes a call to an extension even if the chain mailbox has no greeting.

FCOS 8 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

066 Login during greeting in greet only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

141 Define chain mailbox in Receptionist

FCOS 9: Time

This is a Greeting-Only mailbox that plays its greeting, announces the system time, and asks for a mailbox number. Feature bit 065 (Play system time after greeting) plays the time; if you want this function without announcing the time, you can copy this FCOS to a new number and leave feature bit 065 out of the new version.

A user can log in and change user options (mailbox name, greeting, and passcode), but cannot create or use distribution lists. A time mailbox does not accept messages.

FCOS 9 contains the following bits:

001 Login to mailbox

065 Play system time after greeting

066 Login during greeting in greet only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

FCOS 10: VIP

This FCOS provides advanced options with more feature bits than FCOS 1. It contains these features: Multiple make/give, Attach original message to answer, and Message addressing options (New Message Notification, Mark Confidential, and Return Receipt). This FCOS also includes the Outside Caller's Menu, and will include the mailbox in the Dial-By-Name database.

FCOS 10 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

007 Pause in record or play

015 Change wakeup options

018 Give and mark urgent

019 Answer and mark urgent

020 Make messages

021 Make and request receipt

022 Make to multiple destinations

023 Make and mark confidential

024 Give messages

025 Give and request receipt

026 Give to multiple destinations

027 Give and mark confidential

028 Give with comments

029 Answer messages

030 Answer and request receipt

031 Answer and mark confidential

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Change to master distribution list

036 Auto-receipt for user dist list msgs

038 Attach original message to answer

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist list messages

046 Announce-receipt at login

047 Notification prompt when new msg arrives

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

061 Wait to record (timeout = # key)

066 Login during greeting in greet-only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

075 Audit receipt message

076 Play urgent messages in FIFO order

077 Change pager schedule

078 Activate user tutorial

082 Soft play (interrupt) message count

083 Soft play (interrupt) most prompts

084 Give receipt message with comments

085 Give receipt message to multiple dests

086 Give receipt message

087 Make and mark urgent

088 Receive urgent messages

092 User will be in Dial-by-Name database

094 Change message delivery options

095 Mark message for future delivery

096 Make messages before keep/discard

098 Say “Press 0" to caller before beep

110 Make/give to telephone number

124 Change paging phone number

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

161 Conditional greetings

250 Allow NP PWG View login.

251 Allow NP PWG View telephone playback/record

261 Allow NP PWG View WEB access to messages

289 Enable UM-SMTP

290 Enable UM-WebView

291 Enable RAC (Record a call)

292 Enable NP Director

295 Enable Advanced UM

FCOS 11 - 13: Reserved

FCOS 14: MiCollab

This FCOS is assigned by default to NuPoint Unified Messaging mailboxes when they are created using the MiCollab platform. This includes a set of features relevant to the license configuration bundled with the MiCollab product.

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play outside caller menu prompts

006 Rewind and fast-forward during playback

020 Make messages

024 Give messages

028 Give with comments

029 Answer messages

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Give to master distribution list

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist list messages

045 Receive master dist list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

066 Login during greeting in greet-only mbx

070 User options menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

081 Only One Correct Passcode for Login

098 Say "Press 0" to caller before beep

125 Clear user passcode

126 Make/Give to mailbox with empty GCOS

130 Passcode cannot be same as mailbox

201 Deny Trivial Passcode

290 Enable UM-WebView

291 Enable RAC (Record a call)

292 Enable NP Director

295 Enable Advanced UM

304 Enable UM Standard

FCOS 15: Tree

This FCOS is used to specify a tree mailbox. It plays a greeting and waits for the caller to enter a single digit. When the caller presses a digit, the call is transferred to another mailbox.

FCOS 15 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

066 Login during greeting in greet-only mbx **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Record or change mailbox greeting **121 Define tree mailbox**

FCOS 16: NP Forms

This “template” FCOS is used with NP Forms, an optional feature used to record information from callers in templates, “voice forms.” A mailbox with this FCOS plays the greetings stored in its child mailboxes, sequentially, and records a message after each greeting. A typical application might have a rotational mailbox (see FCOS 17), with several child NP Forms mailboxes, all pointing to the same list of Greeting-Only mailboxes. You can also use feature bit 139 (Template: assume last greet mbox FCOS).

FCOS 16 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt **004 Outside caller functions**

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

007 Pause in record or play **020 Make messages**

041 Receive messages from outside callers

043 Receive message of the day

048 Receive messages of the day

049 No auto-time stamp of played messages **050 Play messages**

052 Auto-play unplayed messages **053 Keep messages**

054 Auto-keep messages **055 Discard messages**

058 Play unplayed messages in FIFO order

059 Play unplayed messages first

066 Login during greeting in greet-only mailbox **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

133 Don't say: "You may start your msg now"

135 Define template mailbox (NP Forms)

136 Don't say: "End of message"

138 Don't say: "Message complete"

FCOS 17: Rotational Mailboxes

Rotational mailboxes allow the caller to hear greetings that change. Greetings change either by time and date (in a "period" rotational mailbox) or with every call (in an "index" rotational mailbox).

FCOS 17 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

066 Login during greeting in greet-only mailbox

068 Define rotational mailboxes **070 User Options Menu**

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

You can also assign any one of the following additional feature bits to a rotational mailbox:

062 Hang up immediately after greeting

063 Call mailbox attendant after greeting

064 Call mailbox user ext after greeting

You can use rotational mailboxes with NP Forms (see FCOS 16) to route the caller to an NP Forms "template" mailbox; this requires feature bit 149 (Login to template thru rotational mbx).

Note:
Do not include feature bit 041 (Receive messages from outside callers) because it disables the mailbox's rotation features.

FCOS 18: Financial

This FCOS provides advanced options with more feature bits than FCOS 1, for administrator convenience. It contains the following features: Multiple make/give, Attach original message to answer, and Message addressing options (New Message Notification, Mark Confidential, and Return Receipt), the Outside Caller's Menu, and it will include the mailbox in the Dial-By-Name database. In addition, the FCOS gives users access to Unified Messaging Web access and access to the embedded secure media player.

FCOS 18 contains the following bits:

001 Login to mailbox

002 Transfer to mailbox attendant

003 Return to welcome prompt

004 Outside caller functions

005 Play Outside Caller Menu prompts

006 Rewind and fast forward during playback

024 Give messages

028 Give with comments

029 Answer messages

032 Make to user distribution list

033 Give to user distribution list

034 Make to master distribution list

035 Change to master distribution list

040 Receive messages from other users

041 Receive messages from outside callers

043 Receive message of the day

044 Receive user dist. list

045 Receive master dist list messages

050 Play messages

053 Keep messages

055 Discard messages

058 Play unplayed messages in FIFO order

059 Play unplayed messages

066 Login during greeting in greet-only mbx

070 User Options Menu

071 Record or change mailbox name

072 Record or change mailbox greeting

073 Enter and change mailbox passcode

074 Create or modify user distribution list

077 Change pager schedule

098 Say “Press 0" to caller before beep

125 Clear user passcode

126 Make/give to mailbox with empty GCOS

290 Enable UM Web View

293 Disable the <Save> <Reply> and <Forward> buttons on the UM Standard Web View web pages

294 Enable the Mitel embedded player on the UM_Std+MWI web pages

26.31 Managing TCOS

Background information and programming for Tenant Class of Service (TCOS) is supplied in the ESMDI section of the *NuPoint Unified Messaging Optional Integrations Guide* available at Mitel OnLine. See About Product Documentation.

26.32 Description - NuPoint Voice Application

Overview

This page provides a description of the configuration and available features for the NuPoint Voice application. Click any link for more details about that item. For programming instructions, see the Procedures section.

The NuPoint Voice application is the standard message-taking and retrieval application providing voice messaging capability for each user's personal mailbox. The NuPoint Voice application can be used with most Central Offices (COs) and some PBXs (check the compatibility list supplied with the Dialogic Media Gateway documentation).

Numerous customized integrations (variations of the NuPoint Voice application) are also available. These are optional features; they provide message waiting control, and functions like personal greetings for forwarded calls.

To use the NuPoint Voice application on your server, you must do the following:

1. Define a line group (assign server ports to the NuPoint Voice application).
2. Configure the application to establish the following parameters:

   - day/night hours
   - a mailbox dialing plan
   - the use of transfers/attendants

   and, optionally:

   - customize administrator's mailbox and attendant's mailbox as required
   - configure Dial-by-Name
   - enable the Dial-back feature

   - add a wait prompt
   - change the default language for system prompts
   - configure NuPoint TDD (Telecommunications Device for the Deaf)
   - configure mailbox passcodes
   - configure an answer delay if required

After the initial configuration is complete and you have activated the changes, you can create mailboxes and record a company greeting.

The NuPoint Voice application can issue different company greetings for day answering and night/weekend answering. With the NP Receptionist optional feature, the software can treat individual extensions differently when calls are received during night and weekend hours, rather than during normal business hours. The hours that constitute a normal work day, and the days of the week that are considered a weekend, can be customized for the individual installation. The company greeting is the greeting in the administrator’s mailbox.

Day and night hours are scheduled for each line group. If you have different day and night/weekend hours for each line group on the server, the greeting that an outside caller hears depends on the line group used to access the mailbox. Of course, if you do not record any custom greetings then all callers hear the same default greeting.

The NuPoint Voice application is configured with default settings from the factory. View default settings.

Day and Night Hours

Start Time of the Work Day

This is the time for the start of the work day in the format “hh:mm AM (or PM)”; where hh is the hour and mm is the minute. The default start time for the work day is 8 a.m. If neither AM nor PM is specified, the server assumes that the time is AM.

End Time of the Work Day

This is the time for the end of the work day in the format “hh:mm AM (or PM)”; where hh is the hour and mm is the minute. The default end time for the work day is 5 p.m. If neither AM nor PM is specified, the server assumes that the time is PM.

If you want to use the same greeting 24 hours a day, enter “12:00AM” in both Start and End time.

Weekend Days Table

This is a table that tells the NuPoint Voice application when to treat calls that are answered during the work day interval (as specified in the two entries above) as day calls, and when to treat these calls as night/weekend calls. The table starts with Monday. The default value is DDDDDNN, which means that the work days are Monday through Friday, and the weekend days are Saturday and Sunday.

Transfers and Attendants

The NuPoint Voice application allows you to specify dial strings and methods for transferring callers, and to specify the use of a wait prompt. If the NP Receptionist optional feature is installed, you can specify the conditions for a company greeting and mailbox greeting.

Attendant’s Transfer String and System Attendant’s Extension

These two dial strings together describe the steps needed to transfer a call to a live attendant, or other general assistance number. These steps are PBX-dependent, and can be determined by actually transferring a call to the attendant from a station set. Use the dial string characters in Table 2-6.

The attendant’s transfer string contains the coding for all the steps that the PBX must take before dialing the attendant’s extension number. The default attendant’s transfer string is S+ which means “do a switch hook flash, then pause for one second.” This string is also used when transferring a caller to a mailbox attendant’s extension number.

The system attendant’s extension consists of the PBX extension number of the live attendant (or a “must answer” number, with no mailbox), plus coding that describes any subsequent steps necessary to complete the call. Up to 30 characters can be entered in this field.

Character	Explanation
0-9, *, #	Keys on a standard pushbutton telephone
(	The following digits should be dial pulsed (10 PPS)
)	Stop pulsing; resume sending DTMF tones
+	Pause for one second
A-D	Fourth column DTMF keys
E	Go off-hook, wait for dial tone or other steady tone (pager go-ahead or confirmation tone, for example), then do next item in string
F	Switch hook flash and wait for dial tone
G	Greet - Wait for a voice or computer tone answer
H	Hang up (go on-hook)
L	Answer supervision - Wait for telephony signal from destination. Use only with trunk (four-wire) connections.
N	Start a new activity; do not go off-hook
O	Ring once
P	Go off-hook, do not wait for dial tone
S	Switch hook flash, no wait required

Character	Explanation
T	**Go off-hook, wait for dial tone**
V	**Voice pager: play the first unplayed message and update mailbox**

The default system attendant's extension number is 0. In addition, the NuPoint Voice application automatically appends an H (hang up) command to the end of the string. This allows the PBX to drop the call if the caller hangs up before the NuPoint Unified Messaging server completes the transfer to the attendant. If your PBX does not allow blind transfers to the attendant, add a G (the code for "wait for a greeting") to the end of the system attendant's extension.

If the PBX allows trunk-to-trunk transfer, you can program an off-site system attendant's extension number.

Each mailbox can be programmed to direct calls to an intermediate attendant when the caller requires assistance. In the absence of an intermediate attendant, calls are routed to the system attendant. Transfer to an attendant can occur in the following situations:

1. When the Key_0 for Attendant Transfer During Greeting parameter is enabled, a caller can press 0 while listening either to the server greeting or to a mailbox greeting. When 0 is pressed during the server greeting, the caller is transferred to the system attendant's extension. When 0 is pressed during a mailbox greeting, the server first checks the mailbox for the attendant's extension number; if none is present, the caller is transferred to the system attendant's extension.
2. While logged in, a mailbox owner can press 0 to be transferred to an attendant, if the mailbox's FCOS includes feature bit 002 (Can Reach Mailbox Attendant). The server first checks the mailbox for the attendant's extension number; if none is present, the caller is transferred to the system attendant's extension. (See the Features Class of Service section for more information about FCOS and feature bits.)
3. If the called party's mailbox FCOS includes outside caller functions, a caller can press 0, after recording a message, to send the message and transfer to an attendant. If the message is left in the attendant's mailbox, the caller is always transferred to the system attendant. If the message is left in a personal mailbox, the caller is transferred to the system attendant only if no attendant's extension number is present in the mailbox.
4. If the attendant's mailbox has been deleted, or has a Greeting-Only FCOS, and the wait prompt is enabled, the outside caller who waits is transferred to the system attendant's extension.

Key_0 for Attendant Transfer During Greeting

This function designates the 0 key as either an attendant access number or a log in code. The default is N, or disabled.

To enable the Key_0 function, you must enter Y. If this function is enabled, be sure to define a suitable system attendant's extension number and dial string.

When the Key_0 for Attendant Transfer During Greeting parameter is enabled:

- The server allows an outside caller to press the zero key, while either the company greeting or a mailbox greeting is playing, to be transferred to the system attendant's extension.
- Mailbox owners must log in by pressing the star (*) key either before or after entering their mailbox numbers. The zero key cannot be used to signal a login.

When the Key_0 for Attendant Transfer During Greeting parameter is disabled:

- Mailbox owners can press either the zero or star (*) key, before or after entering their mailbox number, to log in. (The zero option is essential when telephones at the installation-site do not have a * key.)
- Callers will trip the bad passcode attempt counters. This will cause a higher account for mailboxes getting locked out.
- The server does not allow an outside caller to press 0 while either the company greeting or a mailbox greeting is playing. Therefore, an outside caller cannot be transferred to the system attendant's extension.

Automatic access to the attendant on time out (that is, when the caller waits in response to the "Please enter a mailbox number or wait" prompt) can be provided, if necessary, by assigning a Greeting-Only class of service to the attendant's mailbox. The attendant's mailbox can then be used only to make messages of the day.

Pre-Company Name Dial String

The NuPoint Voice application outputs this dial string immediately after going off-hook, and before playing the Company Greeting (either the standard "Welcome to the message center" prompt, or the Administrator's mailbox greeting).

This string is used only if the NP Receptionist (Receptionist) optional feature has been installed on your server, *and* employees can manually call forward their phones directly to the message center number. In this situation, an NP Receptionist port may inadvertently be connected to one of the ports that is running the message center application. The pre-company name dial string forces NP Receptionist to drop the call, and instructs the server to wait a designated number of seconds before playing the company greeting.

There is no pre-programmed default.

- The pre-company name dial string must include a pound sign (#). You can configure DTMF A (fourth column DTMF key) in place of the pound sign if the PBX recognizes the pound tone as a code for some other function. The port that answers the call issues this tone, which forces NP Receptionist to release the call. Be aware that callers and mailbox owners always hear this dial string when a mailbox is reached through the NuPoint Voice application.
- To give the PBX time to make the connection before the company greeting is played, program a series of plus signs (+++) after the # or A. Each + in the NuPoint Voice application configuration means "wait one second." To determine how many pluses are needed, forward one station to another station, make a test call to the first station, then count the number of seconds that elapse before the second station rings.
- If the test call showed that it takes two seconds for a forwarded call to connect to the second extension, for example, use "#++" for the pre-company name dial string.
- You can experiment to find the optimum number of seconds to wait for call connection. If the first half of the message center greeting does not play when NP Receptionist calls are forwarded, add more pluses to the string. If there is a long silence before the greeting is played, delete pluses from the string.

Pre-Mailbox Greeting Dial String

The NuPoint Voice application outputs this dial string immediately after receiving a valid mailbox number, and before playing the mailbox's greeting.

This string is used only if 1) the NP Receptionist optional feature has been installed on your server and 2) employees may manually call forward their phones directly to their mailboxes. In this situation, an NP Receptionist port may inadvertently be connected to one of the ports that is running the message center application. The pre-mailbox greeting dial string forces NP Receptionist to drop the call, and instructs the server to wait a designated number of seconds before playing the mailbox greeting.

There is no pre-programmed default. The same conditions apply as listed above in "Pre-Company Name Dial String."

Customize Administrator Mailbox

The NuPoint Unified Messaging software is installed with a default dialing plan of 3,3,3,3,3,3,3,3,3 and one administrator's mailbox, which is 998. If you change the dialing plan (i.e. the number of digits in valid mailboxes that start with the digit 9), then you must also change the Administrator's mailbox to match the new criteria. (For example, if your dialing plan were configured as 4,4,4,4,4,4,4,4,4, then mailboxes that start with 9 must have 4 digits - 9998.) An error message is generated if the administrator mailbox number does not match the dialing plan.

The default administrator's mailbox, 998, does not have a default passcode. You must set a passcode for this mailbox before you can access it. The passcode you set must not be trivial (for example, 1111 or 1234).

The administrator's mailbox number has special privileges:

- The administrator's mailbox day and night greetings are the day and night company greetings. If you do not record one or both of these greetings, the default (��Welcome to the message center") is played instead.
- Distribution lists that are created from the administrator's mailbox are server-wide master lists that can be used by any mailbox owner on the server. See Distribution Lists.
- The system administrator may add/delete/modify mailboxes over the telephone, from the Telephone Administration Menu. See Telephone Administration.

Mailbox Security

For increased server security, you can change the administrator's mailbox number from the default. You can use any mailbox number on the server; but if you select a mailbox number other than one of the defaults, you must create the mailbox before it can be used. The mailbox number you select must also be valid for the dialing plan. (See Administrator's Mailbox.) You must also identify the new mailbox in the line group for NuPoint Voice as the administrator mailbox to enable it to perform specialized administrator functions. The recommended FCOS for both mailboxes is 10 (VIP), the LCOS is 1 (Default), the GCOS is 1, and the message waiting type should be whatever is available for your server.

For highest security, you can also delete the Administrator's mailbox and re-create it only when you need to make changes.

Administrator Passcodes

When creating the administrator mailbox, you must ensure that the passcode you enter is not trivial. If you use the following types of passcodes, NuPoint UM will accept the entry but you will not be able to log in to the admin mailbox on subsequent attempts:

- do not use the mailbox number
- do not use consecutive digits (like 1234)
- do not use repeated digits (like 1111)

Examples of valid passcodes are: 1397 or 2684 (as long as the mailbox number is not the same).

Customize Attendant Mailbox

The NuPoint Unified Messaging software is installed with a default dialing plan of 3,3,3,3,3,3,3,3,3 and one attendant's mailbox, which is 999. If you change the dialing plan (i.e. the number of digits in valid mailboxes that start with the digit 9), then you must also change the Attendant's mailbox to match the new criteria. (For example, if your dialing plan were configured as 4,4,4,4,4,4,4,4,4, then mailboxes that start with 9 must have 4 digits - 9999.) An error message is generated if the attendant mailbox number does not match the dialing plan.

The default attendant's mailbox, 999, does not have a default passcode. You must set a passcode for this mailbox before you can access it. The passcode you set must not be trivial (for example, 1111 or 1234).

Note:

For increased server security, you can change the attendant's mailbox number from the default. The attendant's mailbox can be any mailbox number on the server; but if you select a mailbox number other than one of the defaults, you must create the mailbox before it can be used. The mailbox number you select must be allowed by the Dialing Plan. (See Attendant Mailbox.)

The attendant's mailbox also has special privileges:

- Its greeting is the message of the day. This message is heard by all mailbox owners whose FCOSs include feature bit 043 immediately after they log in. The message is played twice (after two separate logins), the first time hard-played and the second time soft-played. (Hard-played prompts cannot be interrupted; soft-played prompts can.)
- The message of the day is stored only in the attendant's mailbox. Once it has been deleted, no mailbox owners hear the message, even if they have not logged in since the last message was created. Conversely, if an old message of the day is not deleted, or replaced by a new message, all newly created mailboxes receive the outdated message. For procedures to record and enable a message of the day, see Record/Delete the Message of the Day or Enable/Disable the Message of the Day.
- A customized site tutorial greeting can also be recorded from the attendant's mailbox. When the system administrator presses G to record a company greeting, the server prompts, "Press M to record the message of the day; press T to record a site tutorial." See Record a Site Tutorial for procedures.
- When outside callers access the message center, they are prompted to "Please enter a mailbox number or wait" after the company greeting is played. Callers who wait (because they have rotary dial phones, or do not know the correct mailbox number, for example) are then prompted, "Please leave your name,

the name of the person you are calling, and a message." These unaddressed messages go into the attendant's mailbox.

Multiple Attendant's Mailboxes

If a large number of unaddressed messages is expected, up to five Attendant's Mailboxes can be configured by entering the mailbox numbers, separated by commas (for example, 999, 910, 911, 912, 913). The message of the day and the site tutorial can be made only from the first attendant's mailbox that is configured; the other mailboxes are used only for storing unaddressed messages. When the first mailbox is full, NuPoint Voice begins using the second mailbox until it is full, and so on until all attendant's mailboxes are full.

You can configure any mailbox as the attendant's mailbox by entering the mailbox number in this field. If you select a mailbox number other than one of the defaults, you must create the mailbox before it can be used. (See Attendant Mailbox.)

Disabling the Attendant's Mailbox

When an outside caller accesses the message center number, NuPoint Voice issues the prompt, "Please enter a mailbox number or wait." Callers who wait are prompted to leave a message in the attendant's mailbox. Some installations require these callers to be transferred to the system attendant's extension, instead. There are two ways to do this:

- If the system administrator does not issue messages of the day, delete the attendant's mailbox.
- Assign a Greeting-Only FCOS to the attendant's mailbox.

Note:

If you disable the attendant's mailbox, and you do not define a system attendant's extension number, be sure to disable the Wait prompt. Otherwise, when a caller waits, NuPoint Voice says "Thank you for calling," then hangs up!

Dial By Name

Dial-by-Name is a feature of NuPoint Voice that allows callers to dial a user's number by saying that user's name. See Dial-by-Name for configuration.

Dial-back

The dial-back feature gives users a second option when answering voice mail messages. When enabled, dial-back allows users to dial the caller who left the voice mail, with the option to either keep or delete the original message. See Dial-back for configuration.

Wait Prompts

When the Wait prompt is enabled, the server issues the prompt “Please enter a mailbox number, or wait” immediately after the server greeting is played. The default value is Y (enabled).

To disable this prompt, you must enter N. In some cases, you must disable the Wait prompt for any number of reasons, among them:

- To record the company greeting (administrator’s mailbox greeting) and the Wait prompt in the same voice. The text of the Wait prompt is recorded as the last sentence of the company greeting.
- When neither a system attendant’s number nor an attendant’s mailbox is defined, and the Wait prompt is enabled, callers who wait are thanked for calling, then disconnected.
- If you disable the Wait prompt and are using the Dial-by-Name function, you must record the “Press [digit] to dial by name” prompt in your own voice. The server prompt for Dial-by-Name plays if the Wait prompt is enabled.

Default Language for Prompts

The default language of voice prompts is English. You must purchase and install language prompts in order to use any other language on your server. For information about installing language prompts, see the NuPoint Unified Messaging Technician's Handbook.

Refer to the General Information Guide for more information about supported languages, or contact your distributor for further information.

A mailbox’s LCOS can specify a different prompts language. Prompts in a secondary language must be installed before these mailboxes issue any prompts in these languages. Callers hear prompts in the default language.

A server can have one default language and up to seven alternate languages, depending on the number and size of the hard drives. For more details about the number and kinds of languages supported, see LCOS.

NP TDD can be installed like any of the language prompts. If NP TDD is installed, selecting it as a response to the Default Language for Prompts parameter enables the NP TDD feature of the NuPoint Voice application in the current line group. When any mailbox owner receives or makes a call through that line group, NP TDD replaces voice prompts with TDD tones. (See “NP TDD for the Hearing Impaired” below for more information.)

NP TDD for the Hearing Impaired

The NP TDD feature of the NuPoint Voice application supports telecommunications devices for the deaf (TDDs). With NP TDD, hearing-impaired mailbox owners can receive TDD-generated text from other users.

NP TDD users can be notified about messages by message waiting lights or any other message waiting indication supported by a NuPoint Unified Messaging server, just as other users can.

Outside callers with a TDD can call a mailbox configured for NP TDD prompts, be answered by a TDD greeting, and leave a message for the mailbox owner. Standard user options such as reviewing and recording over a message, making a message urgent, appending to a message, and dialing an extension are also allowed.

Configuring NP TDD

You can configure NP TDD to apply to either an entire line group or specific mailboxes. To configure NP TDD, make the following changes:

- Set the default language for prompts to TDD in the NuPoint Voice application (if configuring the line group).
- Assign an NP TDD LCOS or another LCOS specifying NP TDD as the prompts language to any mailboxes using NP TDD. This LCOS should also have the Greeting Length and User Name Length limits parameters appropriately set for NP TDD.

Effect of NP TDD on Other Server Features

Certain NuPoint Unified Messaging server features and user options are not available to any mailbox associated with the line group in which NP TDD is configured. These features are:

- NP WakeUp optional feature
- Call scheduling for pages
- Future delivery
- Standard tutorial

Mailbox Passcodes

NuPoint Unified Messaging includes security devices to protect your installation at a server level and mailbox level. A device for use at the mailbox level is mailbox passcodes, which you configure through the NuPoint Voice application. The following paragraphs outline the configuration of mailbox passcodes; for more complete information, see Server Security.

Minimum and Maximum Passcode Length

Minimum and maximum passcode length sets the range for the number of digits a passcode can have.

Enter the minimum number of digits that constitute a valid passcode for users of this line group. The minimum passcode length can be any number from 4 through 10. The default value is 4. This means no user can enter a new passcode shorter than 4 digits. If you want users to have longer passcodes (for security reasons) then you can specify a larger minimum length.

Enter the maximum number of digits that constitute a valid passcode for users of this line group. The maximum passcode length can be any number from 4 through 10. The default value is 10.

If you leave the maximum passcode length at the default, 10, then all passcodes can be no longer than 10 digits. You cannot enter a value greater than 10, and users cannot enter a passcode longer than 10 digits.

Passcode Trip Count, Passcode Trip Period

These two entries set the parameters for the passcode break-in warning, which is a server security feature. The default values for the passcode trip count and the passcode trip period are 5 and 24. This means that a warning is issued to a mailbox if someone attempts to enter an incorrect passcode for that mailbox at least 5 times (the passcode trip count) within a 24 hour period (the passcode trip period).

The passcode trip count can be set to any value from 0 to 255. The passcode trip period can range from 0 to 240 hours. In both cases, zero means the passcode break-in warning function is disabled.

The passcode break-in warning function is enabled when you configure both a trip count and trip period.

Answer Delay

You may set a variable answer delay with the Delay Before Answer parameter. The default for this parameter is zero (no delay), and in most cases, it does not need to be changed.

Users need to use this delay if the application software sometimes answers an incoming call before all the digits are received, causing the switch to stop sending digits. This can happen when E & M trunks are being used.

Note:
The answer delay for the first call into a port after any online configuration change (FCOS, LCOS, GCOS, NCOS, line group, phoneline exceptions) is up to a second longer than for subsequent calls on the port. Consequently, changes to the answer delay parameter do not become effective until the second call is made into the port.

26.33 Default Configuration Settings

The NuPoint Voice application is the only application that is pre-installed in the factory configuration. To add capabilities, and to meet the requirements of a particular site, you may need to change one or more of the defaults. You can use the Web Console or Text console to change the defaults.

The default configuration has the values shown in the following table.

Parameter	NuPoint Voice Default Setting
Administrator's mailbox number	**998**
Allow dial an extension for callers	**N**
Allow dial an extension for users	**N**
Allow multiple messages for outside caller	**Y**
Answer delay	**0**

Parameter	NuPoint Voice Default Setting
Attendant's mailbox number	999
Attendant transfer string	S+
Dial by name, last name first	Y
Exact match break	Y
General greeting mailbox number	None
Group name	None
Key 0 for attendant transfer	N
Line group number	1
Line(s) in group	All on server
Mailbox dialing plan	3,3,3,3,3,3,3,3,3
Number of names threshold	3 names
Passcode length	4 digits min. – 10 digits max.
Passcode trip count	5
Passcode trip period	24 hours
Pre-company name dial string	None
Pre-mailbox greeting dial string	None

Parameter	NuPoint Voice Default Setting
Prompts language	**English**
Single digit access	**None**
Suppress mailbox number	**None**
System attendant's extension	**0**
Wait prompt	**Y**
Weekend days table	**DDDDDNN**
Work day	**8 a.m. – 5 p.m.**

26.34 Dial-by-Name

Dial by Name is a NuPoint UM feature that allows callers to dial a NuPoint UM user by entering some, or all, of the letters of the user's name.

To configure the Dial-by-Name function, you need to perform the following tasks (for more detail, see the explanations below the list):

- Change the dialing plan to specify a digit for Dial-by-Name.
- Specify the name dialing sequence that callers must use, last name-first or first name-first.
- Set a threshold for playing matching names.
- Specify whether a caller must enter a complete name or just enough letters to get a match.
- Specify whether a caller can press a single digit to reach a mailbox or must enter the entire mailbox number.
- Specify whether a caller hears matched names and mailbox numbers or just the matched names.
- Determine the grouping of access within the Dial-by-Name database (sometimes called "Partitioned Dial-by-Name"). Even though mailbox owners may all be in the same Dial-by-Name database, they can only reach others in the database who share the same GCOS group (in a bit-mapped GCOS) or affinity group.

Dialing Plan

In the Dialing Plan, coding a digit with the A element reserves that digit for dialing names. For example, a Dial-by-Name dialing plan might look like this: 3,3,3,3,3,3,3,A,3 which would trigger the prompt, "Please enter a mailbox number or press 8 to dial by name."

Name Dialing Sequence

You specify the name dialing sequence with the Last Name First Flag parameter. This parameter determines whether a user's name must be dialed in the last name-first name sequence or the first name-last name sequence. In most cases, callers need not enter user's full name. When a caller finishes pressing a series of keys, the NuPoint Unified Messaging server searches special files for entries that match the series. If it finds more than one match, it plays the names and mailbox numbers of the partial matches. If the server finds a unique match, it plays either the user's name or personal greeting.

Matching Threshold

Setting a threshold for playing matching names determines the maximum number of names and mailboxes the server plays in response to a partial name match. A partial name match occurs in either of these cases:

- Callers enter some portion, but not all, of a recipient's name.
- Callers enter a complete name, but the server finds more than one recipient that matches the entry.

If more than one name is found that matches the name dialed, the server plays the specified number of matching names. A threshold of 3, for example, means that up to three matching names will be recited, even if there are more than three. If the number of names for a partial match is greater than the threshold, the server prompts a caller to continue entering letters.

Exact Match Break

Specifying an exact match break determines how callers can enter the partial name of a user. When "yes" is specified, the caller hears the name and mailbox number play as soon as there is a match. The caller can, however, end a name entry with the pound (#) key; the caller hears whatever names match. When "no" is specified and a caller stops entering letters, the server waits for a time out period before responding; if a caller presses the # key, the server responds immediately. If the server can determine exactly who the intended recipient is, it plays that recipient's name (and mailbox number if not suppressed). Alternatively, the server plays, for outside callers, that recipient's personal greeting. If more than one recipient's name matches the caller's input, the server plays the names and mailbox numbers of the possible recipients. A caller can interrupt the server during name or greeting play by pressing any key on the telephone keypad.

Single Digit Access

Specifying single digit access means that a caller can enter a single digit to reach a mailbox after matched names have been played, similar to a tree mailbox operation. When single digit access is allowed, a match with the name dialed by a caller causes the server to play a prompt such as:

"There are three entries: Jean Brown, mailbox 4321, press 1; John Brown, mailbox 4222, press 2; Jill Brown, mailbox 4567, press 3. Enter a mailbox number. Press 0 to return to Dial-by-Name."

The caller can then press the appropriate digit to reach the desired person instead of entering the entire mailbox number.

When no single digit access is allowed, a caller must enter an entire mailbox number to reach a mailbox after matched names have been played. A match with the name dialed by a caller causes the server to play a prompt like the one shown above except that there is no single digit stated. The caller must enter the entire mailbox number.

Suppressing Mailbox Numbers

Suppressing the mailbox number means the server omits the mailbox numbers in the list of names played when there is a match with a dialed name. The default is to include the mailbox number.

Dial-by-Name Databases

Each mailbox that can be reached by name must be configured with an FCOS that includes feature bit 92, which places users' mailbox numbers in the two Dial-by-Name databases. The databases are identical but their format is different, with one listing users by last name and the other by first name. The server searches these databases for entries to match a caller's input. For example, if the caller is prompted to dial by last name, when the caller begins entering a name the system will search through the database that lists users by last name. If the caller is prompted to dial by first name, the system will search through the database that lists users by first name. See the FCOS section for more information on this feature bit and how to implement a Feature Class of Service.

Even with all the parameters just described set, a mailbox owner's name can be listed only when the mailbox owner's name is specified in the mailbox configuration. Once all these requirements are met, the name goes into the databases when you exit from the respective configuration menu.

To make sure there is only one mailbox per user's name, you can print out a phone book for your site. This phone book shows the mailbox owners accessible through the Dial-by-Name function and their mailbox numbers.

Same Digit for Dial-by-Name and Mailbox Numbers

Occasionally you may need the same digit for a Dial-by-Name trigger *and* in a mailbox number. With the optional star prefix dialing plan (described above), the digit specified for Dial-by-Name can still be used for mailbox numbers when the digit is *not* followed by a star (*). Suppose, for example, that your server has mailboxes beginning with 1 but you also need the digit 1 for Dial-by-Name. You can specify 1 as the Dial-by-Name dialing plan digit, which causes the server to prompt the caller to press 1 and * to dial by name.

Using a Telephone to Dial by Name

The Dial-by-Name feature allows callers to reach a mailbox user by dialing the user's name on the telephone keypad. By default, the system expects the last name to be dialed before the first name. However, the dialing sequence can be reversed so that the first name is required before the last name. If there is more than one match, the attendant lists the names of the matches along with the key to press to call each match.

Example 1:

You are trying to reach Sarah Jones on a system that requires the last name to be dialed name first. In the Auto Attendant, you hear "Please enter a mailbox number or press <x> to dial by name." You enter 5 6 6 3 7 for JONES. There is only one voice mail user with the last name spelled by the letters 5 6 6 3 and 7, so you hear "You are being transferred to Sarah Jones", and the attendant transfers you.

Example 2:

You are trying to reach Jamal Singh on a system that requires the first name to be dialed name first. In the Auto Attendant, you hear "Please enter a mailbox number or press <x> to dial by name." You enter 5 2 6 for JAM and wait. There is more than one user with the first name starting with the letters on 5 2 and 6, and you hear "3 matches were found. To reach Jamal Singh, press 1. To reach Sarah Jones, press 2. To reach Jamie Beauchamp, press 3". You press 1 and the attendant transfers you.

Using the Phone Keypad:

Callers use their phone keypad to enter letters. For example, to enter A, B or C, a caller presses **2**, and to enter D, E or F, a caller presses **3**. To enter an accented character, callers must press the key for the equivalent unaccented (or "English") character. For example, to enter À, a caller presses 2 (A), and to enter Ø, a caller presses 6 (O). The following table illustrates which keys should be pressed to enter accented and unaccented characters:

Accented Characters		Unaccented Characters		Keypad Key
À	à	A	a	2
Â	â	A	a	2
Ä	ä	A	a	2
Å	å	A	a	2
Å	å	A	a	2
Æ	æ	E	e	3
Ç	ç	C	c	2
È	è	E	e	3
É	é	E	e	3
Ê	ê	E	e	3
Ë	ë	E	e	3
Î	î	I	i	4
Ï	ï	I	i	4
Ô	ô	O	o	6

Accented Characters		Unaccented Characters		Keypad Key
Ö	ö	O	o	6
Ø	ø	O	o	6
Œ	œ	O	o	6
Š	š	S	s	7
Ù	ù	U	u	8
Û	û	U	u	8
Ü	ü	U	u	8
Ÿ	ÿ	U	u	8
Ž	ž	Z	z	9
ß		S	s	7

26.35 Dial-Back

The dial-back feature gives users a second option when answering voice mail messages. When enabled, dial-back allows users to dial the caller who left the voice mail, with the option to either keep or delete the original message.

To enable Dial-back, customize an FCOS to include the following feature bits and assign to the mailbox:

- 263 - Store Caller Line Id as a phone or mailbox number
- 264 - Play outside caller user interface (with FCOS bit 280)
- 270 - Enable Dial-Back feature
- 280 - Enable CLI outside caller interface (with FCOS bit 264)

Program an outgoing call prefix for the MiVoice Business ICP:

- Access the *MiVoice Business System Administration Tool*.

- In the **System Options Form**, set **Outgoing External Call Prefix for Applications** to the digit that users dial to access an outside line (this is often "9").

Prompts received by voice mail users are dependent upon FCOS programming. The voice mail "Answer" operation is independent of dial-back operation so you can enable feature bits for one, both, or neither. The table below describes NuPoint voice prompts for each scenario:

If your system is configured for...	and the voice mail you receive is from...	when you press the Answer key, the NP-UM TUI responds with...
Answer AND Dial-back	another mailbox on the network	the following options: - press 8 for Voice mail answer - press 3 for Dial-back and delete message - press 5 for Dial-back and keep message
	an external (local or long distance) caller *	the following options: - press 3 for Dial-back and delete message - press 5 for Dial-back and keep message
Answer only	another mailbox on the network	with immediate “answer with a voice mail” operation
	an external (local or long distance) caller	[No Answer key option is available in the TUI menu.]
Dial-back only	another mailbox on the network	with dial-back options: - press 3 for Dial-back and delete - press 5 for Dial-back and keep
	an external (local or long distance) caller *	
Neither Answer nor Dial-back	Any call	[No Answer key option is available in the TUI menu.]

*Dial-back will attempt to dial the numbers in the Calling Line Identification. Correct dial-back for long distance and International calls is dependent upon programming in the MiVoice Business ICP. For more information, see the *Automatic Route Selection* topic in the *Features Reference* section of the *MiVoice Business ICP System Administration Tool Help*.

Conditions

- The dial-back feature requires MiVoice Business Release 4.0 (formerly MiVoice Business ICP Release 10.0) or later software on the MiVoice Business ICP
- Dial-back is not supported for SIP integrations like the 5000 CP.
- If a user selects the option to "dial-back and delete message", and then the call is not completed, the original message is restored to the voice mailbox.
- The dial-back feature will not work for messages that have been stored using a version of NP-UM prior to Release 4.0.

Wait Prompts

When the Wait prompt is enabled, the server issues the prompt “Please enter a mailbox number, or wait” immediately after the server greeting is played. The default value is Y (enabled).

To disable this prompt, you must enter N. In some cases, you must disable the Wait prompt for any number of reasons, among them:

- To record the company greeting (administrator’s mailbox greeting) and the Wait prompt in the same voice. The text of the Wait prompt is recorded as the last sentence of the company greeting.
- When neither a system attendant’s number nor an attendant’s mailbox is defined, and the Wait prompt is enabled, callers who wait are thanked for calling, then disconnected.
- If you disable the Wait prompt and are using the Dial-by-Name function, you must record the “Press [digit] to dial by name��” prompt in your own voice. The server prompt for Dial-by-Name plays if the Wait prompt is enabled.

26.36 NuPoint Voice Application Programming - Task List

This procedure summarizes the steps necessary to configure the NuPoint Voice application. It assumes that the appropriate server hardware and NuPoint Voice software have been installed.

1. Complete a NuPoint Voice Application Worksheet. Blank worksheets are here.
2. Define a line group to be used for the NuPoint Voice application.
3. Configure the company greetings schedule. Use the Day/Night Menu to configure working hours and weekends.
4. Establish a dialing plan.
5. Enable Call Placement, if required.
6. Configure for transfer to a system attendant, if required.
7. If you want to use an administrator mailbox other than the default for this application, you need to create a new mailbox and then define it as an administrator mailbox.
8. If you want to use an attendant mailbox other than the default for this application, you need to create a new mailbox and then define it as an attendant mailbox.
9. Prevent unaddressed messages from being left in the attendant mailbox (i.e. always transfer callers to the attendant).

10. Enable multiple messages for outside callers, if required. (Text console only.)
11. If you want to use a prompt language other than the default North American English, select a prompt language.
12. Enable Dial-by-Name if required.
13. Configure the mailbox passcode parameters as required. (See Security.)
14. Verify the configuration parameters.
15. Activate the configuration to make your parameter settings take effect.

26.36.1 Add a Line Group

Note:
For MiCollab deployments of NuPoint UM, you must use the MiCollab Users and Services Provisioning application to set up one or more Network Elements before configuring Line Groups.

To add a line group to your system configuration:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups** and then click **Add**.
4. Configure the following parameters:

Parameter	Description	Value
Line Group Number	Assign a number to this line group or click **Next Available** to add an unused list number.	1 - 24
Name	Enter a name for this line group.	Maximum 25 characters.
Pilot Number	For SIP GATEWAY nodes only. See step 7 for information.	

Parameter	Description	Value
Application	Select the application to associate with this line group. A set of custom tabs appears for each application. Choices are: • NuPoint Voice • NP Receptionist • Outbound (Pager) Dialer • Centrex • Unified Integration • Enhanced InBand • DTMF to PBX Dialer • Speech Recognition • Direct Drop • Disabled Click the links in step 5 for a description of configuration parameters for each application.	Default: NuPoint Voice
User Interface	Select the user interface that corresponds to this line group. Choices are: • None • NuPoint Voice • Call Director	Default: None
Fax Group Connection	Select a fax group from your configured fax groups to associate with this line group. **Note**: If you select a fax group, you cannot enable G.729 audio compression.	Default: None

Parameter	Description	Value
Enable G.729	Select the check box to enable G.729 audio compression for this line group. Clear the check box to restrict the line group to G.711. **Note**: • If you enable G.729, you cannot select a Fax Group Connection for the line group.	Default: Cleared

Parameter	Description	Value
	• This field is available only if a G.729 license has been purchased for the system.	

Parameter	Description	Value
	• Before implementing G.729, check the NuPoint UM Engineering Guidelines to ensure that you do not exceed the recommended port usage limits. This is necessary because G.729 uses more system resources than G.711.	

Parameter	Description	Value
	• For a Mitel 5000 CP integration, access the Speech Encoding Setting field on the 5000 CP (located in System\Devices and Feature Codes \Node IP Connection Groups\<Pxxxx>IP Call Configuration or System\IP-Related Information\Call Configurations) and select **G.729**.	

Parameter	Description	Value
	• For a MiVoice Business ICP integration, create a network zone on the MiVoice Business ICP, enable Intra-zone Compression, and then assign all endpoints, including sets and IP extensions mapped to NuPoint ports, to the zone. In addition, make sure to equip the MiVoice Business ICP with Digital Signal Processors (DSPs) that support G.729.	

Parameter	Description	Value
	• For a Dialogic Media Gateway integration, access the DMG Web Interface, select the network group for this implementation (located under Configuration > VoIP > Network Groups), and then select **Low Bit Rate Codec** as Audio Codec #1.	
	• When deciding which codec to use, be aware that G.711 provides high quality voice but uses more bandwidth. G.729 uses less bandwidth at the cost of some sound quality, although it is still good enough for most calls.	

5. Using the interface tabs, configure the parameters required for your application:

   - The Lines tab is common to all applications.
   - NuPoint Voice/Direct Drop parameters
   - NP Receptionist parameters
   - DTMF to PBX Dialer parameters
   - Outbound Pager/Dialer parameters
   - Centrex
   - Unified Integration parameters
   - Enhanced InBand parameters
   - Speech Recognition parameters

6. Click **Add** to save the configuration data.
7. For SIP GATEWAY nodes only: A "Pilot Number" field appears after a Line Triplet if the line group is mapped to the network element of type SIP GATEWAY. Enter a value for the Pilot Number in this field. A pilot number is made up of 1 to 6 digits.

Note:

- For a Mitel 5000 CP integration, enter a pilot number in the field that matches the Pilot Number defined on the SIP Gateway for NuPoint Unified Messaging.
- All lines in a line group must be mapped to one Network Element item of type SIP GATEWAY. This means that if the first line in a line group is mapped to a SIP GATEWAY port, then other added lines must also be mapped to the same SIP GATEWAY.
- When you map a line-triplet (e.g. 1:0:0) to a port number (e.g. 3), the port number must start from 1 and not zero. The port numbers that can be used in the mapping depend on the number of ports programmed on the menu for Network Element of type SIP GATEWAY (see Number of Ports in Add a Network Element). For example, if the Number of Ports in the Network Element is 16, then the valid port numbers are: 1, 2, 3, etc. up to 16. You cannot not map a line triplet to port 17 or 0, or to any other port that is larger that 16. Also, you cannot map two line triplets to the same port number. For example, you cannot map both of the line triplets 1:0:0 and 1:0:2 to port number 2.

8. Click **Add** again to add the new line group to the list of existing line groups.
9. A confirmation message regarding the configuration changes appears. Click **OK**.
10. In the navigation tree, select **Commit Changes and Exit**. Confirm the **Commit**. Your changes are now saved to the inactive (duplicate) configuration.

Note:
Configuration changes will not take effect until you have activated the inactive configuration.

26.36.2 Edit a Line Group

Follow the steps below to edit a line group:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups**, select a line group to edit, and then click **Edit**.
4. The existing line group configuration parameters appear. Change the parameters as required.
5. Click **Save**. A confirmation message regarding the configuration changes appears. Click **OK**.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **Commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.36.3 Delete a Line Group

Follow the steps below to delete a line group:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups**, select the line group to delete, and then click **Delete**.
4. A confirmation message appears. Click **OK** to delete the line group.
5. The line group is now deleted and disappears from the list shown in the Offline configuration.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **Commit.** Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.36.4 Application Parameters

When you select an application to assign to a line group, the onscreen tabs are customized for the selected application. The Lines and Dialing Plan tabs are the same for all applications.

The Lines tab (common to ALL applications):

Parameter	Description	Value
Line Triplet	Enter a line number for this line group or click **Next Available** to use the next unused line number.	
Number of Lines	Enter the number of lines in this line group.	
PBX	Select the PBX to use for this line group.	

Parameter	Description	Value
Mapping	Enter the module number, line card number, port designator, or directory number (DN) to add to the line group. **Note**: If you are adding multiple DNs (**Number of Lines** is greater than one) that are consecutive, then you only have to enter the first DN. If you are adding multiple DNs that are not consecutive, then you must enter them one at a time.	
Terminal Number	For CENTREX application only. Enter the terminal number required for Centrex for this triplet.	Valid values are 0 - 9. Cannot use leading 0.

NuPoint Voice/Direct Drop Application Parameters

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Dialing Plan	Standard Mode / Length	See Dialing Plan Configuration	
	Classic Mode / Dialing Plan		
Voice mail	Mailbox Numbers		

Tab	Parameter	Description	Value
	Administrator's mailbox number	A special mailbox reserved for administrative purposes. Each line group can have its own admin mailbox. The admin mailbox has special privileges: • add/delete/modify mailboxes through the ADMIN menu, using Admin Dialer • Admin's distribution lists are system-wide "master lists" (accessed as 001 - 009) • Admins GREETING is "Company Name"	Default is 998.
	Attendant's mailbox number	A special Attendant's mailbox. You can chain up to 5 comma-separated mailbox numbers. Each line group can have it's own attendant mailbox. The attendant mailbox has special privileges: • "unaddressed" messages go into the Attendant mailbox (for example, callers with rotary dial phones) • Attendant's GREETING is "Message of the Day"	Default is 999.

Tab	Parameter	Description	Value
	General Greeting mailbox number	A special mailbox whose greetings have a special purpose. Each line group can have a different general greeting mailbox.	
	System Attendant's extension	A number dialed by the application to connect the caller to the PBX attendant.	Default is O. Number of digits in the PBX directory number is determined by the NP Receptionist dialing plan.
	NP Receptionist Dialing Plan		
	Dialing Plan	Defines the number of digits a PBX DN has: • 0 specifies that no valid DN begins with that digit • V specifies a variable number of digits • A specifies dial by name	Default is 3,3,3,3,3,3,3,3,3.
	PBX Console Attendant		
	Day Access Code	This entry connects the caller to the PBX attendant available to take the call during Day hours.	Default is 0H. Valid characters are 0-9, # *, +, (,), A_H, L, N-U.
	Night Access Code	This entry connects the caller to the PBX attendant available to take the call during Night hours.	

Tab	Parameter	Description	Value
	Options		
	Key_0 for Attendant transfer during greeting	Select this check box to allow "key 0 for attendant" transfer during a greeting. Clear this check box to allow "key 0 for attendant" transfer only during the login sequence.	Default is cleared.
	Allow dial an extension for Callers	Select this check box to make the application allow an external caller to dial an extension from inside NuPoint Voice. Clear this check box to prevent an external caller from dialing an extension from inside NuPoint Voice.	Default is cleared.
	Allow dial an extension for Users	Select this check box to make the application allow another user on the same NP-UM server to dial an extension from NuPoint Voice. Clear this check box to prevent another user from dialing an extension from NuPoint Voice.	Default is cleared.
Dial Strings	PBX Dial Strings		

Tab	Parameter	Description	Value
	Post DN dial string	Enter the dial string to be output when the PBX DN has been dialed.	Default is +. Valid characters are 0-9, # *, +, (,), A_H, L, N-U.
	Dial Strings		
	Attendant's transfer string	Enter the dial string that will put the caller on hold so the application can dial the PBX attendant.	Default is S+. Valid characters are 0-9, # *, +, (,), A_H, L, N-U.
	E-mail transfer string	Enter the string that is dialed to connect the caller to an electronic mail system	Valid characters are 0-9, # *, +, (,), A_H, L, N-U.
	Disconnect string	Enter a dial string that NP Voice ports should dial to cause NP Receptionist ports to disconnect.	Valid characters are 0-9, # *, +.
	Pre-company name dial string	Enter the number to be dialed immediately after going off-hook and before playing the Company Greeting.	Valid characters are 0-9, # *, +, (,), A_H, L, N-U.
	Pre-mailbox greeting dial string	Enter the number to dial after receiving a valid mailbox number and prior to playing the greeting for that mailbox.	
	'6' Key Operator transfer dial string	Not used.	

Tab	Parameter	Description	Value
	'6' Key Operator transfer pre-dial string	Not used.	

NP Receptionist Application Parameters

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Dialing Plan	Standard Mode / Length	See Dialing Plan Configuration	
	Classic Mode / Dial Plan		
Voice Mail	All parameters	See Voicemail tab descriptions for NuPoint Voice application	
Dial Strings	All parameters	See Dial Strings tab descriptions for NuPoint Voice application	

Outbound (Pager) Dialer Application Parameters

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Dialing Plan	Standard Mode / Length	See Dialing Plan Configuration	
	Classic Mode / Dial Plan		

Tab	Parameter	Description	Value
Dialers (Pagers)	<system generated list>	Select the dialers(pagers) that are supported by this line group.	
Voice Mail	All parameters	See Voicemail tab descriptions for NuPoint Voice application	
Dial Strings	All parameters	See Dial Strings tab descriptions for NuPoint Voice application	

Centrex Application (Requires system with dual serial port. See Unified Integration for Centrex-like application that works with Precidia.)

Note:
To program a serial port for Centrex, create a line group with an Application setting of "Centrex".

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Dialing Plan	Standard Mode / Length	See Dialing Plan Configuration	
	Classic Mode / Dial Plan		
Centrex	Serial Port		

Tab	Parameter	Description	Value
	Log Serial Port Data Error	Select this check box to log serial port data errors. Clear this check box to prevent logging of serial data errors.	Default is cleared.
	Message Notification		
	Centrex Message Notification	Select this check box to enable message notification. Clear this check box to disable message notification.	Default is cleared.
	Centrex RS232 Link Duplex	Select Full or Half duplex for Centrex communication via the RS232 link.	Default is Full.
	Message Waiting Request Interval	The amount of additional time (ms) that an ESMDI message-waiting task will sleep between sending message requests.	Default is 100 ms.
	Miscellaneous		
	Use calling extension information	Select this check box to have the system use calling extension information. Clear this check box to ignore calling extension information.	Default is cleared.

Tab	Parameter	Description	Value
	Must answer call to get data packet	Select this check box if the switch protocol requires NP-UM to go off-hook on a ringing line before the switch will send the calling information. Clear this check box if the off-hook action is not required.	Default is cleared.
	Centrex data timeout	Enter the time to wait for data when a call is received.	Default is 7 sec. Valid entries are 0-255 seconds.
	Centrex ring timeout	Enter the time to wait for ring before data is received.	Default is 10. Valid entries are 0-255 seconds.
	Baud Rate	Select the baud rate of the serial port.	Default is 1200.
Prefix Strings	Centrex Office Code Prefixes		
	Extensions beginning with n	Select an "extension beginning with" value and enter the digits of the prefix for extensions beginning with that value. For example, if the extension number is 2345, and the phone number is 687-2345, then the prefix for extensions beginning with 2 is 687.	

Tab	Parameter	Description	Value
Voice Mail	All parameters	See Voicemail tab descriptions for NuPoint Voice application	
Dial Strings	All parameters	See Dial Strings tab descriptions for NuPoint Voice application	

Unified Integration

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Unified Integration	Log serial port data errors	Select this check box to log serial port data errors. Clear this check box to prevent logging of serial data errors.	Default is cleared.

Enhanced InBand

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Enhanced InBand	Calling Extension Absorbed Digits	Enter the number of digits to strip from the calling extension.	(0-12)
	Calling Extension Signed Offset	Enter the signed offset to be added to the extension after stripping the leading digits to arrive at a mailbox number.	+ or - (n)

Tab	Parameter	Description	Value
	Called Extension Absorbed Digits	Enter the number of digits to strip from the called extension.	(0-12)
	Called Extension Signed Offset	Enter the signed offset to be added to the extension after stripping the leading digits to arrive at a mailbox number.	+ or - (n)
	MF Enabled	Select this check box to enable use of MF tones. Clear this check box to disable use of MF tones.	Default is cleared.
	Set to T1 Gateway	Select this check box to enable this line group for a MiVoice Business T1 gateway. Clear this check box if there is no T1 gateway requirement.	Default is cleared.

DTMF to PBX Dialer

Tab	Parameter	Description	Value
Lines		See Lines Tab	
DTMF to PBX Dialer	DTMF to PBX Dialer		

Tab	Parameter	Description	Value
	PBX Special Access Code	Some PBXs require the server to dial a special access code before sending message indicators requests. The special access code indicates to the PBX that one of its special features is about to be invoked. For more information, see the Message Waiting Application topic in the *NuPoint Unified Messaging System Administration Online Help*.	Valid characters are 0-9, # *, +, (,), A_H, L, N-U.
	Pre-DN On Dial String	Enter the string to send before the directory number (extension number) to instruct the PBX to turn the message waiting indicator on or off at that station.	
	Pre-DN Off Dial String		
	Post-DN On Dial String	Enter the string to send after the directory number (extension number) to instruct the PBX to turn the message waiting indicator on or off at that station.	
	Post-DN Off Dial String		
	Maximum PBX Message Count	Enter the maximum message count (two chars) of unplayed messages to be included after the mail-box number and before the post DN. If you leave this field blank or set it to 0, no message count is sent.	Valid values are 0 - 99.

Tab	Parameter	Description	Value
	Options		
	Initial Dialtone Detect	Select this check box to enable initial dialtone detection. Clear this check box to disable initial dialtone detection.	Default is selected.
	Dial Tone Confirmation	Select this check box only if (1) a PBX special access code is required and (2) if, after the special access code has been sent, the PBX expects the server to wait for a dial tone before the server outdials any other digits.	Default is cleared.
	Suppress Updates to MWI	Select this check box to prevent the server from sending an indicator-on request when the message indicator is already activated.	Default is selected.
	Wait for Dial Tone	Select this check box if the PBX can return dial tone to the server to indicate that a message indicator has been turned on or off successfully.	Default is cleared.
	Enable Alternate Code	Select this check box when the DN and mailbox number are different.	Default is cleared.

Tab	Parameter	Description	Value
	Use Same Port to Turn On/Off MWI	Select this check box to use the same port to turn MWI on and off. (Some Non-Mitel PBXs require that the MWI of an extension be turned off by the same port that turned it on.)	Default is cleared.

Speech Recognition Parameters

Tab	Parameter	Description	Value
Lines		See Lines Tab	
Speech Recognition	Attendant's Extension	Enter the extension number for the Attendant. (Note: this is an active configuration.)	
	Speech Recognition Application	Select the speech recognition application to associate with this line group. Choices are: - NuPoint Speech Auto Attendant and - Other VoiceXML Application.	
	VoiceXML Start URL	Displays only when the Other VoiceXML application is selected from the Speech Recognition Application list.	

26.37 Configure a Dialing Plan

To configure a standard dialing plan:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. From the navigation tree, click **Line Groups** and then select the line group to which you want to apply a dialing plan. Click **Edit**.
4. Click the **Dialing Plan** tab and use the Standard or Classic fields to enter the dialing plan.
5. Click **Save**.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.38 Transfer to System Attendant

This procedure describes how to configure a server so a caller can press 0 to transfer to an attendant.

To configure transfer to system attendant:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups**, select the line group to modify, and then click **Edit**.
4. On the **Voicemail** tab, in the **System Attendant's Extension** field, enter the number dialed by the application to connect the caller to the PBX attendant.
5. Do one of the following:

1. • To allow a caller to press 0 during, or after, a greeting, select the **Key_0 for Attendant Transfer During Greeting** check box.
   • To allow callers to press 0 only during the login sequence, clear this check box .

1. On the **Dial String** tab, in the **Attendant's Transfer String** field, enter the dial string that will put the caller on hold so the application can dial the PBX attendant.
2. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.39 Prevent Unaddressed Messages

Use this procedure when you want callers to be transferred to the system attendant instead of leaving a message in the attendant's mailbox (an unaddressed message). A system attendant's extension must be configured.

With Message of the Day Capability

1. Edit the Attendant's mailbox using the instructions under Edit Mailboxes.

2. On the **Class of Service** tab, in the **Feature:** field, select **6**.
3. Click **Save**.

Without Message of the Day Capability

1. Edit the NP Receptionist Line Group using the instructions under Edit a Line Group.
2. On the **Voicemail** tab, in the **Attendant's Mailbox Number** field, enter a period (.) which disables the attendant's mailbox. Callers who respond to the wait prompt by waiting will be transferred to the system attendant's extension instead of the attendant's mailbox.

Note:

- If you disable the attendant's mailbox and you do not define a system attendant's extension, be sure to disable the wait prompt. Otherwise, when a caller waits, the server thanks the caller and then hangs up!
- Since the attendant's mailbox is used for recording the message of the day, this capability will no longer be available.

26.40 Enable the Dial by Name Function

To enable Dial-by-Name:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups**, select the line group to edit, and then click **Edit**.
4. On the **Dialing Plan** tab, do one of the following:

   - In **Standard Mode**, select the digit (1-9) that you want to use to trigger the dial-by-name prompt. (For example, if you want the prompt to say "Please enter a mailbox number or press **8** to dial by name.", then select the **(A) Dial by Name** dialing plan from the drop-down list adjacent to position 8.)

     OR
   - In **Classic Mode**, enter the dial plan and include the Dial by Name digit (**A**) in the digit position that will trigger the prompt. (For example, 3,3,3,3,3,3,3,**A**,3 triggers our example prompt, "Please enter a mailbox number or press **8** to dial by name.")
5. Click **Save**.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

Note:
By default, callers must dial a user's last name first. For example, to reach, John Smith, callers would begin dialing S-M-I-T-H followed by J-O-H-N. If you want to switch this functionality and have callers dial a user's first name first (eg. J-O-H-N followed by S-M-I-T-H), you must update the **Last Name First Flag** in the Text Console.

26.41 Configure Media Service (Packet Rate)

To configure packet rate:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Media Service**.
4. In the **Packet Rate** list, select one of the following:
   - **Fixed Packet Rate**: select this option to maintain a fixed packet rate of 20 ms. If a call requiring a non-standard packet rate is made to the NuPoint UM system, it may result in audio distortion.
   - **Variable Packet Rate**: select this option for MCD Release 4.0 (3300 ICP Release 10.0) and later to allow successful streaming of calls that may require a non-standard packet rate.
5. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.42 Verify Configuration Parameters

You can display a list of configuration parameters for each line group, or for all line groups:

1. From the navigation tree, select **Active Configuration > View Active Configuration**.
2. From the **Line Group** list, select a line group to display, or select **all** to see the configuration listing for all groups.
3. Click **View** to display the list onscreen, or click **Download** to open or save the list as a text file for printing.

26.43 Define a Line Group

1. From the Main menu, select **(S) System maintenance**, **(R) Reconfiguration**, **(R) Reconfigure system**, then **(G) Offline Menu**.

2. *Select* **(B) Duplicate Active Configuration**. The system copies the current (active) configuration. When copying is complete, the short form of the Offline menu appears.

> **Note**:
>
> All subsequent steps in this procedure – along with any other configuration entries – affect only the inactive configuration, and will take effect only after you activate the inactive configuration.

3. From the NuPoint Voice Configuration Offline menu, select **(G) Line Groups**.
4. *Select* **(G) Current Group** to specify the line group number.
5. Enter the **number** of the line group (1-24) to be used for the application.
6. Select **(N) Name of Current Group** and enter a descriptive name of the application line group (for example, "Incoming").
7. Add the desired lines:

   Select **(A) Add Lines to Current Group**. Each line number is expressed as a *triplet*, where module, slot, and port number are separated by colons (:). If you have a one-module server, you can refer to just the slot and port number. If you have a multi-module server, you must specify the module number as well, or the server assumes you are configuring Module 1 only. See Module/Slot/Host table.

> **Note**:
>
> Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

All of these formats are valid:

Example	*Specifies*
1: *	All lines
1:0:0-1:0:59	All lines from 0 to 59 on module 1
1:0:*	All lines on module 1
1:0:0-2:0:4	All lines on module 1, slot 0, through module 2, slot 0, port 4

Example	*Specifies*
1:*,2:*	All lines on modules 1 and 2

8. To enable G.729 audio compression (G.711 is enabled by default), select **(P) Enable G729**, and then enter **1** [Yes].
9. Exit to the NuPoint Voice Configuration Offline Menu.
10. Select **(A) Line Group Only applications**. A list of available applications is displayed.
11. Select **(G) Group Selected** and then select the application to configure from the list.

Note:
If this Line Group is going to be used for **Call Director**, select **(V) NuPoint Voice** and then select **(U) User Interface** and **(C) Call Director**.

12. When you have configured the new line group, exit to the main menu and select **(A) Activate Configuration**.
13. When the activation is complete, test the new line group.

Note:
If G.729 audio compression is enabled for the NuPoint UM line group:

- If you enable G.729, you cannot select a Fax Group Connection for the line group.
- For a Mitel 5000 CP integration, access the Speech Encoding Setting field on the 5000 CP (located in System\Devices and Feature Codes\Node IP Connection Groups\<Pxxxx>IP Call Configuration or System\IP-Related Information\Call Configurations) and select **G.729**.
- For a MiVoice Business ICP integration, create a network zone on the MiVoice Business ICP, enable Intra-zone Compression, and then assign all endpoints, including sets and IP extensions mapped to NuPoint ports, to the zone. In addition, make sure to equip the MiVoice Business ICP with Digital Signal Processors (DSPs) that support G.729.
- For a Dialogic Media Gateway integration, access the DMG Web Interface, select the network group for this implementation (located under Configuration > VoIP > Network Groups), and then select **Low Bit Rate Codec** as Audio Codec #1.

26.43.1 Configure a Dialing Plan

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.

2. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, select **(E) Modify Active Configuration**.

3. From the Voice Configuration Menu, select the line group to modify, select **(M) Modify Application** and then **(D) Dialing Plan Menu**.
4. For a standard dialing plan, select **(D) Dialing Plan**. Enter one of the following elements in each of the nine positions as indicated in your NuPoint Voice worksheet, separated by commas:

Element	Explanation
0-11	**Length of the mailbox. Zero means none may start with this number.**
V	**Variable number (1 through 11) of digits; server uses timeout to determine end of mailbox number**
M	**Analog networking (AMIS) mailboxes leading digit**
A	**Dial-by-Name (ASCII) leading digit**
T	**Call placement leading digit**
An	**Networked mailboxes, n = mailbox number length. NV (variable number length) is acceptable**
Pn	**Network mailbox prefix used, n = mailbox length including prefix digit**

See Dialing Plan Examples

Using the Optional Star Prefix Dialing Plan

1. Access the Dialing Plan menu (see steps 1-3 above).

2. To use the Star Prefix dialing plan, select **(E) Optional Star Prefix Dplan**. For example:

   - If you need a star prefix for **Dial By Name**, specify the trigger digit:

     Select (E) Dial By Name Dplan Digit and enter the **digit** that will precede a star to trigger the Dial-by-Name prompt. (For example, to trigger the prompt, "Please enter a mailbox number or press **8** to dial by name." enter "8".)
   - If you need a star prefix for **call placement**, specify the signal digit: *Select* (F) Call Placement Msg Delivery Dplan Digit and enter the **digit** that will precede a star to signal the server that the telephone number following the star is for call placement.
3. Save your entries by exiting to the NuPoint Voice Online Menu. If you chose to modify the Inactive Configuration in step 2, you need to activate the inactive configuration before your changes appear.

26.43.2 Transfer to System Attendant

This procedure describes how to configure a server so a caller can press 0 to transfer to an attendant.

To configure transfer to system attendant:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(R) Reconfigure System**
2. Go to the NuPoint Voice Configuration Online Menu in the active or inactive configuration. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, **select (E) Modify Active Configuration**.
3. Select **(G) Group Selected** and enter the **number** of the line group (1-24), or press **Enter** if the current number is correct.
4. In the application menu, select **(M) Modify Application** and then **(Z) Dial String and Mailbox menu**.
5. Select **(A) System Attendant's Extension** and then enter the system attendant's PBX extension number plus dial string codes (valid dial string codes are listed in the table below) OR enter a **period** (.) to disable the system attendant's extension function.
6. Select **(B) Attendant's Transfer String** and then specify a character from the table below to describe all the dialing steps that the PBX must take to dial the system or mailbox attendant's extension number. This code is represented by the "attendant extension pre-dial index" in the mailbox set-up.
7. Return to the NuPoint Voice Application Menu.
8. Select **(K) Key_0 for Attendant Transfer During Greeting** and then select:

   - **Y** to allow a caller to press 0 during (as well as after) a greeting, **OR**
   - **N** to allow a caller to press 0 only after a greeting has played. This also allows the caller to log into the mailbox, by pressing 0 or star (*).
9. Save the parameter settings by exiting to the Main Menu. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

Dial String Characters	
Character	**Explanation**
0-9, *, #	Keys on a standard pushbutton telephone
(	The following digits should be dial pulsed (10 PPS)
)	Stop pulsing; resume sending DTMF tones
+	Pause for one second
A-D	Fourth column DTMF keys
E	Go off-hook, wait for dial tone or other steady tone (pa ger go-ahead or confirmation tone, for example), then do next item in string
F	Switch hook flash and wait for dial tone
G	Greet - Wait for a voice or computer tone answer
H	Hang up (go on-hook)
L	Wait for an answer supervision signal that indicates the receiving phone has gone off-hook, then dial remaining characters after receiving the signal. Valid only with four-wire connections, not with loop start or ground start ph one lines.
N	Start a new activity; do not go off-hook
O	Ring once
P	Go off-hook, do not wait for dial tone
S	Switch hook flash, no wait required
T	Go off-hook, wait for dial tone
V	Play three seconds of the message for voice pager

26.43.3 Prevent Unaddressed Messages

This procedure describes how to prevent callers from leaving messages in the attendant's mailbox. Use this procedure when you want callers to be transferred to the system attendant instead of leaving a message in the attendant's mailbox (an unaddressed message). A system attendant's extension must be configured.

With Message of the Day Capability

1. From the Main Menu, select **(M) Mailbox Maintenance**, and then **(M) Modify Mailboxes**.
2. Enter the attendant's mailbox number and press **Enter** until you are prompted for New FCOS.
3. At the **New FCOS** prompt, type **6**.
4. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

Without Message of the Day Capability

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Go to the NuPoint Voice Configuration Online Menu in the active or inactive configuration. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it.
   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and enter the number of the line group (1-24) for NP Receptionist OR press **Enter** if the current number is correct.
4. In the NP Receptionist Application Menu, select **(Z) Dial String and Mailbox Menu**.
5. Select **(D) Attendant's Mailbox #** and enter a **period** (.), which disables the attendant's mailbox. Callers who respond to the wait prompt by waiting will be transferred to the system attendant's extension instead of the attendant's mailbox.

Note:

- If you disable the attendant's mailbox and you do not define a system attendant's extension, be sure to disable the wait prompt. Otherwise, when a caller waits, the server thanks the caller and then hangs up!
- Since the attendant's mailbox is used for recording the message of the day, this capability will no longer be available.

6. Save the entry by exiting to the Main Menu. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.43.4 Enable Multiple Messages for Outside Callers

This procedure describes how to allow outside callers to leave multiple messages for multiple mailbox owners in a NuPoint Unified Messaging server with a single call-in. Callers cannot make multiple messages in these cases:

- from tree mailboxes
- when forwarded immediately to a mailbox via a PBX or via an integration that does not allow multiple messages.

To enable multiple messages:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.

2. Go to the NuPoint Voice Configuration Online Menu in the active or inactive configuration. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and enter the **number** of the line group (1-24), or press **Enter** if the current number is correct.
4. Return to the NuPoint Voice Configuration Menu (A/E/F/G/H/X).
5. Select **(M) Modify Application**, and then **(R) NP Receptionist Menu**.
6. Select **(M) Allow Multiple Messages for Outside Caller** and enter **Y** to allow an outside caller to leave more than one message with a single call-in.
7. Save the entry by exiting to the Main Menu. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.43.5 Enable the Dial-by-Name Function

To enable Dial-by-Name:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Go to the NuPoint Voice Configuration Online Menu in the active or inactive configuration. Do **one** of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and enter the **number** of the line group (1-24), or press **Enter** if the current number is correct.
4. Select **(M) Modify Application** and then **(D) Dialing Plan Menu**.
5. Select **(D) Dialing Plan** and code the dialing plan with an **A** in the digit position that triggers a prompt about spelling the name. For example, 3,3,3,3,3,3,3,A,3 would trigger the prompt, "Please enter a mailbox number or press 8 to dial by name." See Configure a Dialing Plan.
6. Exit from the Dialing Plan menu.
7. In the application menu, select **(F) Dial by Name**.
8. Select **(L) Last Name First Flag** and enter **Y** to specify a last name-first name dialing sequence, or **N** to specify a first name-last name dialing sequence. By default, callers must dial a user's last name first when using the Dial-by-Name function. For example, to reach the user John Smith, they would begin entering the keys S-M-I-T-H. The NuPoint UM server search a database for entries that match the series. If it finds more than one match, it plays the names and mailbox numbers of the partial matches. If it finds a unique match, it plays either the user's name or personal greeting.
9. Select **(N) Number of Names Threshold** and enter the **Number** of names (1-9) that the server plays when a multiple partial match occurs. A typical threshold is 3.
10. Select (**E) Exact Match Break** and enter **Y** to allow a mailbox owner's name and mailbox number (or greeting, for an outside caller) to play as soon as a caller enters enough letters to uniquely identify a mailbox owner, or **N** to have the server wait for a caller to either stop entering letters or to press the # key before it responds.

11. Select **(S) Single Digit Access** and enter **Y** to allow a caller to enter a single digit to reach a mailbox after matched names have been played, or **N** to require a caller to enter an entire mailbox number to reach a mailbox after matched names have been played.
12. Select **(M) Suppress Mailbox Number** and enter **Y** to have the server omit the mailbox numbers in the list of names played when there is a match with a dialed name, or **N** to have the server include the mailbox numbers in the list of names played when there is a match with a dialed name.
13. Include feature bit 92 (user will be in Dial-by-Name database) in the FCOS assigned to the mailbox. Customize an FCOS as necessary.
14. Ensure that each mailbox to be accessible through Dial-by-Name shares the same GCOS group (if a bit-mapped GCOS) or GCOS (if an affinity group GCOS).
15. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.43.6 Configure Media Service (Packet Rate)

To configure packet rate:

1. From the Main menu, select **(S) System maintenance**, **(R) Reconfiguration**, **(R) Reconfigure system**, then **(G) Offline Menu**.
2. *Select* **(B) Duplicate Active Configuration**. The system copies the current (active) configuration. When copying is complete, the short form of the Offline menu appears.

All subsequent steps in this procedure – along with any other configuration entries – affect only the inactive configuration, and will take effect only after you activate the inactive configuration.

1. Select **(V) Configure Media Service**.
2. In the Media Service menu, select one of the following:

   - **(F) Fixed Packet Rate**: select this option to maintain a fixed packet rate of 20 ms. **NOTE**: If a call requiring a non-standard packet rate is made to the NuPoint UM system, it may result in audio distortion.
   - **(V) Variable Packet Rate**: select this option for MCD Release 4.0 (3300 ICP Release 10.0) and later to allow successful streaming of calls that may require a non-standard packet rate.

> **Note**:
> These selections are mutually exclusive - when you select one option, the other is automatically disabled.

3. To save your changes, exit to the NuPoint Voice Main menu. Configuration changes will not take effect until you have activated the inactive configuration.

26.43.7 Verify Configuration Parameters

All Applications Except Paging and Message Delivery

1. From the Main Menu, select **(R) Reports.**
2. Select **(C) Configuration** and then select a report configuration type from the following list:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server, or
   - **X** to exit report output options (no report)
3. When prompted, enter the number of the line group to which the application is assigned. Examples of valid formats for this response are:

   - **1** to report the configuration of line group 1
   - **1-4** to report the configuration of line groups 1 through 4
   - **1,2,4-7** to report the configuration of line groups 1, 2, and 4 through 7
   - Press **Enter** to get the configuration of all line groups

The server shows the name of the application assigned to each group specified and displays the parameter settings for that application. To make corrections, go to the appropriate application menu and enter the correct values.

Paging and Message Delivery Applications

1. If you are modifying the Pager or Message Delivery application, go to the Pagers Menu:

   From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and enter the Pager Line Group number. Select **(M) Modify Application**.
4. Select **(S) Show Pagers**. The server displays the pager system number (index number), pager name, access code, and hold time for each pager.
5. Check the displayed configuration for each pager system against your Pager and Message Delivery Worksheet to verify that it is correct.
6. To make corrections, return to the **Pager Systems Supported** option, the **Define Pagers** option, or the **Other Features** option, and then enter the correct values.
7. When your entries are correct, save the parameter settings.

26.44 Add Caller ID to Voice Mail Headers

You can configure mailboxes to include Calling Line ID (CLI) in the headers of voice mail viewed using Web View, or accessed via telephone.

Customize an FCOS to include the following feature bits in the required mailboxes:

- 263 (Store Caller Line ID as a Phone or Mailbox Number)
- **264** (Play Outside Caller User Interface for CLI Capture)

26.45 Description

This topic provides an overview of the following Pager (Outdial) features:

- Pager Overview
- Message Delivery Overview
- Call Placement Overview
- Pager and Message Delivery Allocation
- Cascade Paging

The Pager application causes the NuPoint Unified Messaging server to initiate, rather than receive, a telephone call. Don't let the name "Pager" confuse you. It is used for sending messages to pagers, but also for a number of other functions that require outdials. An outdial is a call placed by the server. Two other uses of this application are message delivery and call placement.

- **Paging** is a function that allows the server to notify a mailbox owner when a message arrives in the mailbox by activating a radio pager. Parameters can be set to limit the hours that a page may be sent, or the types of messages that activate a page.
- **Message delivery** is a function that allows the server to notify a mailbox owner when a message has been received, by calling the mailbox owner at a predefined telephone number and allowing the owner to log into the mailbox. Parameters can be set to limit the hours that a message delivery may be made, or the types of messages that activate the message delivery. If the Cascade Paging feature is enabled and the user receives a new message while the server is in the process of message delivery, the server will not initiate a new notification. If it is disabled, a new message will restart the message delivery function.
- **Call placement** is similar to message delivery, in that it places a call to a telephone number. In this case, the message is made *by* (rather than to) the mailbox owner. The message is addressed to a telephone number rather than to a mailbox. The answering party does not have to log in to hear the message. Call placement was formerly known as "off-system messaging."

Some optional features, such as Cut-through Paging, use the Pager application as well.

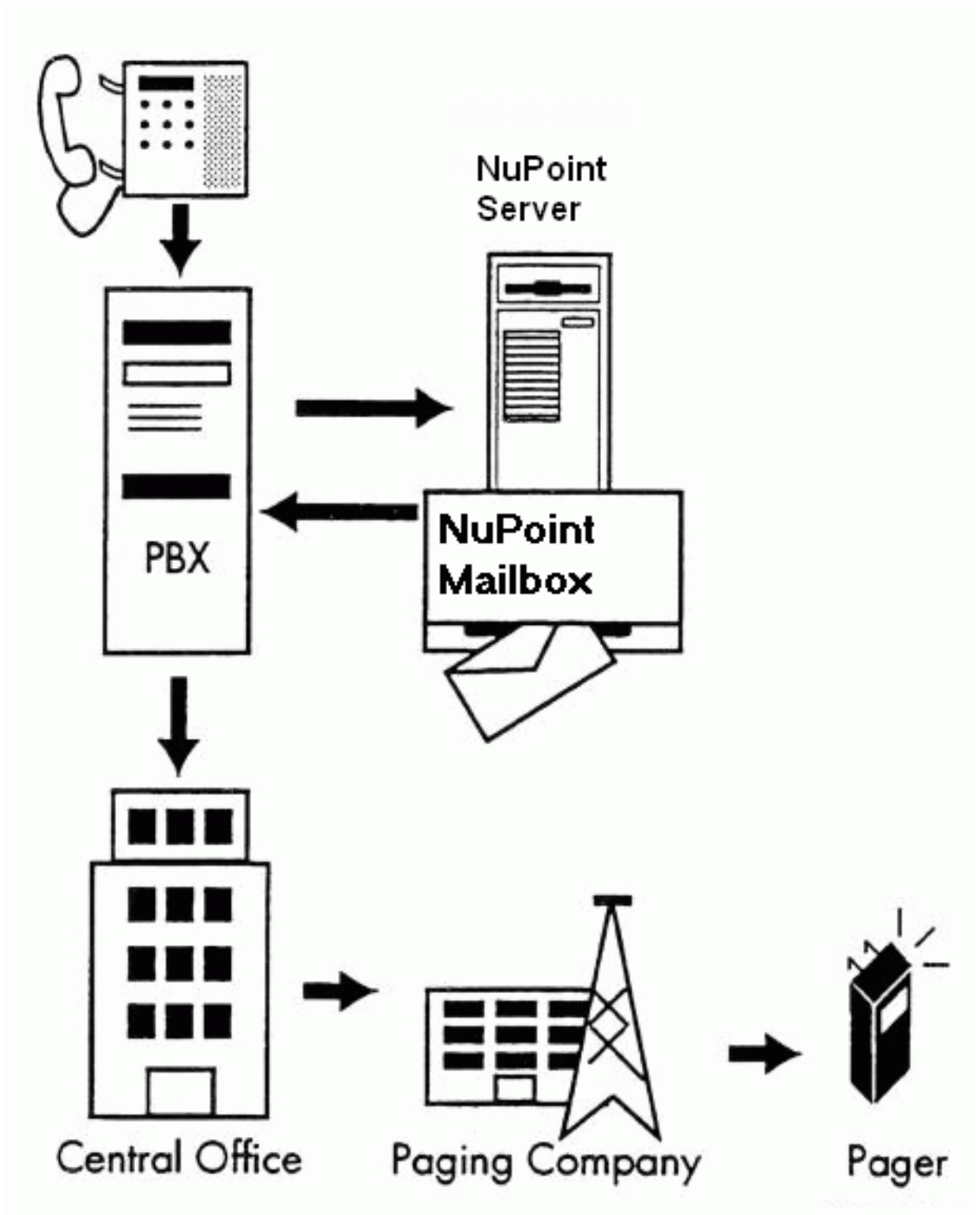
Pager Overview

The NuPoint Unified Messaging server can access the following types of radio pagers:

- **Tone only**: beeps when activated
- **Tone and vibrate**: allows a user to set pager to vibrate when beeping is undesirable
- **Display**: shows the telephone number where the paging party can be reached
- **Voice**: allows a calling party to leave a brief message and can activate the display of a display pager or issue a message for a voice pager when the message is left in a mailbox.

The diagram below shows how one-way paging works in the server. When a message is left in a mailbox configured for paging, the server places a call to the paging company (through the PBX and the CO). The pager then indicates the call.

Pager Call Processing



Features:

- Paging can be activated for specific types of messages.
- Users can specify the hours available for paging.
- Users can enter the number to be paged.

- Limits for paging can be set through the Limits Class of Service (LCOS).
- The server can track number of pages for billing purposes.
- Pages can be billed to a credit card or other billing account.

Message Delivery Overview

Message delivery provides message waiting indication by calling a mailbox owner at a pre-configured telephone number such as a cell phone number. When the phone is answered, the server prompts:

"*Hello <name recorded in the mailbox>. You have <number> unplayed message(s) in your mailbox. Please enter your passcode*."

When the mailbox owner enters a passcode, the server says:

“You have [number] unplayed messages in your mailbox. Press P to play the first message.”

The mailbox owner is now logged into the mailbox, and can use any of the features (Play, Make, Give, etc.) available to that mailbox.

The server prompts for the passcode once, then waits 30 seconds for a response. If someone other than the user answers, and does not know the passcode, the server responds:

“Call back when you can remember your passcode. Good-bye.”

and hangs up.

Message delivery is particularly valuable for users who do not work on-site, and so cannot use ordinary message waiting indicators. Without message delivery, they might have to call in many times a day to receive messages in a timely manner.

Features:

- Message delivery can be activated for specific types of messages.
- Users can specify the hours available for message delivery.
- Users can enter the number to be called.
- Limits for message delivery can be set through the LCOS.
- The server can track number of messages delivered for billing purposes.
- Message delivery calls can be billed to a mailbox owner’s credit card or other billing account.

Call Placement Overview

Call placement (formerly known as “off-system messaging”) allows server users to send messages to the telephones of people who are not server users, that is, who do not have mailboxes. For example, users can send messages when their time at a phone is limited (at a pay phone, for example) and expect the other party to receive their information. A company can send a product announcement to many target customers at once, or a volunteer group can notify its members of a meeting time change. Any mailbox owner can have this feature if you configure the mailbox properly.

Call placement provides voice message delivery by dialing a telephone number entered by the caller. When the phone is answered, the server prompts:

“Hello [recipient’s name]. You have a call from [user name].”

The recipient can accept, reject, delay, or hold the call for 30 seconds. If the call is accepted, the message plays and the recipient can reply to the message.

Call placement is compatible with all applications and integrations.

Features:

- Users can send a single message to any number and combination of mailboxes and call placement numbers.
- The server retries delivery until successful.
- The server administrator can adjust re-dialing interval and frequency.
- A user can give an existing message to an outside number.
- Calls can be passcode protected, to ensure only the intended recipient can play the message.
- Limits for call placement can be set through the LCOS and RCOS (see Other Classes of Service).
- The server notifies users about calls that cannot be delivered.
- The server can track the number of calls for billing purposes.
- Message delivery calls can be billed to a mailbox owner’s credit card or other billing account.

Pager and Message Delivery Allocation

- At least *one port is required to outdial pages; it must be dedicated exclusively to outdialing.*

This means that fewer ports are available to accept incoming calls. If not enough ports are reserved to handle the paging traffic, paging requests will queue, and users will not receive message waiting notification in a timely manner.

Before assigning pagers or message delivery to mailboxes, it is important to analyze call-traffic flow and to decide how much of the system you want to devote to paging.

- Each call to a radio pager ties up an outdialing port for less than one minute. Queuing only becomes a problem in situations when several users have pagers.
- Message delivery requires more ports than paging because each port is tied up for the entire time that the user is logged in.
- If a user does more than simply play the unplayed message (or messages) that activated the message delivery, the outdialing port can be in use for a considerable length of time.
- The installation site (as the calling party) is responsible for any charges that accrue when paging or message delivery calls are made to numbers outside the PBX system.

Cascade Paging

Note: You must use the **Text Console** to enable Cascade Paging.

The Cascade Paging function prevents the server from initiating a new page while a message is already being delivered. The function is disabled by default.

To understand the behavior of Cascade Paging, assume the pager settings for the mailbox are as shown:

Pager Settings	
Mailbox number	2001
Primary Pager Number	2001
Primary Pager Frequency	3
Primary Pager interval	15 min
Alternate Pager Number	3001
Alternate Pager Frequency	3
Alternate Pager Interval	15 min

When Cascade Paging is disabled:

1. A new message arrives in mailbox 2001, initiating a Pager cycle.
2. Extension 2001 rings.
3. If there is no reply from this extension (Ring-No-Answer), the pager system will try to call 2 more times (Frequency setting of 3) after a time interval of 15 minutes (Primary Pager interval) and, if still not answered, will move to the Alternate Pager number to repeat the process.

After there is no reply (RNA) for the first two attempts in the Primary Pager cycle, only one attempt of the Primary Pager remains and after this last attempt the system will call the Alternate Pager.

If, at this moment, a new message arrives in the user's mailbox, the system will behave as if this is first new message and it will restart the Primary Pager cycle.

This scenario continues any time a new message arrives in the user's mailbox.

When Cascade Paging is enabled:

1. A new message arrives in mailbox 2001, initiating a Pager cycle.
2. Extension 2001 rings.
3. If there is no reply from this extension (Ring-No-Answer), the pager system will try to call 2 more times (Frequency setting of 3) after a time interval of 15 minutes (Primary Pager interval) and, if still not answered, will move to the Alternate Pager number to repeat the process.

After there is no reply (RNA) for the first two attempts in the Primary Pager cycle, only one attempt of the Primary Pager remains and after this last attempt the system will call the Alternate Pager.

If, at this moment, a new message arrives in the user's mailbox, the system does not initiate the Primary Pager cycle again. Thus the one attempt remaining for the Primary Pager will be executed and if this remaining attempt is RNA, the system will ring the Alternate Pager Number.

The above scenario continues until the Alternate Paging cycle is complete, even if more new messages arrive in the user's mailbox.

During the Pager call, the user is informed of the total number of unplayed messages in the mailbox.

26.45.1 Configuration Requirements

NuPoint Voice Configuration

Paging, message delivery, and call placement require the following information from the NuPoint Voice configuration:

- The **line group** that will be used for outdials
- **Pager system names**. These are unique names, also called "pager names," to help you identify which pager system you are referring to. An example of a pager system name is "Outside Access."
- **Hold time**. This is the number of seconds that the outdial port remains off-hook after all outdialing is performed. It should be long enough to allow a reorder or busy tone to be returned, which alerts the server that a page has failed. The default value is 20 seconds. The maximum hold time allowed is 90 seconds. Set a value of 3 seconds to clear the port more quickly.
- **Pager systems**. These are outdial indexes that outdial a certain dial string when accessed. Each pager system is represented by a number. (You later enter this number as an internal outdial index, billed outdial index, or unbilled outdial index, and specify the access code index when adding a pager, message delivery, or call placement to a mailbox.)
- **Message delivery** requires enabling the Message Delivery parameter.
- **Call placement** requires:
  - Server features that make it possible for the user to send messages to outside telephone numbers
  - Modification of the NuPoint Voice line group's dialing plan
- Paging and message delivery use message waiting indicators; call placement does not.

Mailbox Configuration

The following information is required in the user's mailbox configuration:

Information Required	Paging	Message Delivery	Call Placement
A properly modified FCOS. (See Class of Service Configuration for Pager or Message Delivery or Call Placement.)	Y	Y	Y
A properly modified LCOS. (See Class of Service Configuration for Pager or Message Delivery or Call Placement.)	Y	Y	Y
The outdial indexes (which point to a specific pager system)	Y	Y	Y
The pager access type (which points to an internal outdial index, billed outdial index, or unbilled outdial index)	Y	Y	Y
The pager number (the telephone number that the server outdials to)	Y	Y	
The pager frequency (the number of times that the server attempts to notify the user of an unplayed message)	Y	Y	
The pager interval (the number of minutes the server waits between repages)	Y	Y	

Information Required	Paging	Message Delivery	Call Placement
The post-pager number (used with display pagers). Once the server has reached the pager number and the call is answered, it then sends the post-pager number to be displayed on the pager.	Y		
The busy pager attempts (the number of times that the server attempts to notify the user of an unplayed message when it receives a busy tone on the last page attempt)	Y		
The busy pager interval (the number of minutes the server waits between re-pages when it receives a busy tone on the last page attempt)	Y		

Pager Application Worksheets

Use these three worksheets to gather and organize the information you need to configure a Pager application:

- Outdial Line Group Worksheet
- NuPoint Voice Application Worksheet
- Mailbox Individual Worksheet

Sample worksheets are shown here. Blank worksheets are available here.

Outdial Line Group Worksheet

- The Outdial Line Group Worksheet organizes information you need to configure the line group that outdials paging and message delivery calls and identify the pager system. A sample Outdial Line Group Worksheet for paging is shown here:

Outdial Line Group Worksheet

Pager Systems Index Plan

Pager System	Pager Name	Access Code	Hold Time
0	Outside Access	T9T	3
1	415 Area Code	T9T1415	3
2	553 Exchange	T9T553	3
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Offline Parameters

Define Line Groups

Current group: 2

Add lines to current group: 1:1:3, 2:0:

Name of current group: Pager Dialer 1

Line Group Only Applications

Group selected: 2

Select application: P

Online Parameters

VoiceMemo Configuration Online Menu

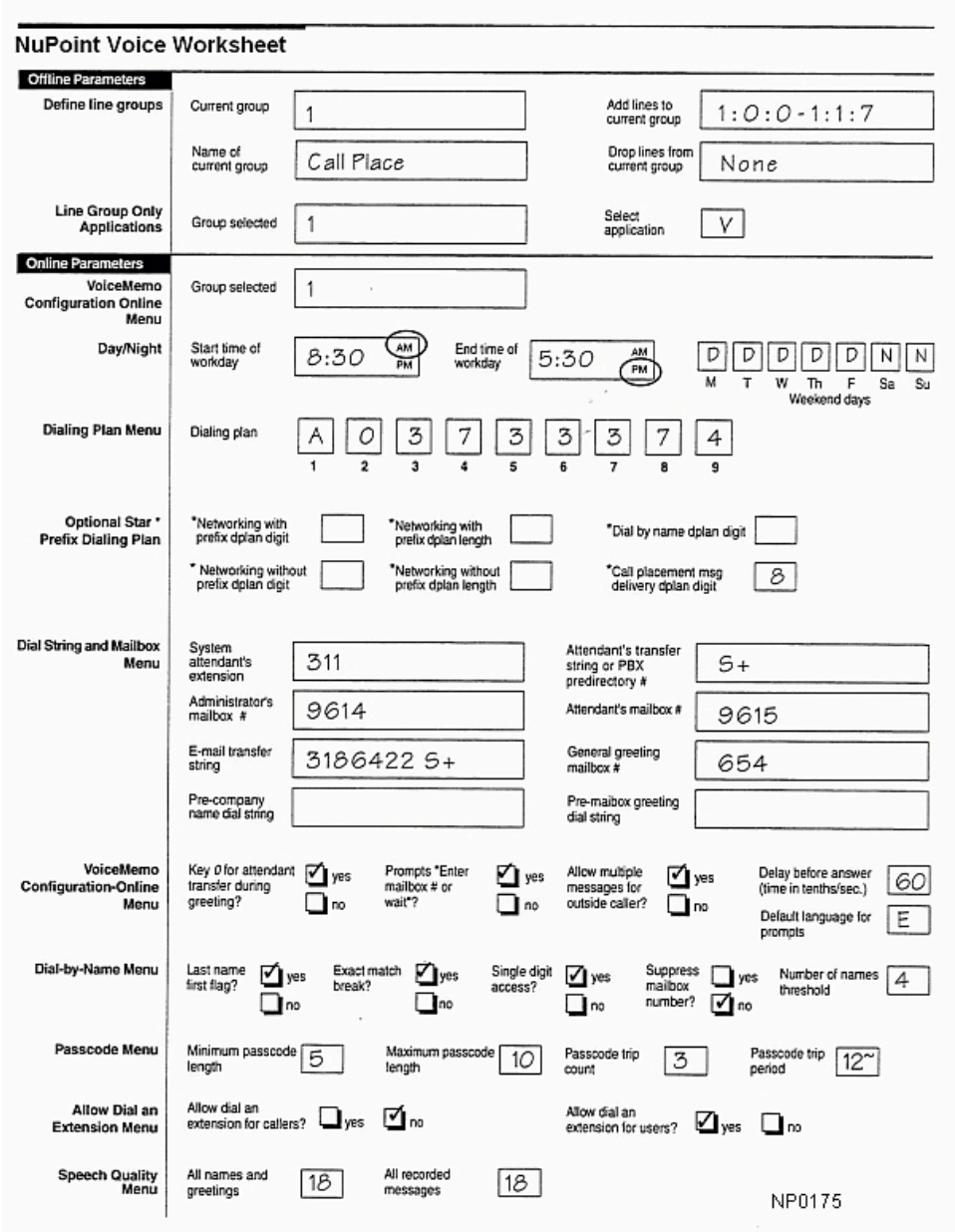
Group selected: 2

Pagers

Pager systems supported (from Pager Systems Index Plan, above): 0,1,2

NuPoint Voice Application Worksheet

- The NuPoint Voice Application Worksheet you completed for the NuPoint Voice application contains information applicable to message delivery and call placement.
- If you are including message delivery in this application, you set all parameters in the Other Pager Features Menu to the same settings as the primary application that is configured on your server. For example, if the NuPoint Voice application is used for processing most calls on your server, copy the entries from the NuPoint Voice Worksheet into the Other Pager Features Menu. (The primary application could be NuPoint Voice or Centrex.)
- If you are including call placement in this application, establish a dialing plan on this worksheet that tells the server that mailboxes starting with the specified digit are actually telephone numbers. See the NuPoint Voice Application section for more information. A sample NuPoint Voice Application Worksheet for call placement is shown here:



NuPoint Voice Worksheet

Offline Parameters

Define line groups
Current group: 1
Add lines to current group: 1:0:0-1:1:7
Name of current group: Call Place
Drop lines from current group: None

Line Group Only Applications
Group selected: 1
Select application: V

Online Parameters

VoiceMemo Configuration Online Menu
Group selected: 1

Day/Night
Start time of workday: 8:30 AM (PM)
End time of workday: 5:30 (AM) PM
M T W Th F Sa Su: D D D D D N N
Weekend days

Dialing Plan Menu
Dialing plan: A 0 3 7 3 3 3 7 4
1 2 3 4 5 6 7 8 9

Optional Star * Prefix Dialing Plan
*Networking with prefix dplan digit:
*Networking with prefix dplan length:
*Dial by name dplan digit:
* Networking without prefix dplan digit:
*Networking without prefix dplan length:
*Call placement msg delivery dplan digit: 8

Dial String and Mailbox Menu
System attendant's extension: 311
Attendant's transfer string or PBX predirectory #: S+
Administrator's mailbox #: 9614
Attendant's mailbox #: 9615
E-mail transfer string: 3186422 S+
General greeting mailbox #: 654
Pre-company name dial string:
Pre-mailbox greeting dial string:

VoiceMemo Configuration-Online Menu
Key 0 for attendant transfer during greeting? yes / no
Prompts "Enter mailbox # or wait"? yes / no
Allow multiple messages for outside caller? yes / no
Delay before answer (time in tenths/sec.): 60
Default language for prompts: E

Dial-by-Name Menu
Last name first flag? yes / no
Exact match break? yes / no
Single digit access? yes / no
Suppress mailbox number? yes / no
Number of names threshold: 4

Passcode Menu
Minimum passcode length: 5
Maximum passcode length: 10
Passcode trip count: 3
Passcode trip period: 12~

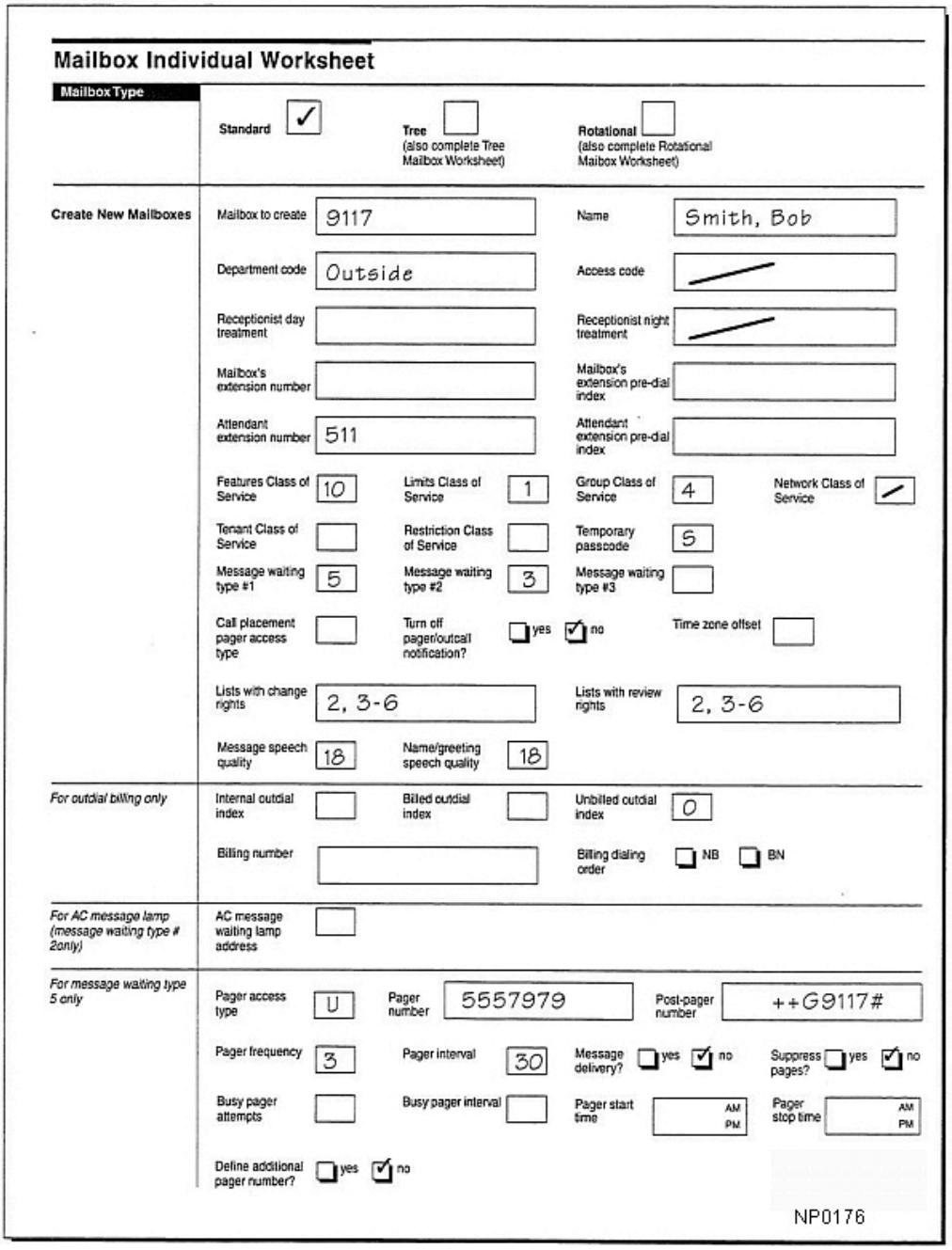
Allow Dial an Extension Menu
Allow dial an extension for callers? yes / no
Allow dial an extension for users? yes / no

Speech Quality Menu
All names and greetings: 18
All recorded messages: 18

NP0175

Mailbox Worksheet

- The Mailbox Worksheet organizes information you need to configure individual mailboxes for paging, message delivery, or call placement, or any combination of these functions.
- If you are including call placement in this application, specify the appropriate outdial index and access type for call placement. Also specify the appropriate FCOS and LCOS for call placement. A sample Mailbox Worksheet for paging is shown here:



Mailbox Individual Worksheet

Mailbox Type

Standard ✓ | Tree ☐ (also complete Tree Mailbox Worksheet) | Rotational ☐ (also complete Rotational Mailbox Worksheet)

Create New Mailboxes

Mailbox to create: 9117		Name: Smith, Bob	
Department code: Outside		Access code: /	
Receptionist day treatment:		Receptionist night treatment: /	
Mailbox's extension number:		Mailbox's extension pre-dial index:	
Attendant extension number: 511		Attendant extension pre-dial index:	
Features Class of Service: 10	Limits Class of Service: 1	Group Class of Service: 4	Network Class of Service: /
Tenant Class of Service:	Restriction Class of Service:	Temporary passcode: 5	
Message waiting type #1: 5	Message waiting type #2: 3	Message waiting type #3:	
Call placement pager access type:	Turn off pager/outcall notification? ☐ yes ☑ no	Time zone offset:	
Lists with change rights: 2, 3-6		Lists with review rights: 2, 3-6	
Message speech quality: 18	Name/greeting speech quality: 18		

For outdial billing only

Internal outdial index:	Billed outdial index:	Unbilled outdial index: 0
Billing number:	Billing dialing order ☐ NB ☐ BN	

For AC message lamp (message waiting type # 2only)

AC message waiting lamp address:

For message waiting type 5 only

Pager access type: U	Pager number: 5557979	Post-pager number: ++G9117#	
Pager frequency: 3	Pager interval: 30	Message delivery? ☐ yes ☑ no	Suppress pages? ☐ yes ☑ no
Busy pager attempts:	Busy pager interval:	Pager start time: AM PM	Pager stop time: AM PM
Define additional pager number? ☐ yes ☑ no			

NP0176

26.45.2 Line Groups for Outdial Functions

Use the information in the following paragraphs for entries on the NuPoint Voice Worksheet and Outdial Line Group Worksheet.

Guidelines for Port Allocation

The server requires at least one port to outdial calls for paging, message delivery, and call placement. Outdialing ports must be dedicated exclusively; this means that there will be fewer ports available to accept incoming calls. If enough ports are not reserved to handle the outdial traffic, however, the requests are queued, and users do not receive message waiting notification or messages in a timely manner. Before assigning pagers or message delivery to mailboxes, you should analyze call traffic flow and decide how much of the server you wish to devote to outdials.

Each call to a radio pager ties up an outdialing port for less than a minute; queuing becomes a problem only when there is a large number of users with pagers. Message delivery can require more ports than paging, since each port is tied up for the entire time that the user is logged in. For example, if a user does more than simply play the unplayed message that activated message delivery, the outdialing port can be in use for a considerable amount of time. Call placement is more like message delivery because ports are in use for more time than for paging.

Note:
The server installation site, as the calling party, is responsible for any charges that accrue when paging, message delivery or call placement calls are made to numbers outside of the PBX system.

Line Group Information

All server ports are assigned to line groups. Each line group, in turn, is assigned to a single application, and any configuring that is done for that application applies to every port in the line group. The number of ports in each line group depends on how heavy the phone traffic is expected to be for the particular application.

Line Group Number

Each line group is represented by a discrete number. Valid line group numbers are 1 through 24.

Group Name

The group name should identify the line group's purpose. For example, "Pager Outdialer."

Lines in Group

You identify each line (or port) in a group by a triplet, which represent the module, slot, and port. Module refers to a CPU, the server's main processor. Modules are numbered at 1. Slots are numbered at 0. Ports are also numbered from 0 and the upper limit depends on the port limit of your system licensing.

For more information about line groups, see About Line Groups.

Call Placement

To use call placement, you must change the dialing plan. Use the letter T as a dialing plan entry. For example, if you entered T in position 8 of the plan, users would enter 8 from the keypad to activate the call placement function. You can use T in any position of the dialing plan, but only once. See About Dialing Plans for more information.

Pager Systems Supported

You can configure the server with up to 16 different outdial access codes, each identified by an index number (0-15). Each outdial line group does not need to support all access codes; for example, a line group dedicated to radio paging for the local area code does not need to support an access code designed for long distance call placement. Assigning only the required access codes to an outdial line group makes it easier to plan and control traffic and prevent abuse.

The mailbox configuration specifies these access codes for use in placing internal calls, unbilled external calls, and external calls charged to a billing number. You enter the appropriate pager system numbers as the internal outdial index, billed outdial index, and unbilled outdial index.

The Pager Systems supported parameter assigns specific pager systems to the line group that is currently selected. You should analyze your needs carefully before assigning pager systems. For example, if your server will have message delivery, call placement, and outdialing to radio pagers, you should take into account the fact that a single message delivery can take several minutes (while the user plays the message, answers it, etc.), while activating a radio pager takes a fraction of that time. Therefore, you might want to assign pager systems that outdial call placement or message delivery calls to a larger line group.

26.45.3 Dial Strings for Outdials

When you are configuring the server to outdial, you create a dial string to duplicate the manual steps that you would perform to dial a pager or place a phone call.

Define the Operations Required to Page or Place a Call

Paging (Calling the Pager)

Many PBXs require that you dial an access code to get an outside line. To call the pager, you usually dial the pager company telephone number, listen for a pager tone, then dial the code number of the pager. Before you dial the pager company telephone number, however, you pick up the receiver on the telephone, and listen for a dial tone to be sure that the telephone system is ready to accept the number that you dial. The steps for successfully activating this pager, therefore, are to:

1. Go off-hook and listen for the dial tone
2. Dial any access code necessary to get an outside line
3. Dial the pager company telephone number
4. Listen for the pager tone
5. Dial the pager number

All of these steps must be configured.

Message Delivery and Call Placement

Many telephone switches require that you dial an access code to get an outside line. The sequence of events that you perform (other than dialing the actual number), such as waiting for tones, must be configured in the dial string.

Translate the Required Operations to a Dial String

This table lists the characters that the server recognizes as the steps required to page or to place a call. You use these characters to make up your dial string:

Dial String Characters

Character	Explanation
0-9, *, #	**Keys on a standard push button telephone**
(	**The following digits should be dial pulsed (10 PPS)**
)	**Stop pulsing; resume sending DTMF tones**
+	**Pause for one second**
A-D	**Fourth column DTMF keys**
E	**Go off-hook, wait for dial tone or other steady tone (pager go- ahead or confirmation tone, for example), then do next item in string**
F	**Switch hook flash followed immediately by dialing**
G	**Greet - Wait for a voice or computer tone answer**
H	**Hang up (go on-hook)**

Character	Explanation
L	**Answer Supervision-** Wait for an answer supervision signal that indicates the receiving phone has gone off-hook, then dial remaining characters after receiving the signal. Valid only with four-wire connections, not with loop start or ground start phone lines.
N	**Start a new activity; do not go off-hook**
O	**Ring once**
P	**Go off-hook, do not wait for dial tone**
S	**Switch hook flash, no wait required**
T	**Go off-hook, wait for dial tone**
V	**Voice pager: play first unplayed message (and update mailbox to count it as played).**

Note:
The server always assumes a G (wait for greeting) as the last character in a message delivery dial string.

The dial string that you formulate is divided into three parts:

- Pager system access code: identified by the pager system index number, contains the first part of the dial string necessary to reach the user's pager. It is usually the part of the dial string that is common to some group of users. A pager system index number from 0 to 15 that assigns a pager system to a mailbox. If you do not select an outdial index for a pager schedule, the server cannot issue a page when a message is left in that mailbox.
- Pager number: is the balance of the dial string necessary to reach the user's pager.
- Post-pager number: used as the data to display on a display pager.

Note:
If there is no pager or post pager dial string entered, a page will not be sent.

Design Rules

When designing your dial strings, observe the following rules in assigning each of the three components:

- The first character in the dial string must make the server go off-hook and wait for a dial tone. A T is recommended.
- An F (switch hook flash) produces the switch hook flash followed immediately by dialing
- The access code is always outdialed before the pager number. The dial string used is dependent on the pager system selected.
- The pager system part of the dial string is limited to 30 characters.
- Only 16 pager systems can be stored in the NuPoint Voice configuration at any one time, regardless of the number of paging groups configured. However, each pager system can be shared by many users or line groups.
- The pager number is limited to 16 characters. The server administrator enters it in a mailbox's configuration.

Programming Notes:

1. After the last character is outdialed, the system goes on-hook ("hangs up") automatically, except when message delivery is specified.
2. When a mailbox is programmed for message delivery, the system automatically waits for a greeting. (If a G is erroneously programmed at the end of the dial string, the system ignores it.)
3. A "V" anywhere in the dial string causes the system to play the first unplayed message only. If there is more than one message in the mailbox, the user will probably be paged again. The next unplayed message will play because each unplayed message generates its own paging request.
4. When the system is programmed to outdial a telephone number to the outside network, and the number is followed by a G (wait for person or pager to answer), the "clicks" and "pops" of particularly noisy switching equipment may be misinterpreted as a greeting. To avoid any misunderstanding, dial the telephone number, then count the number of seconds it takes for the receiving telephone to ring or the pager to answer. If the call is made to a pager, insert the appropriate number of plus signs (+) between the number and the G. For example, if the dial string is "T9T5551212G," and it took five seconds to answer, change the string to "T9T5551212+++++G."
5. Since Message Delivery always assumes a G at the end of the dial string, insert the appropriate number of plus signs (+) at the end of the pager number.
6. You can use the Answer Supervision (L) code if you have analog phone lines. This is a good alternative to the Greet (G) code, because answer supervision can increase reliability and lower connect time. **Answer supervision time out** controls how many seconds the system waits until issuing a time out. If the system does not detect answer supervision (a ringing on the line) by the number of seconds set in this exception, the page is considered a failure. This time out can be set between 0 and 255 seconds, where 0 means no time out period is enforced (wait forever).

Examples:

Example 1:

To page John Smith **manually**, you must lift the telephone receiver, wait for a dial tone; dial 9 to get an outside line; listen for another dial tone; dial (408) 555-9876; allow two seconds for the line to settle; listen for computer tone; then dial 1234. This makes John���s pager beep or vibrate. The code for these actions is:

T9 **4085559876** **++** **G** **1234**	Wait for dial tone. Tell the PBX that you want an outside line Call the pager company's number Wait for the line to settle Wait for computer tone Dial the number of the individual pager

Example 2:

Mary Jones has a DID display pager. To access this pager **manually**, you must lift the telephone receiver; wait for a dial tone; dial 9 to get an outside line; listen for a dial tone; dial (916) 325-9116; wait four seconds for the call to go through; wait for a computer tone; dial the display data, 237-6644; and press the # key (pound) to tell the pager that all the display data has been entered. This process activates the pager. The code for these actions is:

T9 **9163259116** **++++** **G** 2376644 **#**	Wait for dial tone. Tell the PBX that you want an outside line Dial (916)325-9116 Wait four seconds for the call to go through Wait for computer tone Dial the display data Press the pound key to indicate all data has been entered

Note:
When designing your paging setup, choose your pager system dial strings carefully. You can only refer to 16 pager system access codes *per server*.

Reporting Pager System Access Codes

You can create a report of pager systems, and their indexes and dial strings, by running the Pager Access Codes report from the Reports Menu in the **Text console**.

The server displays the available indexes, dial strings, and pager names (“paging system names”) as in the following example.

Sample Report of Pager Systems Access Codes

PAGER SYSTEMS ACCESS CODES			
Mon Aug 10 10:59:33 20XX			
INDEX	**PAGER NAME**	**ACCESS CODE**	**HOLD**
0	INTERNAL	T	10
1	EXTERNAL	T9	10
2	415 Area Code	T91415	20
3	PAGER 916-325	T91916325	20
4	Empty		
5	<no name>		
6	<no name>		
7	<no name>		

PAGER SYSTEMS ACCESS CODES			
Mon Aug 10 10:59:33 20XX			
INDEX	PAGER NAME	ACCESS CODE	HOLD
8	<no name>		
9	<no name>		
10	<no name>		
11	<no name>		
12	<no name>		
13	<no name>		
14	<no name>		
15	<no name>		
Press any key to continue....			

Note that, in this sample, pager systems 5 through 15 have no name. These are pager systems that are not yet set up. Pager system 4 (Empty) is set up for use with pagers whose entire dial strings are contained in the pager number.

If you need to add a pager that requires the outdialing of more than 16 characters (i.e. the coding string is too long to fit into the pager number field) and no appropriate outdial index exists, you must configure a new pager system before you can add the pager.

26.45.4 Class of Service for Pager Mailboxes

You must customize an FCOS to give a mailbox its pager features and limits.

Features COS

The Feature bits listed in the following table control paging:

Feature Bit	Function
070	User Options Menu
077	Enable paging from a telephone; allow schedule changes from a telephone
079	Set message wait # 1 for urgent messages only
080	Set message wait # 2 for urgent messages only
124	Change paging number
168	Message wait 1, pager requeue
169	Message wait 2, pager requeue
181	Paging over message delivery, message waiting 1 over message waiting 2
182	Use pri/alt as week/weekend for MWI (message waiting type) 1
183	Use pri/alt as week/weekend for MWI (message waiting type) 2
212	Send page upon answer, greeting-only mailbox

Two that deserve special mention affect changes to the weekday/weekend schedule and pager re-queuing.

Change Weekday/Weekend Schedule/Paging Number

Users of the Pager application can be configured to perform the following tasks:

- set schedules for weekdays or weekends, showing when they can be reached
- change their paging number using their telephone.

To change a paging schedule, the corresponding mailbox must have an FCOS that includes feature bit 077 (Change pager schedule). To change a paging number, a mailbox owner's mailbox must have an FCOS that includes bit 124 (Change paging phone number). Both these bits require bit 070 (User Options Menu)

to work. The mailbox owner's mailbox FCOS must contain bit 182 or 183 to change the schedule according to the weekday or weekend.

Note:

- **M**ailbox owners whose pager number contains non-numeric characters (G,T, or +) will not be able to change these numbers correctly using the telephone key pad. We suggest you use Post-pager number field to enter the non-numeric values.
- Scheduling is not available when TDD is enabled.

Pager Re-Queue

The pager re-queue feature is activated by feature bit 168 for schedule one and bit 169 for schedule two. If you have paging scheduled from 9 a.m. to 5 p.m. and receive a call at midnight, the server does not automatically page you at 9 a.m., and does not page until another message arrives during the scheduled time period. By including these feature bits in the FCOS you assigned to the paging mailbox, you are called as soon as the scheduled start time begins, instead of having to wait for another message.

For more information about FCOS and feature bits, see Features Class of Service.

Limits COS

The limits listed in the following table affect paging mailboxes:

Limit	Unit	Default	Valid Values
Paging - phone, length	digits	7	3-11
Message Waiting Indicator Msg Length	seconds	0	0-5
Pages per billing period	pages	0	0-999
Receipt retention, regular	hours	0	0-8760

Paging - Phone Length

This limit controls user modification of paging. The paging phone length determines the maximum number of digits users can enter for a paging number. The default is 7, the allowable range is 3 to 11 digits. It is useful for preventing long-distance calls.

MWI Message Length

This limit defines the minimum message length that activates paging or message delivery

Pages per Billing Period

This limit can control the number of pages allowed for a billing period. This allows server administrators to control the number of paging functions allowed a user per billing period, and can be used where a paging service is sold for a flat fee per month. A setting of 0 means no limit is set.

Receipt Retention, Regular

This limit is used in the Pager application to limit the amount of time regular receipts are kept. (The Receipt Retention, CTP limit is used with the Cut-through Paging optional feature.) The limit can be up to 8760 hours (1 year). Alternatively, you can specify unlimited receipt retention by entering 0.

For more information about LCOS and limits, see Other Classes of Service.

26.45.5 COS for Message Delivery

This section covers specifics applicable only to message delivery. Remember that you must set the Message Delivery parameter to Yes in the mailbox owner's mailbox configuration to enable message delivery.

Features COS

You must customize an FCOS to give a mailbox its message delivery features and limits.

The feature bits listed in the table below control message delivery:

Feature Bit	Function
070	**User Options Menu**
079	**Set message wait # 1 for urgent messages only**
080	**Set message wait # 2 for urgent messages only**
094	**Enable message delivery; change message delivery options**

Feature Bit	Function
143	Change message delivery phone number
168	Message wait 1, pager requeue
169	Message wait 2, pager requeue
181	Paging over message delivery, message waiting 1 over message waiting 2
182	Use pri/alt as week/weekend for message waiting type 1
183	Use pri/alt as week/weekend for message waiting type 2

Change Weekday/Weekend Schedule

Message delivery users can set schedules for weekdays or weekends , showing when they can be reached.

To change a message delivery schedule, a user's mailbox must have an FCOS that includes feature bit 094 (Enable message delivery; change message delivery options). To change a message delivery number, a user's mailbox must have an FCOS that includes bit 143 (Change message delivery phone number). Both these feature bits require bit 070 (User Options Menu) to work.

Pager Re-Queue

The pager re-queue functionality is activated by feature bit 168 for schedule one and bit 169 for schedule two. If you have message delivery scheduled from 9 a.m. to 5 p.m. and receive a call at midnight, the server does not automatically call you at 9 a.m., and does not call you until another message arrives during the scheduled time period. With this feature, the server calls you at the beginning of the next scheduled message delivery start time.

For more information about FCOS and feature bits, see the Features Class of Service section.

Limits COS

Only one limit applies to message delivery, the Message Delivery-Phone Length limit. It controls user modification of message delivery. The message delivery phone lengths determine the maximum number of digits users can enter for a message delivery number. The default is 7, the allowable range is 3 to 11 digits. The limit is useful for preventing long-distance calls.

For more information about LCOS and limits, see the Other Classes of Service section.

26.45.6 COS for Call Placement

This section covers specifics applicable only to call placement. Remember that you must set the outdial indexes and the call placement pager access type parameters in the user's mailbox configuration to enable call placement.

Features COS

You must customize an FCOS to give a mailbox its call placement features and limits.

To use call placement, you must add feature bit 110 (Give/make to telephone number) to an existing FCOS or create a new one with this feature in it.

Limits COS

The limits listed in the table below control call placement. You might need to change the LCOS assigned to the call placement mailbox configuration accordingly.

Limit	Unit	Default	Valid Values
Ring No Answer retry limit	**no. of retries**	**10**	**1-255**
Ring No Answer retry interval	**minutes**	**60**	**1-255**
Busy retry limit	**no. of retries**	**10**	**1-255**
Busy retry interval	**minutes**	**10**	**1-255**
Phone length	**digits**	**7**	**3–11**
Recipient Count	**no. of recipients**	190	**1–190**
Max Msg Length	**minutes**	**5**	**0–60**

Ring No Answer (RNA) Retry Limit

This limit determines the maximum number of times the server redials a call placement phone number when no one answers the phone on the first delivery attempt.

RNA Retry Interval

This limit determines how often the server redials a call placement phone number when no one answers the phone on the first delivery attempt.

Busy Retry Limit

This limit determines the maximum number of times the server redials a call placement phone number when the server detects a busy signal on the first delivery attempt.

Busy Retry Interval

This limit determines how often the server redials a call placement phone number when the server detects a busy signal on the first delivery attempt

Message Phone Length

This limit determines the maximum number of digits users can enter for a call placement phone number. Setting this limit higher accommodates long-distance calls.

Recipient Count

This is the maximum number telephone numbers you can enter at any one time, for a single message. This includes both call placement, and AMIS messages.

Maximum Message Length

The length determines the maximum size of a single message made for a call placement phone number.

If you send a message to both mailboxes and telephone numbers, this limit interacts with the limit on the size of messages sent to mailboxes; the shorter of the two limits overrides the longer. For instance, if you limit messages sent to mailboxes to a maximum of five minutes and limit call placement messages to two minutes, the server enforces the two-minute limit for both kinds of messages.

For more information about LCOS and limits, see Other Classes of Service.

26.45.7 Mailboxes for Paging

To use the Pager application, you must configure mailbox parameters as well as offline and online parameters. You must set different mailbox parameters for each capability (paging, message delivery, call placement). This section provides a description of each parameter.

Creating or Modifying Mailboxes for a Pager Application

After specifying the classes of service, you identify the outdial index for the pager system as an internal outdial, billed outdial, or unbilled outdial.

When you select message waiting Pager (or type 5) when creating or modifying a mailbox, you must set the following parameters:

- Pager access type
- Pager number

- Post-pager number
- Pager frequency
- Pager interval
- Message delivery enabled or disabled
- Suppressing of pages enabled or disabled
- Busy pager attempts
- Busy pager interval
- Pager start time
- Pager stop time
- Additional pager (alternate pager)

Pager Access Type

The dial string that you formulated when configuring the Pager application is divided into three parts. The first part of the string is the pager system access code, which is represented in the mailbox by the outdial index. If you do not select an outdial index for a pager schedule, the server cannot issue a page when a message is left in that mailbox. See Configure Dial Strings for Outdials for more information.

Pager Number

The pager number tells the server what numbers and/or characters to dial after the pager system dial string, and before the post-pager number. See Configure Dial Strings for Outdials and Preparing for Mailbox Programming for Pagers.

Pager numbers are limited to 16 characters.

A mailbox FCOS with feature bit 124 (User can change paging phone number) or 143 (User can change message delivery number) allows the user to change the pager number without affecting the post-pager number. Refer to Features Class of Service for more information about FCOS and feature bits.

Post Pager Number

The post-pager number is used in two cases. With display pagers, the post-pager number (typically the NuPoint Voice telephone number or the mailbox owner's mailbox number) is displayed on the pager screen. A second use is when the mailbox owner can change the pager number, and non-numeric pager dial string characters must be transmitted after the pager number to ensure a successful page. If the mailbox owner changes the pager number, then these non-numeric characters cannot be entered on the telephone set. In this case the post-pager number tells the server what numbers and/or characters to dial after the paging or message delivery number a user enters from the keypad. Such characters include G, +, and T. Mailbox owners cannot alter this post-pager number from the keypad.

Post-pager numbers are limited to 24 digits.

Pager Frequency

The pager frequency is the maximum number of times that the server attempts to notify the user of an unplayed message, if each page is successful. The default pager frequency is 3.

A page is considered successful if the server places the call and it is answered. In other words, the server does not encounter a busy signal, reorder tone, or Ring No Answer after the pager/message delivery call is made. After a successful page is made, the server waits the number of minutes that are specified for the pager interval (below) and then, if there is still an unplayed message in the mailbox, repeats the page.

If the page is unsuccessful, the server retries the number until a successful page is made. For this reason, it is very important that you make a test call to verify that pager configuration is correct.

Pager Interval

This is the length of time (0-255 minutes) the server waits between pages. The default is 30 (wait 30 minutes between pages).

Message Delivery Enabled or Disabled

This parameter activates the message delivery option of paging. When enabled (set to Y), a new message causes the server to call the telephone number defined for message delivery, and ask whomever answers to log into the user's mailbox. Then the user can hear the message and perform other NuPoint Voice operations.

If message delivery is enabled, paging is not available for that message waiting type. However, you can set one message waiting type for paging and another one for message delivery. Or, on the same message waiting type, you can set the primary pager for paging and the alternate pager for message delivery. The default is N, no message delivery.

Suppress Pages

This parameter turns off the paging feature without removing all the settings. Use this option to temporarily remove the paging option from a mailbox. The default is N, do not suppress pages. Set this field to N to resume the paging option after turning it off.

Busy Pager Attempts

This is the number of times (0-255) the server retries the page until it completes the specified number of pages or completes a successful page. Set the number of attempts to a high number if the server will be encountering busy pager systems.

The default is 0 (unlimited retries).

Busy Pager Interval

This is the length of time (0-255 minutes) the server waits between pages when a busy signal has been received. Set the Busy Pager Interval lower than the Pager Interval setting. The idea is that if a busy signal has been received, the page should be retried sooner than if speech or silence was received.

The default is 0 (retry every minute).

Pager Start Time

This is the time that the server starts sending pages for this mailbox. To have paging available 24 hours per day, set both start and stop time to 12:00 a.m.

Enter the time in the form **hh:mm xm**, where **hh** is hours, **mm** is minutes, and **xm** is either a.m. or p.m. The default is 12:00 a.m.

Pager stop time

This works with Pager start time, above, and is the time the server stops sending pages for this mailbox. The default is 12:00 a.m.

Define an Additional Pager?

Each mailbox can be configured with up to three message waiting types, and all are activated simultaneously. For example, Message Waiting type #1 could be a pager, and Message waiting type #2 could be a message waiting light.

Note:

- Call placement does not require a message waiting type
- You cannot use the third message waiting type for the Pager application, because it can only be used for the Centrex message waiting type.

You can set up two message waiting types as pagers, each with a primary and an alternate number. So Message waiting type 1 and message waiting type 2 would both have a primary pager number and an alternate pager number. Your mailbox can then be configured to contact up to four pagers or four message delivery numbers, or any pager/delivery number combination. When you designate two message waiting types as pagers, both are activated. The alternate pager numbers, however, are only activated when the primary pager numbers do not receive a successful response.

If you want to use one pager number as a primary and one as a backup, and no other message waiting function, then set up one primary and one alternate pager number using only the message waiting type #1 parameter).

The alternate pager numbers can also be used to assign a second frequency and/or interval to the same pager number.

Note:
The pager numbers are sometimes called “pager 1,” “pager 2,” “pager 3,” and “pager 4.” Pager 2 is an alternate for pager 1, using the first message waiting type parameter, and pager 4 is an alternate for pager 3, using the second message waiting type parameter. See the following table. (These numbers are allocated by how many pager numbers are set up, however.)

Designation	Message Waiting Type Parameter 1	Message Waiting Type Parameter 2
Primary	Pager 1	Pager 3

Designation	Message Waiting Type Parameter 1	Message Waiting Type Parameter 2
Alternate	Pager 2	Pager 4

EXAMPLE: If a user has message delivery, and you want to page twice, five minutes apart, then—if the message has not played—page three times, 30 minutes apart; assign pagers as follows:

Pager 1: frequency of 2, interval of 5

Pager 2: (same Pager number) frequency of 3, interval of 30

26.45.8 Preparing for Mailbox Programming for Pagers

Whether you are programming the system to outdial to a pager or to call a user to provide message delivery, the principle is the same; you want the system to duplicate the steps to activate the pager or to place the phone call. These steps must be programmed into the pager outdial index (access code index) and pager number (“Step 3: Choose Pager System Outdial Index and Pager Number”).

When you select Message Waiting Type 5 (Pager) while creating a mailbox, the system prompts you for an outdial index, a pager number, a pager frequency, and a pager interval. You can program up to three pagers (pagers 1, 2, and 3) per mailbox. Use the following procedure to answer prompts.

Step 1: Determine the Activation Protocol

Manually activate the pager, or call the user who wants message delivery; as you do, carefully note exactly what steps were necessary.

Example:

Many pagers require that you dial the telephone number of the pager company, listen for a computer tone, then dial the code number of the pager. However, before dialling the pager company telephone number, pick up the telephone receiver and listen for a dial-tone to be sure that the telephone system is ready to accept the number.

The steps for successfully activating this type of pager are as follows:

1. Go offhook and listen for the dial tone.
2. Dial the pager company number.
3. Listen for the computer tone.
4. Dial the pager number.

Step 2: Formulate the Coding String

Translate the activation protocol into a coding string that the system understands. Use the following codes to describe your actions:

Code	Description
0-9,#,*	Send out these DTMF tones (as if they are dialed from a standard touch-tone telephone)
A-D	Outdial these fourth column DTMF tones (keys on spec ial phones)
T	Go offhook and wait for a dial tone
( )	Digits enclosed should be dial pulsed (all other tones are DTMF)
+	Pause for one second
G	Greet - wait for a person or pager to answer
F	Switch hook flash and wait for dial tone
S	Switch hook flash (no wait required)
V	Play the first unplayed message (and update the mail box to count it as played)

Special Programming Notes

1. After the last character is outdialed, the system goes on-hook ("hangs up") automatically, except when message delivery is specified.
2. When a mailbox is programmed for message delivery, the system automatically waits for a greeting. (If a G is erroneously programmed at the end of the dial string, the system ignores it.)
3. A "V" anywhere in the dial string causes the system to play the first unplayed message only. If there is more than one message in the mailbox, the user will probably be paged again. The next unplayed message will play because each unplayed message generates its own paging request.
4. When the system is programmed to outdial a telephone number to the outside network, and the number is followed by a G (wait for person or pager to answer), the "clicks" and "pops" of particularly noisy switching equipment may be misinterpreted as a greeting. To avoid any misunderstanding, dial the telephone number, then count the number of seconds it takes for the receiving telephone to ring or the pager to answer.
5. If the call is made to a pager, insert the appropriate number of plus signs (+) between the number and the G. For example, if the dial string is "T95551212G," and it took five seconds to answer, change the string to "T95551212+++++G."
6. Since Message Delivery always assumes a G at the end of the dial string, insert the appropriate number of plus signs (+) at the end of the pager number.

Step 3: Choose Pager System Outdial Index and Pager Number

The coding string you must formulate is divided into two parts:

- Pager system access code, represented by the outdial index (access code index)
- Pager Number

The choice of outdial index and pager number is flexible. For example, if the coding string you formulate is T94085551212++G1234, you can choose:

- Outdial Index 0 and Pager Number 4085551212++G1234; OR
- Outdial Index 2 and Pager Number 5551212++G1234; OR

- Outdial Index 5 (without a dial string), and put the entire coding string into the Pager Number (where outdial indexes match those shown in the table below).

Limitations:

- Pager numbers are limited to 24 characters.
- Access codes are limited to 30 characters.

The outdial index serves two purposes.

- It tells the system what characters to outdial before dialing the Pager Number.
- It assigns a pager system to the mailbox.

If you want to enter the entire outdial string into the Pager Number field, you must choose an outdial index to assign a pager system. If you do not select an outdial index for a mailbox, the system cannot issue a page when a message is left in that mailbox.

You can obtain a report of pager systems, outdial indexes, and dial strings by running the Pager Access Codes Report (Text console only). The system displays the available indexes, access codes (dial strings), and pager system names.

Sample Report:

```
INDEX
 PAGER NAME
                      ACCESS
CODE
              HOLD
TIME
```

0 Internal 20

1 Long Distance T 20

2 Local T9 20

```
3
    415 Area Code
                 T9415
                     20
```

4 Pager 916-325 T991635 20

5 Empty

Up to 16 different page systems are allowed; only 4 were necessary for this installation. Pager System 5 (Empty) is set to use with Pagers that have entire dial strings in the Pager Number.

To add a pager that must outdial more than 24 characters (that is, when the coding string is too long to fit into the Pager Number field) when an appropriate outdial index does not exist, the system technician must configure a new pager system before the pager can be added.

Step 4: Choose the Pager Frequency

The pager frequency is the maximum number of times that the system attempts to notify the user of an unplayed message if each page is successful. The default pager frequency is three.

A page is considered successful if the system does not encounter a busy signal or a reorder tone after the pager/message delivery call is made. After a successful page, the system waits the number of minutes specified for the pager interval (see "Step 5: Choose the Pager Interval"); then (if the message in the mailbox remains unplayed), the system repeats the page. For a review see Successful versus Unsuccessful Pages.

If the page was unsuccessful, the system continuously retries the number until the party is successfully paged. For this reason, it is important that you make a test call to verify the pager programming (see "Step 7: Test the Pager").

Step 5: Choose the Pager Interval

The pager interval is the number of minutes that the system waits before re-paging when the previous page was successful. The default pager interval is 30 minutes.

Step 6: Message Delivery

When messages are left in a user's mailbox, message delivery calls the user at a specified telephone number, indicates the number of messages, and asks whether the user wants to check them.

Step 7: Test the Pager

It is important to test a pager immediately after it is added to a mailbox. An error in programming can cause every page to fail. To test a pager or message delivery, leave a message in the mailbox and contact the user to be sure the page was successful.

- Radio pager - ensure that the pager is activated
- Display pager - the user must check the display digits to ensure that they are accurate
- Voice pager - the user must ensure that the first (unplayed) message plays at the appropriate time
- Message delivery - the system must call the appropriate telephone number

    - When the call is answered, the system should prompt:
    - "Hello, <name>. You have <number> unplayed messages in your mailbox. Please enter your passcode."
    - If the first part of the greeting is cut off, add more plus signs (+) at the end of the pager number.
    - If the user answers, and there is a long silence before the system plays the greeting, decrease the number of plus signs (+) at the end of the pager number.

See Special Programming Note # 4 above.

26.45.9 Allow Mailbox Owners to Control Paging/Message Delivery

This procedure describes the feature bits required to allow mailbox owners to:

- Turn paging/message delivery on or off
- Change their paging or message delivery phone number
- Schedule paging/message delivery

To allow mailbox owners to control paging:

1. Customize an FCOS to include the following bits:
   - **070** (User Options Menu) (Mandatory)
   - **077** (change pager schedule) (Optional)
   - **094** (change message delivery options) (Optional)
   - **143** (change message delivery phone number) (Optional)
2. Assign the FCOS containing these bits to each mailbox that needs paging/message delivery control.

26.45.10 Allow Receipt of Urgent Messages Only

This procedure describes how to restrict paging or message delivery to urgent messages only. With this restriction, a page or message delivery call is activated only if the caller marks a message as "urgent".

1. Include the following feature bits in the FCOS for the mailbox that uses the pagers or message delivery:
   - **40** (receive messages from other users) AND/OR **41** (receive messages from outside callers)
2. - **79** (set msg wait #1 for urgent msgs only) OR **80** (set msg wait #2 for urgent msgs only)
   - **88** (receive urgent messages)
3. Assign the FCOS containing these bits to each mailbox you want for each of these features.

26.45.11 Configure a Tone or Voice Pager

This procedure summarizes the steps necessary to configure the server for tone or voice pagers.

Before You Begin

- Ensure that appropriate server hardware and software have been installed
- Ensure that you have completed the Outdial Line Group Worksheet
- Ensure that you have defined a line group for the Pager application

To configure a Tone Pager:

1. *Follow the instructions in Define a Pager System to set up the paging system.* A typical access code for tone paging is T9 where:

   - *T = Wait for dial tone*
   - *9 = Request an outside line*

2. *Customize an FCOS to include the following feature bits:*

Bit	Description
70	User Options Menu
77	Change pager schedule
79 (or 80)	Set Message waiting #1(or #2) for urgent messages only
124	Change paging phone number
168 (or 169)	Message waiting # 1 (or #2), pager requeue
181	Paging over msg del, mwi 1 over mwi 2
182 (or 183)	Use pri/alt as week/weekend for MWI #1 (or MWI #2)

3. If required, customize an LCOS using the information supplied in COS for Pager Mailboxes.
4. Configure a mailbox for paging to set up a pager mailbox. A typical pager number for tone paging is 9163259116+G where:

   - 9163259116 = Call the pager company's number
   - + = Pause one second
   - G = Wait for a computer tone or an answer (energy on the line)

   The post-pager number can be blank; however, if mailbox owners have the option to change their paging phone numbers, it is recommended to add any non-numeric digits (G, T, or +) to the post-pager number.
5. If required, set billing rates for paging. See Set Billing Rates for Pager Calls.
6. Test the configuration and pager operation using the procedures in the Testing the Pager Application section.

26.45.12 Configure a Display Pager

This procedure summarizes the steps necessary to configure the server for display pagers.

Before You Begin

- Ensure that appropriate server hardware and software have been installed
- Ensure that you have completed the Outdial Line Group Worksheet
- Ensure that you have defined a line group for the Pager application

Note:
Defining pager systems should be done on a duplicate of the active configuration.

To configure a Display Pager:

1. *Follow the instructions to define a pager system to set up the paging system.* A typical access code in a PBX environment for display paging is T9 where:
   - *T = Wait for dial tone*
   - *9 = Request an outside line*
2. *Customize an FCOS to include these feature bits:*

Bit	Description
40	receive messages from other users
41	receive messages from outside callers
70	User Options Menu
77	change pager schedule
79 (or 80)	set Message waiting #1(or #2) for urgent messages only
88	receive urgent messages
124	change paging phone number

Bit	Description
168 (or 169)	Message waiting # 1 (or #2), pager requeue
181	paging over msg del, mwi 1 over mwi 2
182 (or 183)	use pri/alt as week/weekend for MWI #1 (or MWI #2)

3. If required, customize an LCOS using the information supplied in COS for Pager Mailboxes.
4. Configure a mailbox for paging:

   - A typical pager number for display paging contains the account number or the DID number of the user's pager, followed by a one- or two-second pause (++).
   - A typical post-pager number for display paging contains only the display digits to be shown on the pager.
   - Choose no message delivery.
5. If required, set billing rates for paging using the instructions under Set Billing Rates for Pager Calls.
6. Test the configuration and pager operation using the procedures in the Testing the Pager Application section.

26.45.13 Paging Instructions for Users

This section discusses procedures that your users will need to interact with the paging or message delivery system. Give these instructions to users when you assign a paging mailbox.

The User Telephone Interface

Users control their schedules and phone numbers by beginning at the Call Schedule Options Menu, an option on the User Options Menu. From there, they go to the Paging/Message Delivery Schedule Menu, where they can alter the start and stop times and phone numbers.

Note:
When NP TDD is enabled, call scheduling is not available.

When users make a choice from the Paging/Message Delivery Schedule, the server gives them a series of prompts to guide them through each change they make. Whether users hear the prompts for paging or message delivery depends on the FCOS, and whether the Message Delivery parameter is enabled in the mailbox configuration.

Call Placement Telephone Interface

To use this feature, users begin with these steps:

1. Press **M** to start making a message.
2. Press the key that activates call placement (this key is set in the dialing plan).
3. Dial the destination phone number.

The server automatically prompts users to record the name of a recipient, and then to record a message. After recording, users can send their messages immediately (with “normal” delivery), or use message addressing options, including passcode protection (see below). When users send their messages, the system dials the specified phone number.

When someone answers the phone at the destination number, the system announces, ��This is a message for [recipient’s name] from [sender’s name].” Recipients then have the following options from their telephone keypad:

- Accept this message.
- Delay the message for 30 seconds.
- Reject this message.
- Tell the server to retry delivery in an hour.

If recipients accept the message, they can replay it and/or answer the sender. If recipients reject the message or the server cannot deliver it, the server notifies the sender with a non-delivery receipt—even if the sender did not request a receipt. Of course, users can still request the standard receipt.

Note: By default, the system delivers paging prompts in the language programmed for the LCOS assigned to the mailbox. Otherwise, it delivers prompts in the language programmed for the pager line group. For example, if the mailbox has an LCOS with French specified as the alternate language, the user will receive paging prompts in French. However, if the mailbox has an LCOS with the default language (English), and is employing a line group programmed to use German and a pager line group programmed to use Swedish, the user will receive paging prompts in Swedish (and login prompts in German).

Passcode Protection

As a message addressing option, users can attach a 4 to 10-digit passcode to their messages, which recipients must enter before they can play the messages. Of course, a sender and recipient must agree on this passcode beforehand.

To use this feature, a user presses M for message addressing options when making the message for a call placement number. The user then presses O for off-site passcode, and is prompted for a 4- to 10-digit passcode. The user then exits message addressing options and sends the message.

The called person is prompted for the passcode before the message can be played.

To Disable and Enable Paging

Users can turn off paging or message delivery when they do not want to be "on call" so that the pager port is not tied up by issuing unwanted pages. For any mailbox with Pager/Message Delivery as a message waiting indicator, assign an FCOS that includes the feature bits:

- 070 User Options Menu
- 077 Enable/Disable Pager

(Unlimited, Full Guest and VIP default FCOS have these two feature bits).

To disable paging:

1. Log in to the mailbox, press **U** (the **8** key) for User Options. The system prompts, "Press C to change call schedule options, P to schedule paging, E or D to enable or disable paging."
2. Press **D** (the **3** key) to disable paging. The system confirms the choice: "Paging disabled."

When paging is disabled, and the user accesses the User Options menu, the system prompts: "Press E to enable paging."

1. Press **E** (the **3** key) to enable paging. The system confirms the choice: "Paging enabled."

26.45.14 Billing Considerations for Paging

The billing function is capable of billing both paging and message delivery on a per-call basis. Remember, however, that the server site is the calling party and thereby responsible for any charges that accrue when paging or message delivery calls are made to the outside telephone network. As stated earlier, pager calls are usually of very short duration, but message delivery calls can be quite long. Since the cost of each call depends on the time of day that it is made, the duration of the call, the distance between the server and the user, and the rates of the local telephone company, the server makes no provisions for this aspect of the billing.

Outdial Billing

Outdials such as paging calls can, however, be billed back to a mailbox owner's account. This form of outdial billing can be implemented through individual mailboxes' configuration and is explained more fully in the Mailboxes section.

Example:

Henry Huggins has a pager and has his pager calls billed to his calling card number. To perform this manually, you lift the telephone receiver; wait for a dial tone; dial 9 to get an outside line; dial 0-612-555-4534 (0 indicates you will charge the call); wait for a computer tone; dial the calling card number; wait for another tone; dial his mailbox number, 6446; then dial # to tell the pager that all the display data has been entered. (This activates the pager). The dial string for these actions is:

Caller Action	Dial String
Wait for dial tone.	T
Dial 9 to get outside access.	9

Caller Action	Dial String
Dial individual pager number is.	06125554534
Wait four seconds for line to settle.	++++
Wait for computer tone.	G
Dial calling card number	503102533346666
Wait four seconds for line to settle.	++++
Wait for computer (dial) tone.	G
Dial display data (mailbox).	6446
Enter # to indicate that all the data has been entered and make paging terminal hang up.	#

In this case, such as in Example 2 (DID Display pager), configuration is complex, since there is not enough room in the mailbox parameter (Pager Number) to specify the individual pager number, the calling card number, *and* the display data, all of which are unique to this pager. In most installations, however, DID display pagers share a common area code and prefix (0-612-555, in this case), and configuring the area code and prefix into the outdial index allows more than one pager to use that pager system.

The organization of the dial string is as follows:

Pager system dial string	T90612555
Pager Number	4534++++G503102533346666
Post-Pager Number	++++G6446#

The paging Mailbox Worksheet entries are:

Pager access type	B (billed outdial index)

Billing order	nb
Message delivery	No

Individual Rates

The server's billing rates structure does allow you to specify an individual rate for each pager system. This rate is multiplied by the number of pages that are issued for the mailbox. If you put message delivery accounts and radio pager accounts on separate pager systems, you can increase the charges on the pager systems that serve message delivery subscribers to compensate for any toll charges that the telephone company levies.

26.45.15 Add, Edit or Delete a Pager System

Add a New Dialer (Pager)

To add a new dialer (pager):

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. From the navigation tree, click **Dialers (Pagers)** and then click **Add.**
4. In the **Number** field, enter the index number (0-15) of the dialer (pager) system or click **Next Available** to use the next unused number.
5. In the **Name** field, enter a descriptive name that identifies this pager system. (For example, "553 exchange".)
6. In the **Access Code** field, enter the code (1-24 characters) that is common to mailbox owners using this pager system.
7. In the **Hold Time** field, Enter the number of seconds (0-90) the server holds a call before hanging up after a successful send attempt. (2 to 5 seconds is recommended.)
8. Click **Add**.
9. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.
10. **Note**: If, after the setup is complete, the pager fails to outdial, a system reboot may be required to enable the pager systems.

Edit a Dialer (Pager)

To edit an existing dialer (pager):

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click **Dialers (Pagers)** and then select the pager you want to edit by selecting its check box and then clicking **Edit**.

4. Edit the Name, Access Code, and Hold Time fields as required and then click **Save**.
5. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

Delete a Dialer (Pager)

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click **Dialers (Pagers)** and then select the pager you want to delete by selecting its check box and then clicking **Delete**. A confirmation message is displayed.
4. Click **Yes** to delete the selected pager.
5. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.45.16 Configure a Mailbox for Paging

To configure a mailbox for paging:

1. Follow the instructions to add a mailbox or edit a mailbox
2. Enter the required parameters on the **Message Waiting** tab and the **Outdial Parameters** tab.

These two tabs provide configuration for the following parameters:

- Mailbox configuration for paging
- Access type
- Frequency
- Interval
- Paging Start/Stop Times
- Alternate Pager
- Call placement

26.45.17 Add an Alternate Pager to an Existing Mailbox

You can add an alternate pager to an existing pager mailbox. If your pager mailbox is unsuccessful at contacting your primary pager after the frequency or "busy attempts" parameters have expired, the server attempts to contact any programmed alternate pager.

To add an alternate pager to an existing mailbox:

1. From the navigation tree, click **Mailbox Maintenance > Mailboxes**.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select a mailbox in the list, and then click Edit > Selected. The mailbox data is displayed.

4. On the **Message Waiting** tab, under the Pager message waiting Type, click the Details link.
5. Select **Enable Alternate Pager/Telephone Number** and configure as required using Message Waiting Tab parameters for reference.
6. Click **Save**.

26.45.18 Set Pager Start and Stop Times

To set pager start/stop times:

1. In the navigation tree, click **Mailboxes > Mailbox Maintenance**.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select a mailbox in the list, and then click Edit > Selected. The Mailbox data view is displayed.
4. On the **Message Waiting** tab, click the Details link associated with the Pager MWI type.
5. Select a **Start Time** and **Stop Time** for the primary and/or alternate pager.
6. Click **Save**.

26.45.19 Turn Pagers/Message Delivery Off for a Mailbox

You can suppress message delivery or paging for a mailbox temporarily without removing pager programming.

To suppress pager/message delivery for a mailbox:

1. From the navigation tree, click **Mailbox Maintenance > Mailboxes**.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select the mailbox to modify, and then click Edit > Selected. The mailbox data is displayed.
4. On the **Message Waiting** tab, under the Pager message waiting Type, click the Details link.
5. Scroll to the Primary or Alternate pager, as required, and select **Suppress pages/Message Delivery**.

To turn pagers and message delivery back on, repeat the steps 1 to 4, and then clear the **Suppress pages/ Message Delivery** check box.

26.45.20 Enable Call Placement

To allow mailbox owners to send messages to any telephone:

1. From the navigation tree, click **Mailbox Maintenance > Mailboxes**.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select a mailbox in the list, and then click Edit > Selected. The mailbox data is displayed.
4. Click Advanced.
5. On the **Outdial Apps** tab, scroll down to the **Call Placement** section.

6. In the **Call Placement Access Type** list, select one of the following:

   - **Use Internal Access type** if call placement outdials from this mailbox are to use the internal outdial index (specified earlier in the mailbox configuration) for internal calls.

     OR
   - **Use Billed Access Type** if call placement outdials from this mailbox are to be charged to a billing account. Outcalls will use the billed outdial index specified earlier in the mailbox configuration.

     OR
   - **Use Internal Access type** if call placement outdials from this mailbox are to use the internal outdial index (specified earlier in the mailbox configuration) for internal calls.

     OR
   - **Use Non-billed Access Type** if call placement outdials from this mailbox are not to be charged to a billing account. Outcalls will use the Unbilled Outdial Index specified earlier in the mailbox configuration.

     OR
   - **0-15** to select the index **number** of the pager system (0-15) this mailbox uses. This is the same as the pager system number specified in the Define Pagers Menu.

26.45.21 Define a Pager System

This procedure describes how to assign an identification (index) number to each supported pager system, how to name each supported pager system, and how to specify an access code and hold time for each supported pager system.

Before You Begin

Ensure that you are familiar with access code (dial string) configuration and that you have completed the Outdial Line Group Worksheet.

To define a pager system:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it

   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and then enter the **number** of the line group (1-24) to which the Pager application is assigned, or press **Enter** if the current number is the Pager application line group.
4. Select **(M) Modify Application**, and then **(P) Pager System Support**.
5. Using your Outdial Line Group Worksheet as reference, enter the information requested as shown in the following steps.

6. Select **(P) Pager Systems Supported** and then enter the pager system index **numbers** (0-15), separated by commas, of the pager systems that will be supported by this pager. (For example, to add two pager systems (one for internal and one for external), enter **0,1**.)
7. In the Pagers menu, select **(D) Define Pagers**.
8. Select **(P) Current Pager System** and then enter the index **number** of the first supported pager system. (For example, **0**.)
9. Select **(N) Pager Name** and then enter a name for this pager system. (For example, "Internal". Up to 30 characters are allowed.)
10. Select **(D) Access Code** and enter the **code** (1-24 characters) that is common to mailbox owners using this pager system. This code indicates what the server should dial before the unique number. It comprises the first part of the dial string.

    OR

    Press **Enter** if the current access code is correct.

    OR

    Enter a **period** (.) to delete an existing access code.
11. Select **(H) Hold Time** and enter the number of **s econds** (0-90) the server holds a call before hanging up after a successful send attempt. We recommend 2-5 seconds.
12. Save the parameter settings by exiting to the NuPoint Voice Configuration Main Menu.

If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.45.22 Configure a Mailbox for Paging/Message Delivery

Whether you are modifying existing mailboxes or creating new ones for paging, the following procedure outlines the required parameters. For detailed information about any parameter listed here, see the overview topic Mailboxes for Paging.

Before you begin, ensure that you have completed the Mailbox Worksheet.

To configure a mailbox for paging:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** and enter the **n umber** of the new mailbox you want to configure for paging

   OR

   Select **(M) Modify Mailboxes** and enter the n**umber** of the existing mailbox you want to re-configure for paging,

   Note: The prompts are almost the same for creating a new mailbox and modifying an existing one, except that "New" precedes each prompt when you select Modify Mailboxes.

3. Press **Enter** until the **Features Class of Service** prompt appears. Enter the **number** of the FCOS (1-640) that includes the appropriate feature bits. See Configure COS for Pager Mailboxes for more information.
4. At the **Limits class of service:** prompt, enter the **number** of the LCOS (1-640) that includes the applicable limits. See Configure COS for Pager Mailboxes for more information.
5. Press Enter until the **Message waiting type #1:** prompt appears and then enter **5** for paging.
6. At the **Pager Access Type** prompt, enter the index **number** of the pager system (0-15) this mailbox uses. This is the same as the pager system number specified in the Define Pagers Menu,
7. **OR** enter one of the following parameters:

   - **I** if pages from this mailbox are to use the internal outdial index (specified earlier in the mailbox configuration) for internal calls.
   - **B** if pages from this mailbox are to be charged to a billing account. Pages will use the billed outdial index specified earlier in the mailbox configuration.
   - **U** if pages from this mailbox are not to be charged to a billing account. Pages will use the Unbilled Outdial Index specified earlier in the mailbox configuration.
8. At the **Pager number** prompt, enter the unique **number** (1-16 characters) of the pager. The pager number must contain at least one character. (This number is dialed immediately following the access code specified in the Define Pagers Menu and can contain any additional characters from the Dial String Characters table.)
9. At the **Post-pager number** prompt, enter one of the following:

   - For display pagers, the display **digits** (0-24) to be shown on the pager.
   - For tone or voice pagers, leave blank; however, if mailbox owners have the option to change their paging phone numbers, coding a greet-and-wait (G) character in the post-pager number is recommended. Also enter any overflow from the tone or voice pager number (up to 24 characters) that did not fit in the pager number field. Table 1 at the end of this procedure shows valid post-pager number characters. **Note**: If a post-pager number is entered, it comprises the last part of a paging dial string.
10. At the **Pager frequency** prompt, enter *t*he number of **times** (0-255) this mailbox will be notified with a page every time there is an unplayed message in the mailbox. Either 0 or 1 indicates one notification only.
11. At the **Pager interval** prompt, enter the number of **minutes** (0-255) between pages for this mailbox. Either **0** or **1** indicates a one-minute interval.
12. At the **Message delivery** prompt, enter **Y** to enable Message Delivery or **N** to disable.
13. At the **Suppress pages** prompt, enter **N** to leave paging enabled OR enter **Y** to turn off the paging feature.
14. At the **Busy pager attempts** prompt, enter the number of **times** (0-255) this mailbox will retry a page when a busy condition is encountered. Either 0 or 1 indicates one retry. Setting both the busy pager attempts and busy pager interval to 0 specifies unlimited retries upon reaching a busy signal.
15. At the **Busy pager interval** prompt enter the number of **minutes** (0-255) between pager attempts. Either 0 or 1 indicates a one-minute interval. Setting both the busy pager attempts and busy pager interval to 0 specifies unlimited retries upon reaching a busy signal.
16. At the **Pager start time** prompt, enter the **time** at which paging is to start. Enter the time in hours and minutes followed by "am" or "pm"; for example: 6:00pm. If 12:00am is entered for start time and stop time, paging is enabled at all times.
17. At the **Pager stop time** prompt, enter *t*he **time** at which paging is to stop. Enter the time in hours and minutes followed by "am" or "pm"; for example: 8:30am If 12:00am is entered for stop time and start time, paging is enabled at all times.

18. At the **Define an additional pager number?** prompt, you can add an alternate pager to be used when the primary pager does not respond. Set the applicable parameters (step 7-17) for the additional pager as described for the primary.

> **Note**:
> If you use one of the billing outdial indexes, you cannot use Pager 4 (Message Waiting 2 alternate pager) because they use the same post-pager field.

19. Press **Enter** until the **Turn Off Pager/Outcall Notification** prompt appears. Enter **Y** to suppress all notifications (pages or message delivery) or **N** to leave pages and message delivery notification on.
20. If you require the Call Placement option, press **Enter** until the ***C* all placement pager access type** prompt appears and then enter one of the following:

    - **I** if call placement outdials from this mailbox are to use the internal outdial index (specified earlier in the mailbox configuration) for internal calls.
    - **B** if call placement outdials from this mailbox are to be charged to a billing account. Outcalls will use the billed outdial index specified earlier in the mailbox configuration.
    - **U** if call placement outdials from this mailbox are not to be charged to a billing account. Outcalls will use the Unbilled Outdial Index specified earlier in the mailbox configuration.
21. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.45.23 Setting Start and Stop Times

To set pager start/stop times:

1. From the Mailbox Maintenance Menu, select **(M) Modify Mailboxes**.
2. Enter the number of the mailbox to modify.
3. Press **Enter** until the **Pager Start Time** parameter appears.

> **Note**:
> If both the start time and the stop time remain unspecified, paging or message delivery is enabled at all times.

4. Enter the **Pager Start Time**: The time at which paging or message delivery is to start. Enter the time in hours and minutes followed by "am" or "pm"; for example: 6:00pm.
5. Enter the **Pager Stop Time**: The time at which paging or message delivery is to stop. Enter the time in hours and minutes followed by "am" or "pm"; for example: 8:30am.
6. Press **Enter** until the prompts stop. After the last prompt, the server displays the new mailbox configuration.

26.45.24 Change Paging Schedules or Intervals

This procedure describes how to:

- Schedule weekday and weekend paging or message delivery
- Receive queued pages or message delivery calls at the pager start time
- Change selection of pagers or message delivery when schedules overlap.

Setting a Weekday-Weekend Schedule

1. Customize an FCOS to include one of these feature bits in the FCOS for the mailbox that uses the pagers or message delivery:
    - **182** Use Pri/Alt as Week/Weekend for MWI 1: if the pagers or message delivery were configured as the first message waiting type.
    - **183** Use Pri/Alt as Week/Weekend for MWI 2: if the pagers or message delivery were configured as the second message waiting type.
2. Configure an alternate pager. This will be the weekend pager.
3. Make sure the weekday pager number or message delivery number is specified for the primary and the weekend pager number or message delivery number is specified for the alternate.

Receiving Queued Pages or Message Delivery Calls at the Start Time

Customize an FCOS to include one of these feature bits in the FCOS for the mailbox that uses the pager or message delivery:

- **168** Message Wait 1, Pager Requeue: if the pager was configured through the first message waiting type prompt.
- **169** Message Wait 2, Pager Requeue: if the pager was configured through the second message waiting type prompt.

Prioritizing Paging When Schedules Overlap

Customize an FCOS to include these feature bits in the FCOS for the mailbox that uses the pager or message delivery:

- **70** User Options Menu
- **77** Change Pager Schedule
- **181** Paging over msg del, Message waiting #1 over Message waiting #2: if the schedules for pagers in both message waiting types overlap, the server selects the pager in the first message waiting type. If message delivery is in the first message waiting type and paging only is in the second message waiting type and their schedules overlap, the server selects paging only.

26.45.25 Enable Cascade Paging

The Cascade Paging feature is disabled by default and can only be enabled using the Text Console.

To enable Cascade Paging:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System, (G) Offline Menu, and (S) Auto Task Menu**.
2. Select **(P) Cascade Paging Feature** .
3. Select **(E) Cascade Paging Enable (Y/N)**.
4. Enter **Y** to enable Cascade Paging.
5. Enter **X** to exit the menu and save changes.

26.45.26 Turn Pagers/Message Delivery Off for a Mailbox

You can suppress message delivery or paging for a mailbox temporarily without removing pager programming.

To suppress pager/message delivery for a mailbox:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(M) Modify Mailboxes** and enter the mailbox number to modify.
3. Press **Enter** until the **Turn off pager/outcall notification** prompt appears and enter **Y** to turn off.
4. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

To turn paging/message delivery back on, follow the above procedure and select **N** at the **Turn off pager/outcall notification** prompt.

26.45.27 View Pager Configuration

You can view pager configuration from two different sources: the Reports menu or the Pagers menu.

To view pager information through the Reports menu:

1. From the Main Menu, select **(R) Reports Menu**.
2. Select **(R) Pager Access Codes**.
3. When prompted for output routing, select (C) Console screen or (P) Console with Pause. The server displays information about each supported pager:

PAGER SYSTEMS ACCESS CODES			
Wed Aug 12 14:36:11 2009			
INDEX	**PAGER NAME**	**ACCESS CODE**	**HOLD TIME**
0	Internal		20
1	Long Distance	T	20
2	Local	T9	20
Press any key to continue....			

To view pager information through the Pagers menu:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(R) Reconfigure System**.
2. Select **(E) Modify Active Configuration**.
3. From the Voice Configuration Online Menu, select **(G)Group Selected** and enter the Pager Line Group number.
4. Select **(M) Modify Application**.
5. Select **(S) Show Pagers**. The server displays information about each supported server:

```
Pager Systems:

Pager System [0], Pager Name = "Internal"

Access code = [], Hold time = [20]

Pager System [1], Pager Name = "Long Distance"

Access code = [T], Hold time = [20]

Pager System [2], Pager Name = "Local"

Access code = [T9], Hold time = [20]
```

You can also see Pager application parameters in the System Configuration report.

26.45.28 Enable Call Placement

To allow mailbox owners to send messages to any telephone:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:
   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and then enter *the* **number** of the line group (1-24) to which the Pager application is assigned, or press **Enter** if the current number is the Pager application line group.
4. Select **(M) Modify Application**, **(F) Other Features**, **(D) Dialing Plan Menu.**
5. Select **(D) Dialing Plan**.

6. At the **NuPoint Voice dialing plan=** prompt, enter **T** in the digit position that activates call placement, then the desired **code** in each of the other digit positions. Valid codes are:

0	No mailbox numbers start with the digit marked by 0
1-11	Number of digits allowed in a valid mailbox number
A	The digit marked by A enables Dial-by-Name. When this digit is pressed, it triggers a prompt that instructs the caller to begin spelling the name. You may use this element in any position of the dial plan.
V	Mailbox numbers starting with the digit marked by V are variable length, up to 11 digits.

7. Save the dialing plan by exiting to the Main Menu.
8. Customize an FCOS to include feature bit 110 (make/give to telephone number) and assign to the mailboxes.
9. If required, modify the LCOS limits that control call placement. You can modify any of the following limits:

    a. RNA retry limit
    b. RNA retry interval
    c. Busy retry limit
    d. Busy retry interval
    e. Message phone length
    f. Message count
    g. Maximum message length
10. Define a pager system with message delivery to provide an outdialing port.
11. For each mailbox that uses the call placement function, modify the mailbox to:

    a. Assign the FCOS containing feature bit 110.
    b. Assign the LCOS modified to support call placement.
12. Specify the pager system, defined in step 10, as the Call Placement index number. This is also set in the mailbox configuration. After setting FCOS and LCOS, press **Enter** until the Call Placement Pager Access Type prompt appears.

13. At the **Call placement pager access type:** prompt, enter one of the following:

    a. index **number** of the pager system (0-15) this mailbox uses. This is the same as the pager system number specified in the Define Pagers Menu.

    OR

    b. **I** if call placement outdials from this mailbox are to use the internal outdial index (specified earlier in the mailbox configuration) for internal calls.

    OR

    c. **B** if call placement outdials from this mailbox are to be charged to a billing account. Outcalls will use the billed outdial index specified earlier in the mailbox configuration.

    OR

    d. **U** if call placement outdials from this mailbox are not to be charged to a billing account. Outcalls will use the Unbilled Outdial Index specified earlier in the mailbox configuration.

14. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the system displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.46 Testing Overview

After telephone lines have been installed, and after you create and configure mailboxes for a Pager application, test pager operation using the procedures in this section.

Note:
It is very important to test a pager immediately after it is added to a mailbox, since a seemingly minor error in configuration can cause every page to fail. Furthermore, the server can tie up pager ports for a long time dialing invalid paging codes.

Successful vs Unsuccessful Outdialing

The server applies specific criteria to call processing and treats an outdial as successful or unsuccessful accordingly.

Successful Outdialing

If the server encounters speech, other than a lengthy greeting, after outdialing, it considers the call successful.

Successful pages are retried a specified number of minutes apart (the pager interval), for a maximum number of times (the pager frequency). Paging is discontinued when any of the following occurs:

- The frequency number is reached

- The user listens to all unplayed messages in the mailbox and logs out
- The user disables paging

Unsuccessful Outdialing

If the server encounters a Busy or Reorder tone, or a Ring No Answer condition after outdialing, the call is considered unsuccessful. Other examples of unsuccessful calls are if no dial tone is detected, or no tone or voice “greets” the server after the page is made. The server retries the page according to the busy frequency and busy interval.

When the server detects that an “illegal” dial string (that is, a string that does not conform to configuration rules) has been outdialed, it considers the page successful. This prevents the server from continually retrying the page. However, if a dial string is configured incorrectly (that is, it cannot activate the pager), but conforms to pager configuration rules, the server continually retries the page. This is why it is critical to test every pager immediately after configuring is completed.

Note:
If you are using answer supervision (the L code) in any of your outdial strings, your outdial is considered a failure unless the server detects a ringing on the line.

26.46.1 Test Pager Configuration

This procedure describes how to test a tone pager, display pager, or voice pager after it has been configured. Prerequisites for this procedure are:

- All appropriate hardware has been installed.
- Telephone lines have been installed and tested for dial tone.
- Test mailboxes have been configured for pagers.
- Pager systems have been configured.

Testing a Pager

1. If you have not already done so, obtain a System Configuration Report. Refer to the report as needed for such information as the access code.
2. When the user has a radio pager, check to see if the pager is activated.
3. When the user has display pager, ask the user to check the display digits to be certain that they are accurate.
4. When the user has a voice pager, be sure that the first unplayed message is played at the appropriate time.

Testing Primary Pager Configuration (Text Console only)

You can use the *Testing Primary Pager* instructions in the Text Console .

Testing Alternate Pager Configuration

1. Set a very short frequency and interval in the test mailbox.
2. Test the primary pager as described above, but allow the frequency and interval of the primary pager to expire without responding to the test page.
3. Verify that the page is then received by the alternate pager.
4. If not successful, check the Event Log file to determine if the correct digits are being dialed. Review Event Recorder data reported at the server maintenance console to determine if any errors were encountered during the page.

Note: If you use one of the billing outdial indexes, you cannot use Pager 4 (Message Waiting #2 alternate pager) because they use the same post-pager field.

Message Waiting Types	
Number	Message Waiting Type
0	None
1	Not available
2	Not available
3	DTMF to PBX
4	Not available
5	Pager
6	Not available
7	Not available
8	Not available
9	Not available
10	Not available
11	Centrex
12	Not available
13	Not available
14	Not available
15	Not available
16	HIS PMS
17	Unified Integration (for 9.0)
18	Not available
19	Not available
20	Not available
21	Hitachi PMS
22	Not available
23	Not available
24	Not available

26.46.2 Test Call Placement

This procedure describes how to test the call placement function after it has been configured. Prerequisites for this procedure are:

- All appropriate hardware has been installed.
- Telephone lines have been installed.

To test call placement:

1. If you have not already done so, obtain a System Configuration Report. Refer to the report as needed for configuration parameter settings.
2. *Create a test mailbox for originating Call Placement messages. You will need another telephone (not the one associated with the originating mailbox) to simulate an off-server telephone number. The originating mailbox should include feature bit 110 in its FCOS so it can make messages to a telephone number, as well as the standard feature bits in, for example, FCOS 1.*
3. *L*og into the sending mailbox and place a call to the simulated off-server telephone number (the receiving telephone), then hang up.
4. Verify that the call was placed. Check the Event Log file to determine if the correct digits are being dialed. (For more information about Event Recorder, see the Troubleshooting section of the *NuPoint UM Technician's Handbook*.)
5. Accept and answer the call placement message from the simulated off-server telephone.
6. Log into the sending mailbox and verify that there is one unplayed message. This unplayed message should be the answer you made in the preceding step to the call placement message.
7. Play the message, then delete it.

26.46.3 Test Message Delivery

This procedure describes how to test the message delivery function after it has been configured.

Prerequisites for this procedure are:

- All appropriate hardware has been installed.
- Telephone lines have been installed.
- Test mailboxes have been configured for message delivery.
- Associated pager systems have been configured.

If you have not already done so, obtain a System Configuration Report. Refer to the report as needed for such information as message delivery parameter settings.

Using the Lights Test

You can test message delivery calls using the Lights Test as described for pager message waiting lights; however, if you make an actual message delivery test call, you can check server prompts and the mailbox user interface at the same time.

Using a Test Call

1. Log into the test mailbox, ensure that there are no unplayed messages, then log out of the test mailbox.

> **Note**:
> To streamline the test, you should set the number of retries to 0; otherwise, the server keeps trying to complete the call until the maximum number of retries has been reached.

2. Set event Recorder (CDR) for "3: Pager/Prog.RS232" and run event recorder.
3. Call the test mailbox and leave a message.
4. You can check the Event Log file to determine if the correct digits are being dialed. You want to see a result code of "0" in the log file, which indicates that it was dialed as programmed and completed the action.
5. When the telephone that you have called rings, answer it at the first ring (or have an assistant do so if necessary). The server should say, "Hello [mailbox name]. You have one unplayed message in your mailbox. One message total. Please enter your passcode."
6. Enter the passcode and play the message. If problems occur while attempting to play the message:

   - Check the dialing plan in the active configuration.
   - Check the mailbox FCOS.
   - Check the mailbox Pager Index number, Pager number, and Post pager number data.
   - Check the "Other Features" parameter settings for the pager line group, to ensure that they match the corresponding parameter settings for the NuPoint Voice application.
7. Verify that there is no further paging.

Troubleshooting

For message delivery, the server should call the appropriate telephone number and, when the call is answered, should prompt,

“Hello, [user’s name]. You have unplayed message(s) in your mailbox. Please enter your passcode.”

If the first part of the greeting has been cut off, add more plus signs to the end of the pager number or post-pager number. Conversely, if the user answers and there is a long silence before the server plays the greeting, decrease the number of plus signs at the end of the pager number or post-pager number.

Message delivery calls can be tested using the Lights Test option mentioned earlier; however, if an actual test call is made, you can check server prompts and the mailbox user interface at the same time.

The server can outdial very quickly—too quickly for some PBXs. One result can be that the server fails to get an outside line. To prevent this situation, try slowing down the server’s outdialing speed. You do this by inserting pluses (++) in dial strings. Each plus tells the server to pause for one second.

For example, suppose you have the following outdial string:

T94155551212++

You can slow the pacing of the sequence by inserting two pluses after each major step in the string. The result would be then be:

T9++4155551212++++

If this result works, you can experiment by removing one pause at a time to achieve the fastest speed that your PBX can handle.

26.46.4 Testing Primary Pager Configuration

Use this procedure and an extension that is part of the Pager line group and that has a mailbox configured for paging to test pager operation.

1. From the Main Menu, select **(S) System Maintenance**, and then **(O) Additional Options**.
2. Select **(L) Lights Test** to start the Lights Test and then enter the number of the test extension that has a mailbox configured for a pager. **Note**: You can also select a range of mailbox numbers separated by a hyphen, but be aware that the Lights Test may queue up a long list of message waiting requests and could take a long time to process.
3. At the **Light off/on/existing value (0/1/2):** prompt, enter **0** to turn the light off (to clear any existing indicator on the test extension).
4. At the **Message waiting type** prompt, enter **5** for paging. When prompted for mailbox number, enter the number of the test mailbox you used in step 3.
5. At the **Light off/on/existing value (0/1/2):** prompt, enter **1** to turn the light on. Check the indicator on the test extension.
6. Do one of the following:

   - If the light test is successful, you can either press Enter to stop the Lights Test menu, or you can test another extension.

   - If the light is not successful, check the Event Log file to determine if the correct digits are being dialed. Review Event Recorder data reported at the server maintenance console to determine if any errors were encountered during the page. (For more information about Event Recorder, see the Troubleshooting section of the *NuPoint UM Technician's Handbook*.)

26.47 Configure External Applications

External applications allow servers to use serial or IP ports to control an external device by sending signals over data links. The data links can be direct serial connections to the PBX, they can connect to modems that are connected to analog ports on the PBX (the modem is used to "forward" DTMF signals to the PBX), or they can be direct IP connections.

External applications are programmed using the External Applications menu of the **Web Console**. Click the following links for application-specific instructions:

- Message Waiting Indicator Applications (including RS-232 MWI)
- Property Management Services (PMS)

- SMS Notification (UK Only)
- Other External Applications (parameters reference)

26.47.1 External Application (RS232) Programmable Application Parameters

Parameter	Description	Value
Programmable Parameters		
Initialization String	Enter the ASCII string required by the PBX. To create the string, consult the PBX operating manual or the PBX vendor for the correct code.	0-30 characters
Reply String	Enter the ASCII string sent by the PBX.	0-30 characters
Delay between requests	Enter the time to wait between requests.	0 - 255 seconds
Pre-DN ON string	If the PBX requires the string **before** the directory number (sometimes called extension number), create an ASCII string . If the PBX sends the string **after** the directory number: - enter a period (.) to delete an existing string, if necessary. - enter values for the Post-DN ON String and Post-DN OFF String parameters.	0-30 characters
Pre-DN OFF string		

Parameter	Description	Value
Post-DN ON string	If the PBX requires the string **before** the directory number (sometimes called extension number), create an ASCII string . If the PBX sends the string **after** the directory number: - enter a period (.) to delete an existing string, if necessary. - enter values for the Post-DN ON String and Post-DN OFF String parameters.	0-30 characters
Post-DN OFF string		
Department Code as DN	Select this check box to use the department code instead of the mailbox extension as the DN to turn lights on/off.	
Unplayed Number Sent	Select this check box to send the number of unplayed messages currently in a mailbox to be included after the mail-box number.	
Delay after Post-DN String	Enter the time to wait between Post-DN and Trailing String.	0 - 255 seconds
Ending Trailing String	If the PBX requires this string, create an ASCII string If the PBX does not require this string, enter a period (.) to delete an existing string.	0-30 characters
Suppress Updates to MWL	Select this check box to suppress updates of MWL after a user accesses the mailbox without changing status.	

Parameter	Description	Value
Modem Result Code	This modem result code will be used to compare against the actual result code returned from the modem after it has finished outdialing the MWI string. If they are not matched, NuPoint Voice will retry the MWI request again later on. **Recommendation**: For *better display* of CDR events, please turn OFF the Local Echo mode of the modem, ie. if the modem has dialed a MWI string like "ATDT*13658", it should not echo back this same string prior to returning the result code. If event messages for modem dial result are desired, enable "Pager" CDR in the Event Recorder menu.	See Valid String Characters table below.
Connection Settings		
IP Address	Enter the IP address of the remote system.	(Used for PMS configuration)
Server Port Number	Enter the port that the remote device/system is listening on.	

Valid String Characters

Character	Explanation
\b	Backspace
\f	Form Feed
\n	New Line

\r	Carriage Return
\t	Tab
\\	Backslash
\"	Double Quotes
\?	Question Mark

26.48 Descriptions

Some integrations do not handle message waiting indicators (MWI) so NuPoint Unified Messaging provides MWI applications that allow the server to activate message waiting indicators on the PBX. These applications are:

- DTMF-to-PBX
- MiTAI
- RS-232 (modem-based, legacy application)

DTMF to PBX Message Waiting Application

The DTMF-to-PBX MWI application allows the server to turn PBX message waiting indicators on and off by sending DTMF signals over the telephone lines. Some PBXs allow telephone users to turn message waiting indicators on and off by dialing in a code. If your PBX has this capability, and if the code is not sent using proprietary signaling, you may be able to configure the server to behave as if it were a station user.

When a message is left in a mailbox that uses this type of message waiting, the server takes a line-card port off-hook, dials a string of DTMF digits, then goes on-hook. The PBX translates these digits and turns the appropriate indicator on. When all unplayed messages have been played, the server follows the same procedure (dialing a different string of digits) to turn the indicator off.

MiTAI Message Waiting

MiTAI MWI has similar behavior to the DTMF dialer but does not generate a dialing sequence and does not require a port. MiTAI MWI uses the proprietary MiTAI Messaging API to communicate directly with the MiVoice Business ICP to activate message waiting indicators on designated phones. Because the MWI does not actually dial out, outbound calls with the MiVoice Business ICP are reduced.

RS-232 MWI (Legacy)

The RS-232 MWI application allows servers to turn PBX message waiting indicators on and off by sending signals to the PBX over RS-232 data links. The data links can be either direct serial connections to the PBX, or they can connect to modems that are connected to analog ports on the PBX.

When a message is left in a mailbox, the server sends an ASCII message that tells the PBX to turn on the message waiting indicator at the appropriate station. Conversely, when all unplayed messages are played, the server sends an ASCII string that directs the PBX to turn off the message waiting indicator.

26.48.1 Assign Message Waiting Type to a Mailbox

Web Console:

To assign message waiting indicators to a mailbox:

1. Edit the selected mailbox using the instructions under Edit Mailboxes.
2. On the **Message Waiting** tab, in the **Message Waiting #1** field (or Message Waiting # 2 if #1 is used for another MWI application), assign the applicable Message waiting type from the table below:

Number	Message Waiting Type
0	None
3	DTMF to PBX
5	Pager (See Pager Application)
7	Program RS232
9	Centrex RS232
11	Centrex
16	HIS PMS
17	Unified Integration
21	Hitachi PMS
28	MiTAI Messaging

1. Click **Save**.

Text Console

To assign message waiting indicators to a mailbox:

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** or **(M) Modify Mailboxes** and enter the number of the mailbox to which you want to assign a message waiting indicator.
3. Press **Enter** until **Message waiting type #1:** or, if #1 is used for another MW application, until **Message Waiting Type #2:** appears and then assign the applicable Message waiting type from the table above.
4. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.48.2 DTMF-to-PBX Configuration Requirements

The DTMF-to-PBX application allows the server to turn PBX message waiting indicators on and off by sending DTMF signals over the telephone lines. Some PBXs allow telephone users to turn message waiting indicators on and off by dialing in a code. If your PBX has this capability, and if the code is not sent using proprietary signaling, you may be able to configure the server to behave as if it were a station user.

When a message is left in a mailbox that uses this type of message waiting, the server takes a port off-hook, dials a string of DTMF digits, then goes on-hook. The PBX translates these digits and turns the appropriate indicator on. When all unplayed messages have been played, the server follows the same procedure (dialing a different string of digits) to turn the indicator off.

You need to set up a line group of at least one line, which is dedicated to outdialing DTMF-to-PBX message waiting signals.

DTMF-to-PBX Message Lights Worksheet

Configuring these message indicators involves two steps:

- setting up a line group of at least one line to serve as an outdialer of message indicators requests, and
- configuring the dial strings that constitute these requests.

Complete the worksheet (sample below) before configuring the server. Blank worksheet is here.

Configuring the PBX

Assign, to each server line that is dedicated to this application, a PBX class of service that permits the server to turn message waiting indicators on and off.

Note:

- Message waiting indicators are affected by timer settings in the MiVoice Business system. To avoid premature extinguishing of MWI, ensure that the **SUPERSET Callback Message Cancel Timer** parameter in the **System Options Assignment** form is **BLANK**. (An entry in this field sets a time limit for MWI to be displayed, after which the indicator is extinguished.)
- In an environment with resilient MiVoice BusinessICPs,an open communication path is required between the ICPs whenever a MWI messaging event occurs. Without a communication path, events will not be synchronized and the user's message waiting lamp will fail to turn on/off correctly.

Configuring the Application

There are three steps to configuring DTMF-to-PBX message indicators:

1. Determine what DTMF strings the PBX uses to turn message waiting indicators on and off, and use this information to complete the DTMF-to-PBX Message Lights Worksheet.
2. Create a line group with one or more lines to be used as an outdialer port. If your PBX only allows a message waiting indicator to be turned off by the same extension that turned it on, you can still configure a multi-line group if needed for heavy traffic volumes. The NuPoint Unified Messaging server uses the correct port to turn off message waiting indicators for specific extensions.
3. Enter the information at the server maintenance console.

All configuring of the DTMF-to-PBX message waiting indicators is PBX-dependent. If your PBX allows users to turn the message indicators of other users on and off, then the proper coding can usually be found in the PBX users' guide. Otherwise, consult the PBX operating manual or your PBX vendor for the necessary codes.

The DTMF-to-PBX Message Lights application menu prompts for specific sections of the dial strings. The dial strings are dialed out in the following order:

1. PBX special access code
2. Pre-DN on or off string (after dial tone confirmation)
3. Directory number
4. Post-DN on or off string (followed by a wait for dial tone)

Sample DTMF-to-PBX Message Lights Worksheet

Line Group Information

All server ports are assigned to line groups. Each line group is then assigned to a single application, and any configuring that is done for that application applies to every port in the line group. The number of ports in each line group depends on how heavy the phone traffic is expected to be for that particular application.

Line Group

Each line group is represented by a distinct number. Valid line group numbers are 1 through 24.

Group Name

The group name is optional. It serves to easily identify the line group's purpose; for example, the line group for this application can be called "DTMF-to-PBX Outdialer."

Line(s) in Group

You identify each line (or port) in a group by a triplet, which represent the module, slot (line card), and port. Module refers to a CPU, the server's main processor. Modules are numbered at 1. Slots are numbered at 0. Ports are also numbered from 0 and the upper limit depends on the port limit of your system licensing (maximum is 60, so the range is 0-59). In a sense, you connect one telephone line to each port.

For more information on triplets and line group numbering, see NuPoint Voice Application.

Initial Dial Tone Detection

When building outdial strings, the Initial Dialtone Detect parameter gives you precise control. This parameter allows you to include a T code (Go Off-Hook, Wait for Dial Tone) if you are integrating with most PBXs, or delete a T code in the dial string if you are integrating with cellular or other non-PBX equipment that cannot produce a dial tone.

The outdial string consists of the following parts:

- Initial T code produced by this parameter, if enabled
- PBX special access code parameter, if any
- Appropriate on or off dial string parameter (the pre-DN on dial string, pre-DN off dial string, post-DN on dial string, or post-DN off dial string).

Note:
If you enable this parameter ("enabled" is the default), do not enter a T code as the first part of the special access code. If you do, the server waits for two separate dial tones. But two separate dial tones cannot occur in this context, so every message indicator request fails.

If you disable this parameter, you typically begin the special access code with the S (Go Off-Hook, Do Not Wait for Dial Tone) code.

PBX Special Access Code

Some PBXs require the server to dial a special access code before sending message indicators requests. The special access code indicates to the PBX that one of its special features is about to be invoked. Table 4-1 lists the characters allowed in this code.

Note:
The NuPoint Unified Messaging server automatically configures a T (Go Off-Hook, Wait for Dial Tone) as the first part of the outdial string. DO NOT enter a T as the first part of the special access code because then the server waits for two separate dial tones.

There is no default PBX special access code.

Dial Tone Confirmation

Answer Yes to this parameter only if (1) a PBX special access code is required and (2) if, after the special access code has been sent, the PBX expects the server to wait for a dial tone before the server outdials any other digits. The default is No (no wait).

Pre-DN On or Off String

This string is sent before the directory number (extension number) to instruct the PBX to turn the message waiting indicator on or off at that station. There is no default Pre-DN on or off string.

Note:
Never enter a T as the first part of the Pre-DN on string because then the server waits for two separate dial tones.

Enter the coding, if any, that must be sent before the directory number to turn message waiting indicators on or off.

Suppress Updates to MWL

Each time a mailbox receives a new message, the server sends a request to the PBX to turn on the message indicator. However, if the user logs into the server, listens to all the new messages, and logs out, a single indicator-off request is sent to the PBX. Some PBXs stack the indicator-on requests. Then, when the single indicator-off request is sent, it cancels only one of the indicator-on requests, and the message indicator stays on. To prevent the server from sending an indicator-on request when the message indicator is already activated, leave this feature at the default setting of Yes. This feature also cuts down on overall message waiting indicators traffic.

PBX Special Access Code Characters

Character	Explanation
0-9, *, #	Keys on a standard pushbutton telephone
(	The following digits should be dial pulsed (10 PPS)
)	Stop pulsing; resume sending DTMF tones
+	Pause for one second
A-D	Fourth column DTMF keys
E	Go off-hook, wait for dial tone or other steady tone (pager go-ahead or confirmation tone, for example), then do next item in string
F	Switch hook flash and wait for dial tone
G	Greet - Wait for a voice or computer tone answer
H	Hang up (go on-hook)
L	Answer Supervision - Wait for telephony signal from destination. Use only with trunk (four-wire) connections.
N	Start a new activity; do not go off-hook
O	Ring once
P	Go off-hook, do not wait for dial tone
S	Switch hook flash, no wait required

Character	Explanation
T	Go off-hook, wait for dial tone
V	A voice pager system is being used

Post-DN ON or OFF String

This string is sent after the directory number (extension number) to instruct the PBX to turn the message waiting indicator on or off at that station. There is no default post-DN on or off string.

Enter the coding, if any, that must be sent after the directory number to turn message waiting indicators on or off.

Wait for Dial Tone

The default value is N. If the PBX can return dial tone to the server to indicate that a message indicator has been turned on or off successfully, answer Yes. The server registers an error condition if dial tone is not returned, and redials the appropriate dial string.

Enable Alternate Code

The alternate code is the DTMF string that the server transmits after the pre-DN on string. Typically, the directory number (DN) and the mailbox number are the same. The server expects this to be the case, because it includes the mailbox number as the DN when it sends a message indicators request to the PBX. Sometimes, though, the DN and mailbox number are different. In those cases, do the following to make sure users get message waiting indication:

- Enable this parameter.
- Put the DN in the Department Code parameter of the mailbox's configuration. (The software supports up to 2000 department codes.)

After you complete these steps, the server uses the value of the Department Code parameter in the mailbox's configuration as the DN when it sends the request to the PBX.

Testing

Testing is done using the Text Console.

26.48.3 DTMF to PBX MWI Configuration

This procedure summarizes the steps for configuring DTMF-to-PBX message waiting indicators.

To configure DTMF TO PBX MWI, for each node:

1. Complete a DTMF-to-PBX Message Lights Worksheet. For detailed parameter information, see Configuration Requirements.

2. Define a line group to be used for the DTMF-to-PBX Message Lights application. You must define at least one line to serve as an outdialer of message indicator requests.

1. *Set DTMF-to-PBX protocols.*
2. *I*f user mailbox numbers are different from extension numbers, configure the server to use alternate codes.
3. Verify the configuration.
4. Assign message waiting type **3** as the first or second message waiting type in mailboxes that are to send message waiting indicator requests.
5. Test the DTMF-to-PBX Message Lights application (Text console only).

26.48.4 Configure Message Cancel Timer



If you have a MiVoice Business ICP, on the System Options form you must change the SUPERSET Callback Message Cancel Timer setting from 24 (hours) to blank to ensure the Message Waiting Indicator continues to flash until you have listened to your messages.

26.48.5 Turn off MWI for Skipped Messages

FCOS bit 302 allows users to skip a new message, have it remain in the unplayed queue and then, if no other unplayed messages exist, have the MWI lamp turn off when they log out. Users are still able to log in at any time and listen to the skipped messages that are marked as unplayed and are announced as such.

This alternate MWI behavior is controlled by FCOS bit **302** (Enable Alternate MWI for Skipped Messages) and can be assigned on a per mailbox basis.

Conditions

Must have the following feature bits enabled:

- **204** - Message Skip, Forward and Backward
- **145** - Message Stays in Original Queue on Hangup

To enable this feature, customize an FCOS as necessary and apply to the required mailboxes.

26.48.6 Set DTMF-to-PBX Protocols

This procedure describes how to set the following parameters for DTMF-to-PBX message waiting indicators:

- Dial strings (feature access codes) that the server must send to the PBX before or after the mailbox number in order to set message waiting indicators
- Places in the dial string at which the server must wait for dial tone from the switch while setting message waiting indicators

- Whether the server should send a message wait "on" request to the switch for every new message, or only when a mailbox with no new messages receives a message

To set DTMF-to-PBX protocols:

1. From the navigation tree, select **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups** and then click **Add**.
4. In the Application list, select **DTMF to PBX Dialer**.
5. Configure the parameters on the **Lines** and **DTMF to PBX Dialer** tabs as described in the DTMF-to-PBX application parameters listing. Use the parameters on this tab to set the following optional settings:
   - Initial Dialtone Detect
   - Dial Tone Confirmation
   - Suppress MWI Updates
   - Wait for Dial Tone
   - Enable Alternate Code (to compensate for different directory and mailbox numbers)
6. Click **Save**.
7. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.48.7 Set DTMF-to-PBX Protocols

This procedure describes how to set these parameters for DTMF-to-PBX message waiting indicators:

- Dial strings (feature access codes) that the server must send to the PBX before or after the mailbox number in order to set message waiting indicators
- Places in the dial string at which the server must wait for dial tone from the switch while setting message waiting indicators
- Whether the server should send a message wait "on" request to the switch for every new message, or only when a mailbox with no new messages receives a message

To set DTMF-to-PBX protocols:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.

CAUTION:
You should make all offline configuration entries on a duplicate of the active configuration so that you can easily check them, and easily correct them if necessary, before activating the configuration.

2. Select **(B) Duplicate Active Configuration**. The server copies the current (active) configuration.

Note:
All subsequent steps in this procedure – along with any other configuration entries – affect only the duplicate (inactive) configuration, and will take effect only after you activate the inactive configuration.

3. Select **(T) DTMF to PBX Message Lights**.
4. Select **(G) Group Selected** and enter the **number** of the line group (1-24) or press **Enter** if the current number is correct.
5. Select **(D) DTMF to PBX Message Lights**.

Set Pre- and Post-DN Dial Strings

1. If the PBX requires a special access code to be dialed first, select **(A) PBX Special Access Code** and enter the required dial **string** (0-24 characters) or type a **period** (.) to delete an existing dial string. Consult the PBX operating manual or the PBX vendor for the correct code or use the table below to configure a string.
2.

Note:
If you are planning to enable a "wait for an initial dial tone", do not enter a T (wait for dial tone) as the first part of the special access code.

3. If the PBX requires a dial string BEFORE the directory number to turn the message waiting indicator ON, select **(D) Pre-DN ON Dial String** and enter the required dial **string** (0-24 characters), or enter a **period** (.) to delete an existing dial string.
4. If the PBX requires a dial string BEFORE the directory number to turn the message waiting indicator OFF, select **(F) Pre-DN OFF Dial String** and enter the required dial **string** (0-24 characters), or enter a **period** (.) to delete an existing dial string.
5. If the PBX requires a dial string AFTER the directory number to turn the message waiting indicator ON, select **(P) Post-DN ON Dial String** and enter the required dial **string** (0-24 characters), or enter a **period** (.) to delete an existing dial string.
6. If the PBX requires a dial string AFTER the directory number to turn the message waiting indicator OFF, select **(Q) Post-DN OFF Dial String** and enter the required dial **string** (0-24 characters), or enter a **period** (.) to delete an existing dial string.

Set Dial Tone Call Progress Verification

1. To enable/disable a "wait for initial dial tone", select **(I) Initial Dialtone Detect**. Select **Y** if integrating with PBX equipment that produces an initial dial tone, or **N** if integrating with cellular or other non-PBX equipment that cannot produce a dial tone.
2. To enable/disable dial tone confirmation, select **(C) Dial Tone Confirmation**. Select **Y** if a PBX special access code is required and the PBX expects the server to wait for a dial tone before outdialing any other digits, or **N** in all other cases.
3. To enable/disable a "wait for a dial tone after a message indicators" request, select **(W) Wait for Dial Tone** and then select **Y** if the PBX returns a dial tone to indicate that a message indicator request was successful, or **N** in all other cases.

Set Successive Indicator "On" Requests

1. To enable/disable successive indicator-on requests, select **(S) Suppress Updates to MWL** and then select **Y** to to suppress updates of Message Waiting Lights after users access their mailbox without a change in status, or N to enable successive indicator-on requests.
2. Save the changes to the inactive configuration by exiting to the NuPoint Voice Configuration Main Menu.

Dial String Characters	
Character	**Explanation**
0-9, *, #	Keys on a standard push button telephone
A-D	Fourth column DTMF keys
( )	Dial Pulse (10PPS) the characters between the parent heses
+	Pause for one second
T	Go off-hook, wait for dial tone
P	Go off-hook, do not wait for dial tone
E	Go off-hook, wait for dial tone or other steady tone then do next item in string
G	Greet - Wait for a voice or computer tone answer
H	Hang up (go on-hook)
F	Switch hook flash and wait for dial tone
S	Switch hook flash, no wait required
N	Start a new activity; do not go off-hook
L	Wait for an answer supervision signal that indicates the receiving phone has gone off-hook, then dial remaining characters after receiving the signal. Valid only with four-wire connections, not with loop start or ground start ph one lines.

26.48.8 Compensate for Different Directory and Mailbox Numbers

This procedure describes how to configure the server when the directory number differs from the mailbox number in the following applications:

- DTMF-to-PBX Message Lights
- RS-232 Message Waiting Indicators

To allow your MWI application to compensate for different directory and mailbox numbers:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. Duplicate the configuration by selecting **(B) Duplicate Active Configuration**. The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears. All subsequent steps in this procedure – along with any other configuration entries – affect just the copy, and take effect only after you activate the configuration.

For configuration procedures for the RS-232 MWI interface, go to step 11.

To configure the server for different directory and mailbox numbers for the DTMF-to-PBX MWIs:

1. Specify the line group to which the DTMF-to-PBX Message Lights application is assigned by selecting **(G) Group Selected**. At the **Enter a group number**prompt, enter the **number** of the line group (1-24) to which the DTMF-to-PBX Message Lights application is assigned.
2. Select **(T) DTMF to PBX Message Lights**.
3. Enable an alternate code by selecting **(T) Enable Alternate Code**. At the **Enable alternate code (y/n)**prompt, enter **Y** for yes.
4. Save the setting by exiting to the NuPoint Voice Configuration Main Menu.
5. Exit to the Mailbox Maintenance Menu, and select **(C) Create New Mailboxes** or **(M) Modify Mailboxes**.
6. Enter the number of the mailbox to create/modify.
7. Press **Enter** until the **Department Code** prompt appears.
8. Enter the DN (directory number) by entering the DTMF **string**, which is the alternate code the server transmits after the pre-DN ON string.
9. Press Enter to skip through the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.
10. At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

To configure the RS-232 MWIs Interface:

1. From the Offline Menu, select **(M) RS232 Only Applications** and then select **(R) Programmable**.
2. Enable an alternate code by selecting **(D) Dept Code as DN?**. At the **E nter "N" for mailbox #, "Y" for dept code**, enter **Y** for department code.
3. Save the setting by exiting to the NuPoint Voice Configuration Main Menu.
4. Exit to the Mailbox Maintenance Menu, and select **(C) Create New Mailboxes** or **(M) Modify Mailboxes**.

5. Enter the number of the mailbox to create/modify.
6. Press **Enter** until the **Department Code** prompt appears.
7. Enter the DN (directory number) by entering the DTMF **string** that is the alternate code the server transmits after the pre-DN ON string. Any ASCII character is valid in this string.
8. Press Enter to skip through the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number.
9. At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.48.9 Refresh or Suppress MWI

You may want to refresh or suppress message waiting indicators. Reach the Suppress/Refresh MWI menu from the Main Menu by selecting **(S) System Maintenance**, **(R) Reconfiguration**, then **(C) Suppress/ Refresh MWI**.

At the Suppress/Refresh MWI menu, you can set parameters to refresh some or all message waiting indicators, suppress message waiting indicators for specific MWI types, and view the current MWI types and settings. When you set the first and last mailboxes, be sure that the range is no more than the maximum of 2400 mailboxes.

26.48.10 Test DTMF-to-PBX MWI Configuration

LEAVE VISIBLE TO THE WEB CONSOLE

Create at least one mailbox with the DTMF-to-PBX message waiting type that is appropriate for your server. To test the message waiting indicators, choose the Lights Test option from the server maintenance console, and select the proper message waiting type.

The following procedure describes how to test the MWI configuration:

1. From the Main Menu, select **(S) System Maintenance**, and then **(O) Additional Options**.
2. Select **(L) Lights Test** to start the Lights Test and then enter the number of the test extension that has a mailbox configured for DTMF-to-PBX MWI (MWI type 3).
3. At the **Light off/on/existing value (0/1/2):** prompt, enter **0** to turn the light off (to clear any existing indicator on the test extension).
4. At the **Message waiting type** prompt, enter **3** for DTMF-to-PBX. When prompted for mailbox number, enter the number of the test mailbox you used in step 3.
5. At the **Light off/on/existing value (0/1/2):** prompt, enter **1** to turn the light on. The system dials the message waiting code to light the MWI lamp on the test extension. Check the indicator on the test extension.

Note:
The light off/on/existing value field is interpreted as 0 for off, 1 for on and 2 to send the existing value for the mailbox (useful if you want to refresh the message waiting lamps).

26.48.11 Test Message Waiting Indication (Text Console only)

This procedure describes how to test message waiting lights after they have been configured for mailboxes in your server.

Prerequisites for this procedure are:

- All appropriate hardware has been installed.
- Telephone lines have been installed and tested for dial tone.
- Test mailboxes have been configured for message waiting lights.

To test MWI:

1. If you have not already done so, obtain a System Configuration Report. Refer to the report as needed for the configuration parameters that you have set.
2. Use Event Recorder to monitor server activity during test pages and report the resulting data:
   - Specify the line on which the pager being tested is defined.
   - Specify the message level to be saved.
   - Enable Event Recorder.
   - Run Event Recorder.
   - Display the data at the server maintenance console.
3. From the Main Menu, select **(S) System Maintenance**, and then **(O) Additional Options**.
4. Select **(L) Lights Test** and enter the **number** of the mailbox to light or a range of mailbox numbers separated by a hyphen.

> **Note**:
> If you select a large range of mailboxes, the Lights Test could queue up a long list of message waiting requests and could take a long time to process.

5. At the **Light off/on/existing value (0/1/2):** prompt, enter **0** to turn the message waiting lights off.
6. At the **Message waiting type:** prompt, enter the **number** of the message waiting type assigned to the mailboxes you selected or press **Enter** for all message waiting types.

Number	Message Waiting Type
0	None
3	DTMF to PBX
5	Pager (See Pager Application)
7	Program RS232
9	Centrex RS232
11	Centrex
16	HIS PMS
17	Unified Integration

Number	Message Waiting Type
21	Hitachi PMS
28	MiTAI Messaging

7. At the **Mailbox to light (1-99999999999):** prompt, enter the same mailbox **number**, or range of numbers that you entered in step 4.
8. At the **Light off/on/existing value (0/1/2):** prompt, enter 1 to turn the message waiting lights on.
9. At the **Message waiting type:** prompt, enter the **number** of the message waiting type assigned to the mailboxes you selected or press **Enter** for all message waiting types.
10. The server prompts for another mailbox to light. To repeat the test, perform steps 4 through 9 again.
11. Review Event Recorder data reported at the server maintenance console to determine if any errors were encountered.
12. At the **Mailbox to light (1-99999999999):** prompt, enter another mailbox number to test OR press **Enter** to stop the Lights Test, then Exit to the Main Menu.

26.49 MiVoice Business ICP Programming for MiTAI MWI

Note:

- The MiTAI Messaging MWI does not support the configuration of MiVoice Business ICP as a gateway.
- In an environment with resilient MiVoice BusinessICPs, an open communication path is required between the ICPs whenever a MWI messaging event occurs. Without a communication path, events will not be synchronized and the user's message waiting lamp will fail to turn on/off correctly.

MiTAI MWI must be configured on both the MiVoice Business ICP and the NuPoint Unified Messaging systems.

Creating an HCI Reroute Hunt Group on the MiVoice Business ICP

For programming the MiVoice Business ICP to support HCI Reroute Hunt Group, the following steps need to be performed on the MiVoice Business ICP side:

1. Open the MiVoice Business ICP System Administration Tool and in the Selection: drop-down menu, click **System Administration**.
2. Navigate to the **Hunt Groups** form (click Users and Devices > Group Programming > Hunt Groups).
3. Click **Add**.
4. In the **Hunt Group** field, type the hunt group **number**.
5. In the **Hunt Group Type** field, select **HCIReroute**.
6. Click **Save**.

7. Navigate to the **Call Rerouting Always Alternatives** form (Call Routing > Call Handling > Call Rerouting Always Alternatives). Choose an unused **Always Alternative Number**, then click **Change**. Do not use Call Reroute number 1.

Note:
Remember the Always Alternative Number, because you need it in the final step of this procedure.

8. In the **Call Rerouting Always Alternatives** form, change all four **Always Originating Device** values to **Reroute**, and change **Directory Number to Reroute to** to the NP-UM messaging hunt group pilot number.
9. Click **Save**.
10. Navigate to the**Call Rerouting**form (Call Routing > Call Handling > Call Rerouting).
11. In the Call Routing folder, navigate to the pilot number of the HCI Reroute hunt group.
12. Click **Change**.
13. In the **Call Rerouting** window, change the **Call Rerouting Day**, **Call Rerouting Night1**, and **Call Rerouting Night2** numbers to the **Call Rerouting Always Alternative** number created in Step 7.

Note:
Message waiting indicators are affected by timer settings in the MiVoice Business system. To avoid premature extinguishing of MWI, ensure that the **SUPERSET Callback Message Cancel Timer** parameter in the **System Options** form is **BLANK**. (An entry in this field sets a time limit for MWI to be displayed, after which the indicator is extinguished.)

For detailed programming information, refer to *the MiVoice Business System Administration Tool Online Help.*

Web Console:

- *Configure NuPoint UM for MiTAI MWI*

Text Console:

- *Configure NuPoint UM for MiTAI MWI*

26.49.1 MiVoice Business ICP Programming for MiTAI MWI

Note:

- The MiTAI Messaging MWI does not support the configuration of MiVoice Business ICP as a gateway.
- In an environment with resilient MiVoice BusinessICPs, an open communication path is required between the ICPs whenever a MWI messaging event occurs. Without a communication path, events will not be synchronized and the user's message waiting lamp will fail to turn on/off correctly.

MiTAI MWI must be configured on both the MiVoice Business ICP and the NuPoint Unified Messaging systems.

Creating an HCI Reroute Hunt Group on the MiVoice Business ICP

For programming the MiVoice Business ICP to support HCI Reroute Hunt Group, the following steps need to be performed on the MiVoice Business ICP side:

1. Open the MiVoice Business ICP System Administration Tool and in the Selection: drop-down menu, click **System Administration**.
2. Navigate to the **Hunt Groups** form (click Users and Devices > Group Programming > Hunt Groups).
3. Click **Add**.
4. In the **Hunt Group** field, type the hunt group **number**.
5. In the **Hunt Group Type** field, select **HCIReroute**.
6. Click **Save**.
7. Navigate to the **Call Rerouting Always Alternatives** form (Call Routing > Call Handling > Call Rerouting Always Alternatives). Choose an unused **Always Alternative Number**, then click **Change**. Do not use Call Reroute number 1.

Note:
Remember the Always Alternative Number, because you need it in the final step of this procedure.

8. In the **Call Rerouting Always Alternatives** form, change all four **Always Originating Device** values to **Reroute**, and change **Directory Number to Reroute to** to the NP-UM messaging hunt group pilot number.
9. Click **Save**.
10. Navigate to the**Call Rerouting**form (Call Routing > Call Handling > Call Rerouting).
11. In the Call Routing folder, navigate to the pilot number of the HCI Reroute hunt group.
12. Click **Change**.
13. In the **Call Rerouting** window, change the **Call Rerouting Day**, **Call Rerouting Night1**, and **Call Rerouting Night2** numbers to the **Call Rerouting Always Alternative** number created in Step 7.

Note:
Message waiting indicators are affected by timer settings in the MiVoice Business system. To avoid premature extinguishing of MWI, ensure that the **SUPERSET Callback Message Cancel Timer** parameter in the **System Options** form is **BLANK**. (An entry in this field sets a time limit for MWI to be displayed, after which the indicator is extinguished.)

For detailed programming information, refer to *the MiVoice Business System Administration Tool Online Help*.

Web Console:

- *Configure NuPoint UM for MiTAI MWI*

Text Console:

- *Configure NuPoint UM for MiTAI MWI*

26.49.2 Configure NuPoint UM for MiTAI MWI

MiTAI MWI support requires configuration in the server and in Mailbox maintenance.

Server Configuration

The NuPoint Unified Messaging server needs to know the HCI Reroute Hunt Group number to generate the proper MWI messages. Set this up in the MiVoice Business ICP Integration menu:

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, **(G) Offline Menu**, **(I) Server Options and Configuration**, and then **(C) Configure Mitel MCD integration**.
2. Select **(H) HCI Reroute Hunt Group Number for Mitai MWI** and enter the HCI Reroute Hunt Group number.

26.50 Introduction

This section includes an overview of RS-232 message waiting indicator interfaces, provides hardware requirements, worksheets and planning information, and includes the following configuration procedures:

- Configuring a Programmable MWI application
- Testing RS-232 MWI Configuration

The RS-232 MWI application allows servers to turn PBX message waiting indicators on and off by sending signals to the PBX over RS-232 data links. The data links can be either direct serial connections to the PBX, or they can connect to modems that are connected to analog ports on the PBX.

When a message is left in a mailbox, the server sends an ASCII message that tells the PBX to turn on the message waiting indicator at the appropriate station. Conversely, when all unplayed messages are played, the server sends an ASCII string that directs the PBX to turn off the message waiting indicator.

RS-232 Serial Port or Modem Requirements

To use any of the RS-232 message waiting indicator interfaces, an RS-232 cable must be run from a server serial port to the PBX (or, in the case of CentrexRS-232 MWI interface, to a modem that communicates with the Central Office).

The physical setup uses RS-232 pins 2, 3, and 4, with communications parameters of 1200 baud, 8 data bits, 1 stop bit, no parity, full duplex, and no flow control.

If you have an expansion serial port card installed in your server, you can use as many serial ports as necessary for the programmable RS-232 message waiting application. You must first assign and configure a single serial port using index 1, which enables any additional ports assigned to the application to adopt the configuration of the first port.

26.50.1 Defining an RS-232 Serial Port

Introduction

The RS-232 MWI application allows servers to turn PBX message waiting indicators on and off by sending signals to the PBX over RS-232 data links. The data links can be either direct serial connections to the PBX, or they can connect to modems that are connected to analog ports on the PBX.

When a message is left in a mailbox, the server sends an ASCII message that tells the PBX to turn on the message waiting indicator at the appropriate station. Conversely, when all unplayed messages are played, the server sends an ASCII string that directs the PBX to turn off the message waiting indicator.

Requirements

To use any of the RS-232 message waiting indicator interfaces, an RS-232 cable must be run from a server serial port to the PBX (or, in the case of Centrex RS-232 MWI interface, to a modem that communicates with the Central Office).

The physical setup uses RS-232 pins 2, 3, and 4, with communications parameters of 1200 baud, 8 data bits, 1 stop bit, no parity, full duplex, and no flow control.

If you have an expansion serial port card installed in your server, you can use as many serial ports as necessary for the programmable RS-232 message waiting application. You must first assign and configure a single serial port using index 1, which enables any additional ports assigned to the application to adopt the configuration of the first port.

26.50.2 Programmable RS-232 MWI Interface

Planning

The programmable option allows you to customize the RS-232 message indicator software interface between the server and the PBX. All codes are sent in ASCII. Numbers, letters, and certain special characters (see table below) are understood by the software.

RS-232 Message Waiting Indicators Interface Codes

Code	Explanation
\r	carriage return
\n	new line
\t	tab
\b	backspace
\f	form feed
\\	backslash
\"	double quotes
\?	question mark
.	no string needed

The RS-232 Message Waiting Lights Worksheet organizes the information that is necessary for configuring the programmable interface. You can use ASCII codes in any of strings listed below.

Sample RS-232 Message Waiting Lights Worksheet

The following list provides definitions for the RS-2323 Message Waiting Lights Worksheet:

Initialization String

This string is sent to the PBX to notify it that the server is ready to send message waiting indicator requests.

Reply String

After the initialization string is sent, the server waits for the PBX to return this reply string, before sending message indicators requests.

Pre-DN On String

This string is sent before the directory number (extension number) to instruct the PBX to turn the message waiting indicator on at that station.

Pre-DN Off String

This string is sent before the directory number (extension number) to instruct the PBX to turn the message waiting indicator off at that station.

Post-DN On String

Enter the coding, if any, that must be sent after the directory number to turn message waiting indicators on. There is no default post-DN on string.

Post-DN Off String

Enter the coding, if any, that must be sent after the directory number to turn message waiting indicators off. There is no default post-DN off string.

Department Code as DN?

Enter Yes if you want the server to send the department code as the DN when issuing a request to turn indicators on or off. When this feature is set at the default value, No, the server sends the mailbox number as the DN.

Unplayed Number Sent?

Enter Yes if you want the server to send the number of unplayed messages after the DN, when issuing a request to turn indicators on. The default value is No.

Delay After Post-DN String

This parameter is the period of time, in seconds, between the post-DN off string and the ending trailer string. This delay gives the PBX time to process each request correctly. If requests come too quickly, the PBX could drop or corrupt them. From 0 to 255 seconds can be specified. There is no default delay.

Ending Trailer String

If the PBX requires this string, the server sends it after the delay just described. Use the characters in Table 5-3 to create this string, up to 30 characters long. There is no default ending trailer string.

Suppress Updates to MWL?

A server administrator can configure whether message waiting indicator on or off requests are sent out for every new unplayed message, or only when the message waiting indicator state changes from off to on or from on to off. Using the latter functionality (only when the message waiting indicator state changes) makes better use of server resources.

The server does not suppress message waiting indicator updates by default. To suppress them, you must enter the message waiting type number of your RS-232 system, then enter Yes. (The default is No for all types.) Message waiting types are listed in the following table.

Message Waiting Types

Number	Message Waiting Type
0	None
3	DTMF-to-PBX
5	Pager
11	Centrex
16	HIS PMS

Number	Message Waiting Type
17	Unified Integrations
21	Hitachi PMS
28	MiTAI Messaging

Modem Result Code

The modem result code parameter allows the server to determine if a message waiting request was accepted by the switch, and to retry a failed request if necessary. The modem result code tells the server to look for a certain message from the modem to indicate that the message waiting request was accepted by the switch. You must know the message that the modem returns, for example, "NO CARRIER." The server looks for the exact message set in the Modem Result Code field, and, if it does not see it, retries the message waiting request up to 18 times.

You can find out what result code the modem returns by setting this field to some value (it doesn't matter what), and then turning on the Pager/Programmable RS232 interface in Event Recorder. Use the Lights Test to send an MWI request to a mailbox that has its MWI type set to Programmable RS232. The Event Recorder message will show you the actual result string that is returned from the modem. You can then set the Modem Result Code field to that value, assuming that the request was completed successfully.

Leave this field blank to have the server ignore any result code returned by the modem and assume that all message waiting requests are successful. To remove a previously configured value, enter a period.

26.50.3 Configure Programmable RS-232 MWI

The programmable RS-232 MWI interface is configured entirely offline, through the External Applications menu. This procedure assumes that the appropriate server hardware and software have been installed.

Perform the following steps to configure the programmable RS-232 message waiting indicators interface in a server:

1. Complete an RS-232 Message Waiting Indicators Interface Worksheet.
2. Create the interface string. See Creating a Programmable RS-232 Interface String. This procedure includes instructions for:
   - setting delay times
   - enabling indicator-on requests for successive messages
   - sending the number of unplayed messages
   - compensating for different directory and mailbox numbers
3. Assign message waiting type **7** (programmable interface) through the first or second message waiting type prompt in mailboxes that are to receive message waiting indicator requests. See Assigning Message Waiting Indicators to a Mailbox.
4. Use the Lights Test (Text console) described in the DTMF-to-PBX section to test RS-232 configuration. The modem will go off hook and dial the message waiting code to light the MWI lamp on the telephone set.

26.50.4 Creating a Programmable RS-232 Interface String

The RS-232 programmable interface string consists of the following parts:

- Initialization string, if required by the PBX.
- Reply string, if required by the PBX.
- Any of the applicable indicator-on or indicator-off request strings (pre-DN ON, pre-DN OFF, post-DN ON, post-DN OFF, ending trailer string).

To create a string of ASCII codes for the RS-232 programmable interface:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click **External Applications**.
4. Select the **Serial port** (1-2) or **IP port** (1-4) to program.
5. In the Application list, select **Programmable**.
6. In the **Initialization String** field, enter the ASCII **string** (0-30 characters) required by the PBX, or a period (.) to delete an existing string. To create the **string**, consult the PBX operating manual or the PBX vendor for the correct code, and use the ASCII Characters table at the end of this procedure.
7. In the **Reply String** field, enter the ASCII **string** (0-30 characters) sent by the PBX, or a period (.) to delete an existing string. To create the **string**, consult the PBX operating manual or the PBX vendor for the correct code, and use Table 1 at the end of this procedure.
8. In the **Delay Between Requests** field, set the delay time between successive message waiting indicators requests in **seconds** (0-255).
9. In the **Pre-DN ON String** field, perform the action that corresponds to the following PBX behavior:
    - If the PBX requires the string before the directory number (sometimes called extension number), create an **ASCII string** (0-30 characters) using the characters in the table at the end of this procedure.
    - If the PBX sends the string after the directory number:
        - enter a **period** (.) to delete an existing string, if necessary.
        - enter values for the Post-DN ON String and Post-DN OFF String parameters.
10. In the **Pre-DN OFF String** field, perform the action that corresponds to the following PBX behavior:
    - If the PBX requires the string before the directory number, create an ASCII string (0-30 characters) using the characters in Table 1.
    - If the PBX sends the string after the directory number:
        - enter a **period** (.) to delete an existing string, if necessary.
        - enter values for the Post-DN ON String and Post-DN OFF String parameters.

11. In the **Post-DN ON String** field, perform the action that corresponds to the following PBX behavior:

    - If the PBX requires the string before the directory number, create an ASCII string (0-30 characters) using the characters in Table 1.
    - If the PBX sends the string after the directory number:

        - enter a **period** (.) to delete an existing string, if necessary.
        - enter values for the Post-DN ON String and Post-DN OFF String parameters.

12. In the **Post-DN OFF String** field, perform the action that corresponds to the following PBX behavior:

    - If the PBX requires the string before the directory number, create an ASCII string (0-30 characters) using the characters in Table 1.
    - If the PBX sends the string after the directory number:

        - enter a **period** (.) to delete an existing string, if necessary.
        - enter values for the Post-DN ON String and Post-DN OFF String parameters.

13. To use the Department Code as the DN for MWI (i.e. when the directory number differs from the mailbox number) select the **Department Code as DN** check box. (Note: If Department Code is not configured, MWI lights on the mailbox number.)
14. To send the number of unplayed messages through the RS-232 interface after the directory number in a message light-on request, select the **Unplayed Number Sen**t check box.
15. To set the time for delays between the post-DN OFF string and ending trailer string, enter the number of **seconds** (0-255) in the **Delay After Post-DN String** field.
16. In the **Ending Trailing String** field, perform the action that corresponds to the following PBX behavior:

    - If the PBX requires this string, create an **ASCII string** (0-30 characters) using the characters in the table below.
    - If the PBX does not require this string, enter a **period** (.) to delete an existing string.

17. Click **Save**.
18. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

ASCII Characters

Character	Explanation
\b	Backspace
\f	Form feed
\n	New line
\r	Carriage return

Character	Explanation
\t	Tab
\\	Backslash
\"	Double quotes
\?	Question mark

26.50.5 Programming RS-232 MWI Using a Modem

The NuPoint Unified Messaging system offers a programmable RS-232 message waiting application that allows you to set up either the built-in COM port 2 or a single port of an optional add-in serial card to provide the necessary AT commands to be sent to an external modem.

The modem line port is in turn connected to an ONS port on the PABX which allows NuPoint UM to turn on and off message waiting lamps in a similar way as that done by the DTMF-to-PBX message waiting application.

Mitel recommends that external US Robotics modems be used for this application. Other modems will work, however, Mitel cannot provide support in troubleshooting other vendor modems.

Note:
This procedure uses the NuPoint Unified Messaging RS-232 COM2 port in conjunction with a US Robotics modem. A straight-through cable should be used from the modem to the COM2 port.

The following switch settings need to be set on the US Robotics Sportster modem:

US Robotics Switch Settings

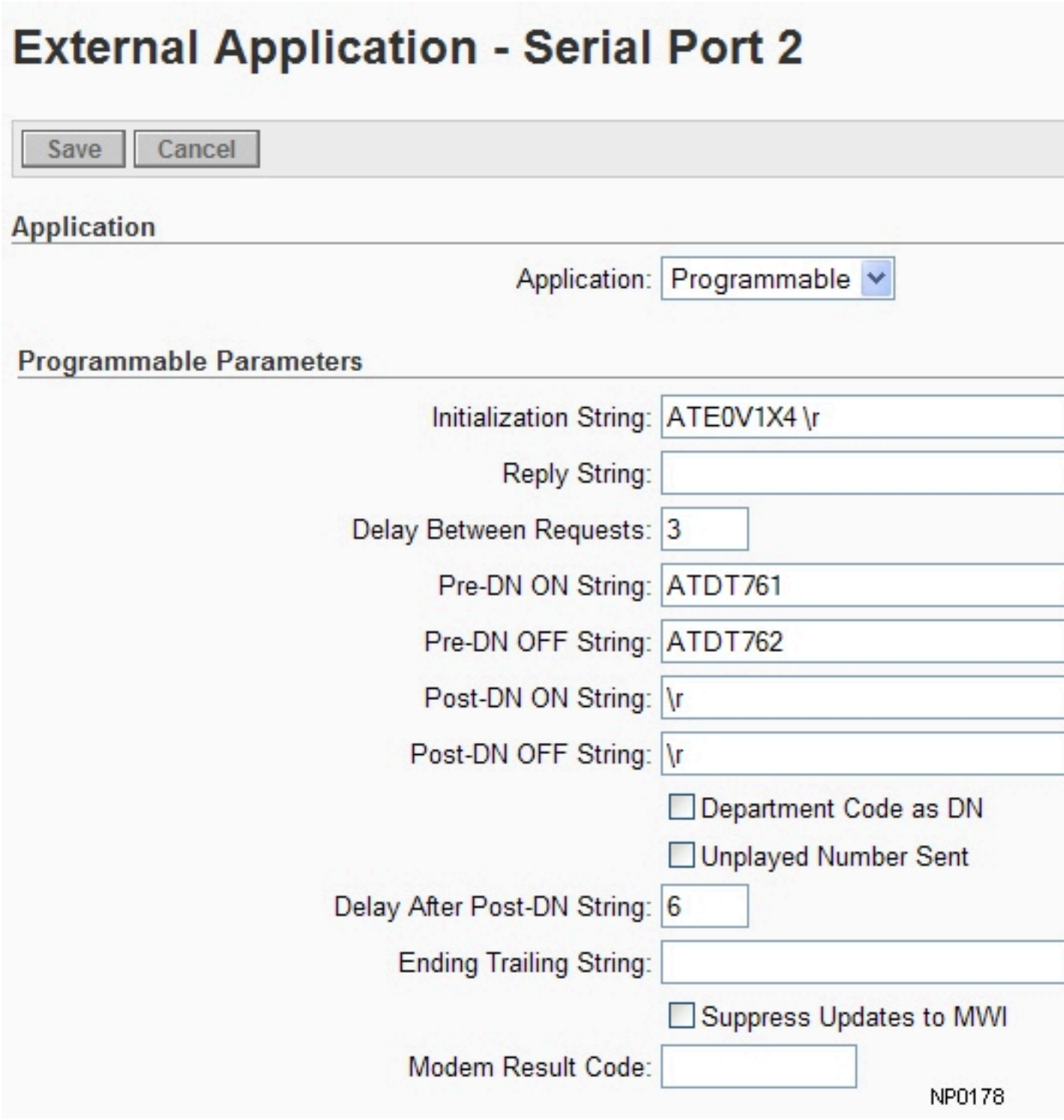
1	2	3	4	5	6	7	8
down	up	down	down	up	up	down	down

Note: The NuPoint Unified Messaging system expects to see the string 'NO CARRIER' returned by the modem after each message waiting activation. If the modem does not send this string, the NuPoint Unified Messaging system treats it as a failure and queues the message waiting task again and again (up to 18 times). The US Robotics modem with the switches set as above will meet this requirement and will work. If you do not have a modem that returns the 'NO CARRIER' result code, the message waiting application will not work.

Perform the following steps to configure the programmable RS-232 MWI using a modem:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click **External Applications**.
4. Select a free **Serial Port** and then select **Programmable** from the Applications list. Set up the parameters as shown below.

Note:
The Pre-DN ON and Pre-DN OFF strings will contain the feature access code for the SX200D/L that has been chosen as the send message. In the example below, we are using 76 as the feature access code for send message, and therefore we need to send 761 to the PABX to turn the lamp on and 762 to turn the lamp off. This number will change from system to system, depending on the feature access code chosen.



Note:
The initialization string is a back up to the switch settings mentioned above and sets the modem to no echo and verbose result codes. The \r code is a carriage return character that is sent to the modem.

1. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.
2. To complete the RS-232 message waiting application, you must now assign the correct message waiting type to the mailboxes that will be using it.

26.50.6 Define a Serial Port

Perform the following steps to define a serial port that enables the RS-232 Message Waiting Indicators Interface application and allows for RS-232 cabling:

1. Reach the NuPoint Voice Configuration Offline Menu:

   From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. If desired, duplicate the configuration by selecting **(B) Duplicate Active Configuration**.

   The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears.

   All subsequent steps in this procedure – along with any other configuration entries – affect just the copy, and take effect only after you activate the configuration.
3. Select **(M) RS232 Application Only**.
4. Specify the serial port index by selecting **(P) Serial Port Selected**.

   At the prompt **Enter a serial port index (0-2) =**, enter one of the following:

   - **1** to indicate index 1
   - **2** to indicate index 2
   - **0** to disable the port and the RS-232 Message Waiting Indicators Interface application.
5. At the prompt **Enter the serial port type, 1 for cpu, 2 for smart card:**, enter one of the following to specify the serial port type:

   - **1** to indicate that you will send signals through a CPU-based serial port (serial port 1 or serial port 2)
   - **2** to indicate a smartcard-based serial port, which allows up to 32 ports.
6. At the prompt **Enter the serial port number, 1-2:**, enter one of the following to specify the serial port type:

   - **1** to indicate CPU-based serial port 1
   - **2** to indicate CPU-based serial port 2
   - **1-32** to indicate a smartcard-based serial port.
   - a smartcard-based serial port, which allows up to 32 ports.

Note:
Do not select serial port 1 if you are using this port for your console.

7. Save the parameter settings by exiting to the Main Menu.

26.50.7 Configure Programmable RS-232 MWI

The programmable RS-232 message waiting indicators interface is configured entirely offline, through the RS-232 Only Application Menu. This procedure assumes that the appropriate server hardware and software have been installed.

Note:
Perform the following steps to configure the programmable RS-232 message waiting indicators interface in a server:

1. Complete an RS-232 Message Waiting Indicators Interface Worksheet.
2. To enable the RS-232 Message Waiting Indicators Interface application and allow for RS-232 cabling, define an RS-232 serial port. See Defining an RS-232 Serial Port.
3. Create the interface string. See Creating a Programmable RS-232 Interface String.
4. Set delay times to allow for PBX processing of RS-232 message waiting indicators requests. See Setting Delay Times for RS-232 Message Waiting Requests.
5. Enable or disable indicator-on requests for successive messages. See Enabling/Disabling Light-on Requests for Successive Messages.
6. If desired, have the number of unplayed messages sent after the directory number when the server issues a request to turn indicators on. See Sending the Number of Unplayed Messages through the Programmable RS-232 Interface.
7. Compensate for different directory number and mailbox numbers, if necessary. See Compensate for Different Directory and Mailbox Numbers.
   - Set the **Dept Code As DN** parameter in the RS-232 Programmable Menu to **Yes**.
   - Enter the directory number in the Department Code parameter of the mailbox.
8. Verify that the configuration is correct.
9. Activate the configuration.
10. Assign message waiting type 7 (programmable interface) through the first or second message waiting type prompt in mailboxes that are to receive message waiting indicator requests. See Assigning Message Waiting Indicators to a Mailbox.
11. Test the RS-232 Message Waiting Indicators Interface application.

26.50.8 Creating a Programmable RS-232 Interface String

The RS-232 programmable interface string consists of the following parts:

- Initialization string, if required by the PBX.
- Reply string, if required by the PBX.
- Any of the applicable indicator-on or indicator-off request strings (pre-DN ON, pre-DN OFF, post-DN ON, post-DN OFF, ending trailer string).

To create a string of ASCII codes for the RS-232 programmable interface:

1. *From the Main Menu, select* **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. If desired, duplicate the configuration by selecting **(B) Duplicate Active Configuration**.

   The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears.

   All subsequent steps in this procedure – along with any other configuration entries – affect just the copy, and take effect only after you activate the configuration.
3. *Select* **(M) RS232 Application Only**.
4. Select **(P) Serial Port Selected** or **(I) IP Serial Port Selected** and enter the serial port index number (1-4).
5. Select **(R) Programmable**.
6. Select **(I) Initialization String**.
7. At the **RS232 initialize string (0 - 30 chars) =** prompt, enter the ASCII **string** (0-30 characters) required by the PBX, or a period (.) to delete an existing string. To create the **string**, consult the PBX operating manual or the PBX vendor for the correct code, and use Table 1 at the end of this procedure.
8. Select **(R) Reply String**.
9. At the **RS232 reply string (0 - 30 chars) =** prompt, enter the ASCII **string** (0-30 characters) sent by the PBX, or a period (.) to delete an existing string.

   To create the **string**, consult the PBX operating manual or the PBX vendor for the correct code, and use Table 1 at the end of this procedure.
10. Select **(O) Pre-DN ON String**.
11. At the **RS232 pre-DN ON string (0 - 30 chars) =** prompt, perform the action that corresponds to the following PBX behavior:
12. If the PBX requires the string before the directory number (sometimes called extension number), create an ASCII string (0-30 characters) using the characters in Table 1.
13. If the PBX sends the string after the directory number:

    - enter a **period** (.) to delete an existing string, if necessary.
    - enter values for the Post-DN ON String and Post-DN OFF String parameters.
14. Select **(F) Pre-DN OFF String**.
15. At the **RS232 pre-DN OFF string (0 - 30 chars) =** prompt , perform the action that corresponds to the following PBX behavior:
16. If the PBX requires the string before the directory number, create an ASCII string (0-30 characters) using the characters in Table 1.
17. If the PBX sends the string after the directory number:

    - enter a **period** (.) to delete an existing string, if necessary.
    - enter values for the Post-DN ON String and Post-DN OFF String parameters.
18. Select **(P) Post-DN ON String**.
19. At the **RS232 post-DN ON string (0 - 30 chars) =** prompt , perform the action that corresponds to the following PBX behavior:
20. If the PBX requires the string before the directory number, create an ASCII string (0-30 characters) using the characters in Table 1.

21. If the PBX sends the string after the directory number:

    - enter a **period** (.) to delete an existing string, if necessary.
    - enter values for the Post-DN ON String and Post-DN OFF String parameters.

22. Select **(Q) Post-DN OFF String**.
23. At the **RS232 post-DN OFF string (0 - 30 chars) =** prompt , perform the action that corresponds to the following PBX behavior:
24. If the PBX requires the string before the directory number, create an ASCII string (0-30 characters) using the characters in Table 1.
25. If the PBX sends the string after the directory number:

    - enter a **period** (.) to delete an existing string, if necessary.
    - enter values for the Post-DN ON String and Post-DN OFF String parameters.

26. Select **(M) Ending Trailer String**.
27. At the **RS232 trailer string (0 - 30 chars) =** prompt , perform the action that corresponds to the following PBX behavior:
28. If the PBX requires this string, create an ASCII string (0-30 characters) using the characters in the table below.
29. If the PBX does not require this string, enter a **period** (.) to delete an existing string.
30. Save the parameter settings by exiting to the Main Menu.

ASCII Characters

Character	Explanation
\b	Backspace
\f	Form feed
\n	New line
\r	Carriage return
\t	Tab
\\	Backslash
\"	Double quotes
\?	Question mark

26.50.9 Setting Delay Times for Programmable RS-232 MWI

Perform the following steps to set the delay time between successive message waiting indicators requests, and to set the delay time between the post-DN OFF string and the ending trailer string:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. If necessary, duplicate the configuration by selecting **(B) Duplicate Active Configuration**.

   The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears.

   All subsequent steps in this procedure – along with any other configuration entries – will affect just the copy, and take effect only after you activate the configuration.
3. Select **(M) RS232 Application Only**.
4. Select **(K) Delay Between Request**and set the time for delays between requests. When the prompt Delay in secs (0 - 255) = appears, enter the **seconds** (0-255) that the server should delay between successive message waiting indicators requests.
5. Select **(L) Delay After Post-DN String**and set the time for delays between the post-DN OFF string and ending trailer string. When the prompt Post-DN delay in secs (0 - 255) = appears, enter the **seconds** (0-255) that the server should delay after sending the post-DN OFF string and before sending the ending trailer string.
6. Save the parameter settings by exiting to the Main Menu.
7. You must activate the inactive configuration for the changes to take effect.

26.50.10 Enabling/Disabling Light-on Requests for Successive Messages

Perform the following steps to turn on or turn off message waiting light-on requests for successive messages:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. If desired, duplicate the configuration by selecting **(B) Duplicate Active Configuration**.

   The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears.

   All subsequent steps in this procedure – along with any other configuration entries – affect just the copy, and take effect only after you activate the configuration.
3. Select **(M) RS232 Application Only.**
4. Enable or disable updates to message waiting lights by selecting (S) Suppress Updates to MWL.

   When the prompt Suppress updates of MWL (y/n) = [] ? appears, enter

   - **Y** to suppress updates of Message Waiting Lights
   - **N** to permit updates as normal.

Enabling this feature stops updates after a user accesses the mailbox without a message waiting lights status change.

1. Save the parameter settings by exiting to the Main Menu.
2. You must activate the inactive configuration for the changes to take effect.

26.50.11 Sending the Number of Unplayed Messages

1. Perform the following steps to configure the server to send the number of unplayed messages through the RS-232 interface after the directory number in a message light-on request:
2. Reach the NuPoint Voice Configuration Offline Menu:

   From the Main Menu, select (S) System Maintenance, (R) Reconfiguration, (R) Reconfigure System, and then (G) Offline Menu.
3. If desired, duplicate the configuration by selecting (B) Duplicate Active Configuration.

   The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears.

   All subsequent steps in this procedure – along with any other configuration entries – affect just the copy, and take effect only after you activate the configuration.
4. Go to the RS-232 Programmable Menu.

   From the Main Menu, select (S) System Maintenance, (R) Reconfiguration, (R) Reconfigure System,(G) Offline Menu, and then (M)RS232 Application Only.
5. Request that the number of unplayed messages be sent by selecting (U) Unplayed Number Sent?

   When the prompt Enter "Y" to send # of unplayed messages after DN = appears, enter

   - **Y** to send the number of unplayed messages
   - **N** to not send this information
6. Save the parameter settings by exiting to the Main Menu.

26.50.12 Assigning Additional Serial Ports for Programmable RS-232 Interface

This procedure describes how to assign additional serial ports for the RS-232 Message Waiting Indicators Application. This procedure assumes:

- You have defined one serial port for the application, and it is using index 1(see Defining a RS-232 Serial Port).
- You have configured the programmable RS-232 interface (see Configure Programmable RS-232 Interface).
- You have a serial interface card installed in your server.

The additional serial ports automatically copy their settings from the serial port assigned to index 1. Changes made to that serial port will also be applied to these serial ports.

Perform the following steps to assign additional serial ports:

1. Reach the NuPoint Voice Configuration Main Menu, then go to the NuPoint Voice Configuration Offline Menu: *From the Main Menu, select* **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. If desired, duplicate the configuration by selecting **(B) Duplicate Active Configuration**. The server copies the current (active) configuration. When copying is completed, the short form of the Offline Menu appears.
3. Select **(M) RS232 Application Only**.
4. Verify that the Serial Port Selected (at the top of the menu) is the one you want to use for the RS-232 Programmable Interface Application. Select a different port if it is not correct.
5. Navigate to the RS-232 Programmable $CTI Serial Port Menu by selecting **(M) Multiple Programmable**.
6. Assign additional serial ports for RS-232 message waiting by selecting **(A) Add Serial Port .**

   When the prompt **Serial ports to add =** appears, enter the **number** (1-32) of the serial port on the card that you want to assign to the RS-232 Programmable interface.

   You can enter multiple port numbers by separating them with commas (1,3,5).
7. If necessary, delete serial ports from this function by selecting **(D) Delete Serial Port**.

   When the prompt **Serial ports to delete =** appears, enter the **number** (1-32) of the serial port on the card that you want to remove from the RS-232 Programmable interface.

   You can enter multiple port numbers by separating them with commas (1,3,5)..
8. View the assigned serial ports by selecting **(S) Show Serial Port Table**.

   When the prompt **$CTI PORTS = [1,2,3]** appears, enter the **number** (1-32) of the serial port you want to view.
9. Save the parameter settings by exiting to the Main Menu.
10. You must activate the inactive configuration for the changes to take effect.

26.50.13 Testing the RS-232 MWI Configuration

Use the Lights Test described in the DTMF-to-PBX section to test RS-232 configuration. The modem will go off hook and dial the message waiting code to light the MWI lamp on the telephone set.

26.51 Worksheets Index

- NuPoint Voice Worksheet
- Mailbox Individual Worksheet
- Mailbox Group Worksheet
- FCOS Worksheet

- GCOS Worksheet
- LCOS Worksheet
- RCOS Worksheet
- Billing Worksheet (1 of 2)
- Billing Worksheet (2 of 2)
- Outdial Line Group Worksheet
- Rotational Mailbox Worksheet
- Tree Mailbox Worksheet
- DTMF-to-PBX MWI Worksheet
- RS-232 MWI Worksheet

- Sample Worksheets

26.51.1 NuPoint Voice Worksheet

VoiceMemo Worksheet

Offline Parameters

Define Line Groups

Current group

Add lines to current group

Name of current group

Drop lines fr current group

Line Group Only Applications

Group selected

Select application

Online Parameters

VoiceMemo Configuration Online Menu

Group selected

Day/Night

Start time of workday AM PM

End time of workday AM PM

Dialing Plan Menu

Dialing plan

1 2 3 4 5 6 7 8

Optional Star * Prefix Dialing Plan

*Networking with prefix dplan digit

*Networking with prefix dplan length

*Dial by nam

* Networking without prefix dplan digit

*Networking without prefix dplan length

*Call placem delivery dpl

Dial String and Mailbox Menu

System attendant's extension

Attendant's transfe string or PBX predirectory #

Aministrator's mailbox #

Attendant's mailbox

E-mail transfer string

General greeting mailbox #

Pre-company name dial string

Pre-maibox greeting dial string

VoiceMemo Configuration-Online Menu

Key *0* for attendant transfer during greeting? yes no

Prompts "Enter mailbox # or wait"? yes no

Allow multiple m s for outside caller?

26.51.2 Mailbox Worksheets

Before configuring a standard mailbox, complete the Mailbox Individual Worksheet. Each worksheet entry is explained in the following sections. If you want to use a default value, indicate that fact on the worksheet. Then you will not need to select or enter any information for that parameter during re-configuration. See a sample Mailbox Individual Worksheet.

To configure a mailbox for paging, message delivery, or call placement, see also the Mailbox topics in the Pager Application section.

Department codes are required for some message waiting applications. In addition, the billing report includes the department code to allow billing by department. If the mailbox uses a department code, the software supports up to 2000 department codes.

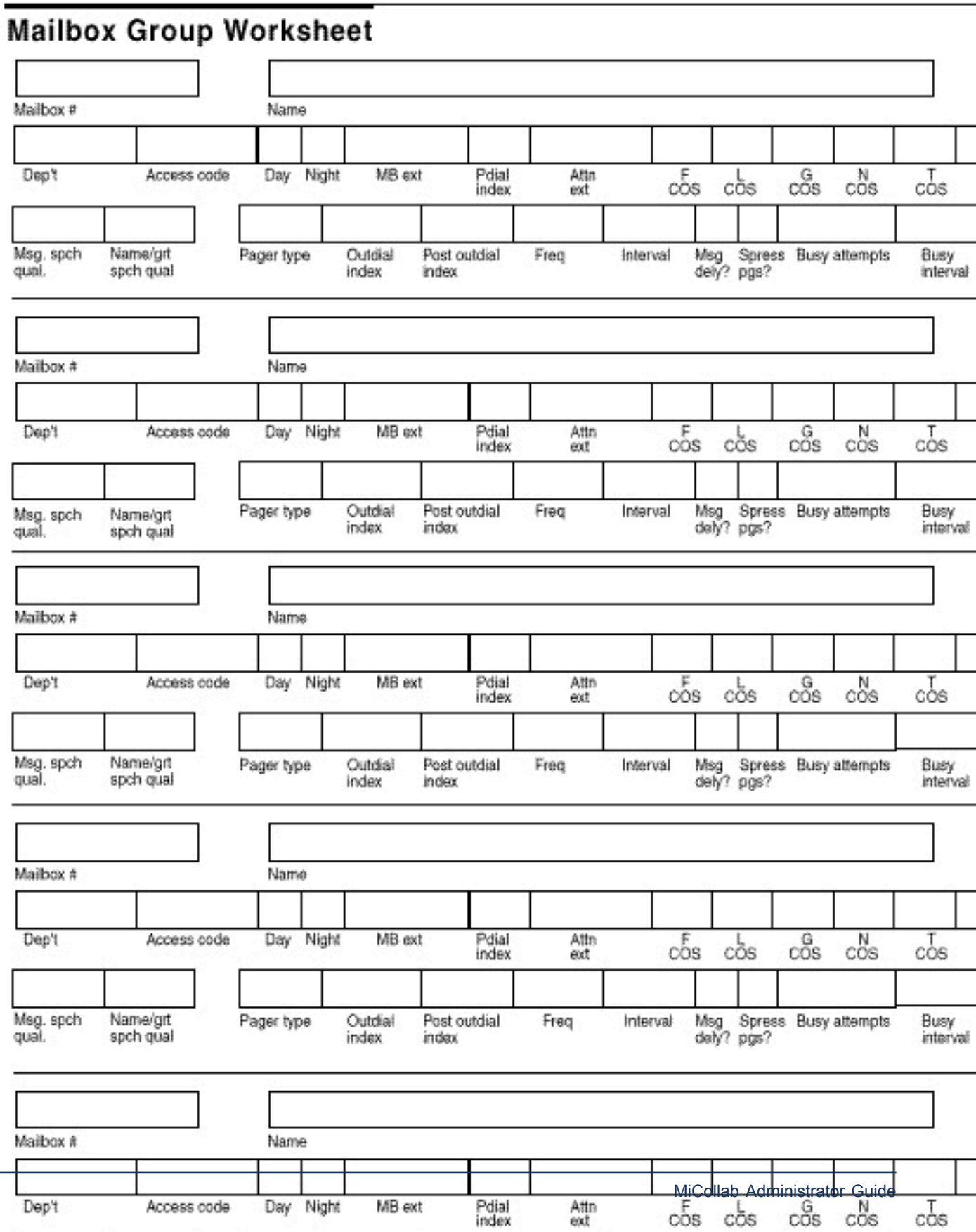
When you need to organize information for large groups of mailboxes, you can use a mailbox group worksheet. This worksheet allows you to enter configuration values for several mailboxes on a single sheet. Use it in conjunction with the Mailbox Individual Worksheet when appropriate. A blank Mailbox Group Worksheet is located in this manual.

26.51.3 Mailbox Individual Worksheet

Mailbox Individual Worksheet

Mailbox Type	**Standard** ☐		**Tree** ☐ (also complete Tree Mailbox Worksheet)		**Rotational** ☐ (also complete R Maibox Workshe
Create New Mailboxes	Mailbox to create				Name
	Department code				Access code
	Receptionist day treatment				Receptionist nigh treatment
	Mailbox's extension number				Mailbox's extension pre-dia index
	Attendant extension number				Attendant extension pre-dia index
	Features Class of Service ☐		Limits Class of Service ☐		Group Class of Service
	Tenant Class of Service ☐		Restriction Class of Service ☐		Temporary passcode
	Message waiting type #1 ☐		Message waiting type #2 ☐		Message waiting type #3
	Call placement pager access type ☐		Turn off pager/outcall notification?	☐ yes ☐ no	
	Lists with change rights				Lists with review rights
	Message speech quality ☐		Name/greeting speech quality ☐		
For outdial billing only	Internal outdial index ☐		Billed outdial index ☐		Unbilled outdial index
	Billing number				dialing

26.51.4 Mailbox Group Worksheet



Mailbox Group Worksheet

Mailbox # | Name

Dep't | Access code | Day | Night | MB ext | Pdial index | Attn ext | F COS | L COS | G COS | N COS | T COS

Msg. spch qual. | Name/grt spch qual | Pager type | Outdial index | Post outdial index | Freq | Interval | Msg dely? | Spress pgs? | Busy attempts | Busy interval

Mailbox # | Name

Dep't | Access code | Day | Night | MB ext | Pdial index | Attn ext | F COS | L COS | G COS | N COS | T COS

Msg. spch qual. | Name/grt spch qual | Pager type | Outdial index | Post outdial index | Freq | Interval | Msg dely? | Spress pgs? | Busy attempts | Busy interval

Mailbox # | Name

Dep't | Access code | Day | Night | MB ext | Pdial index | Attn ext | F COS | L COS | G COS | N COS | T COS

Msg. spch qual. | Name/grt spch qual | Pager type | Outdial index | Post outdial index | Freq | Interval | Msg dely? | Spress pgs? | Busy attempts | Busy interval

Mailbox # | Name

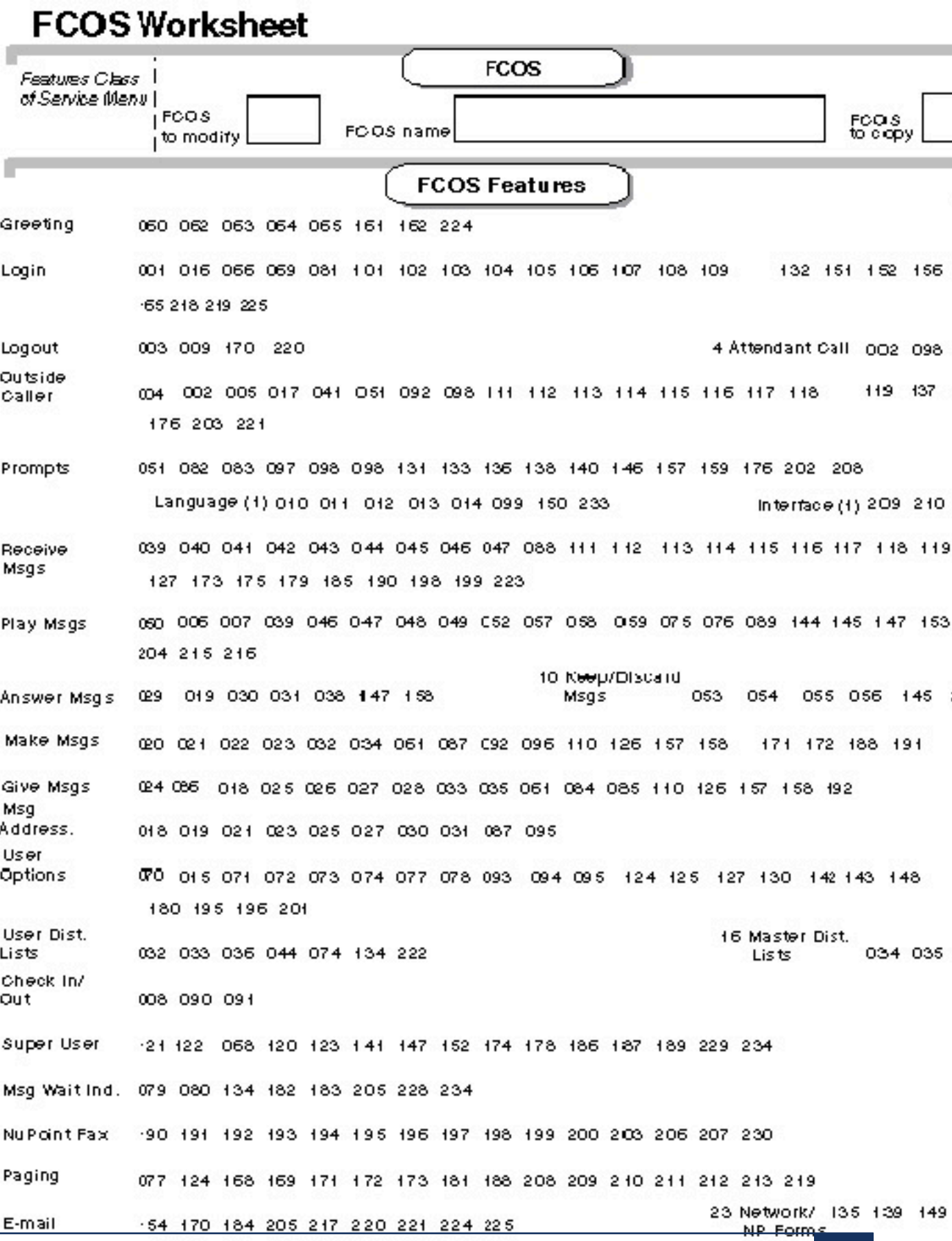
Dep't | Access code | Day | Night | MB ext | Pdial index | Attn ext | F COS | L COS | G COS | N COS | T COS

Msg. spch qual. | Name/grt spch qual | Pager type | Outdial index | Post outdial index | Freq | Interval | Msg dely? | Spress pgs? | Busy attempts | Busy interval

Mailbox # | Name

Dep't | Access code | Day | Night | MB ext | Pdial index | Attn ext | F COS | L COS | G COS | N COS | T COS

26.51.5 FCOS Worksheet



FCOS Worksheet

Features Class of Service Menu

FCOS

FCOS to modify

FCOS name

FCOS to copy

FCOS Features

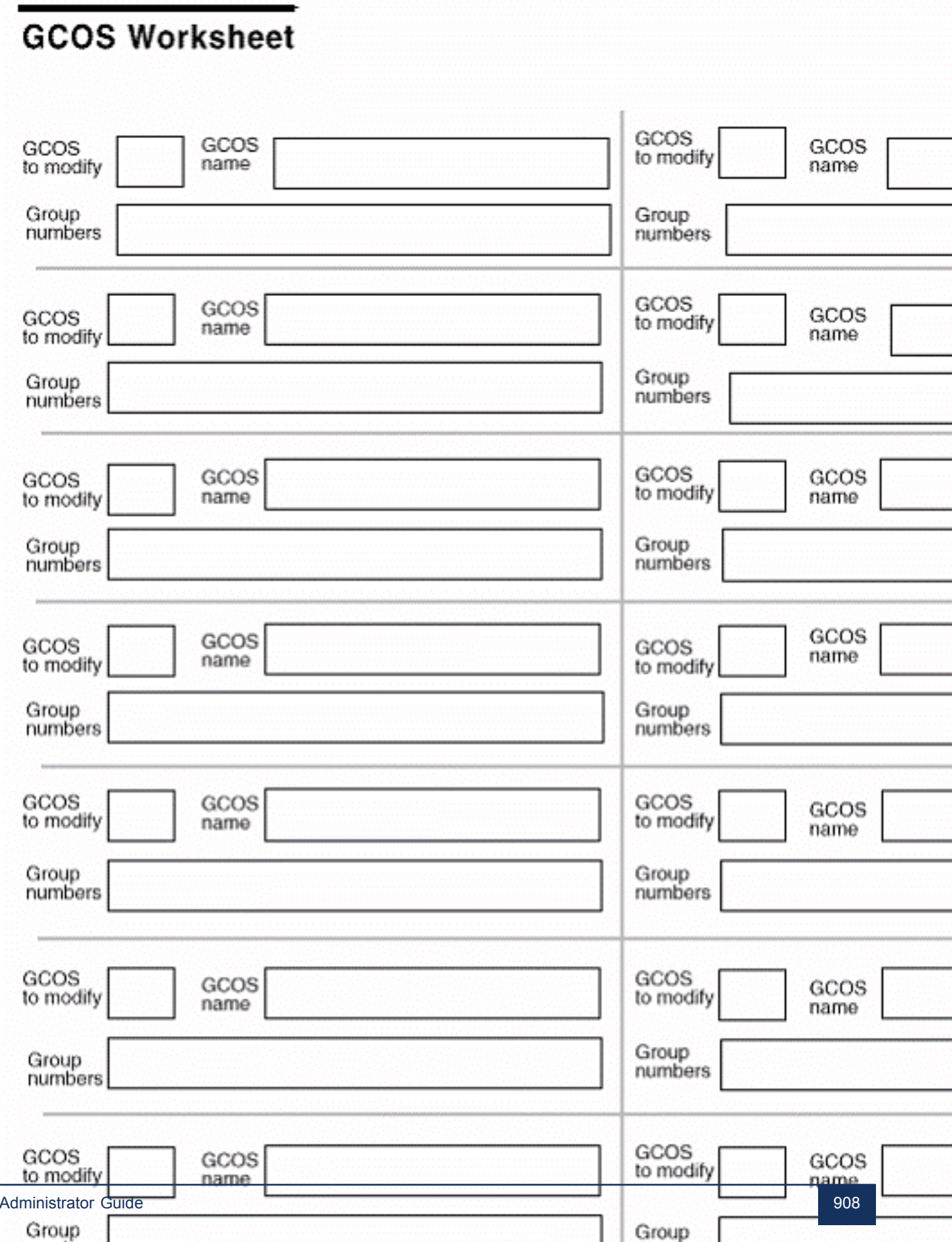
1 Greeting	060 062 063 064 065 161 162 224
2 Login	001 016 066 069 081 101 102 103 104 105 106 107 108 109 132 151 152 156 165 218 219 225
3 Logout	003 009 170 220
4 Attendant Call	002 098
5 Outside Caller	004 002 005 017 041 051 092 098 111 112 113 114 115 116 117 118 119 137 176 203 221
6 Prompts	051 082 083 097 098 098 131 133 136 138 140 146 157 159 176 202 208 Language (1) 010 011 012 013 014 099 150 233 Interface (1) 209 210
7 Receive Msgs	039 040 041 042 043 044 045 046 047 088 111 112 113 114 115 116 117 118 119 127 173 175 179 185 190 198 199 223
8 Play Msgs	060 006 007 039 046 047 048 049 052 057 058 059 075 076 089 144 145 147 153 204 215 216
9 Answer Msgs	029 019 030 031 038 147 158
10 Keep/Discard Msgs	053 054 055 056 145
11 Make Msgs	020 021 022 023 032 034 061 087 092 096 110 126 157 158 171 172 188 191
12 Give Msgs	024 086 018 025 026 027 028 033 035 061 084 085 110 126 157 158 192
13 Msg Address.	018 019 021 023 025 027 030 031 087 095
14 User Options	070 015 071 072 073 074 077 078 093 094 095 124 125 127 130 142 143 148 180 195 196 201
15 User Dist. Lists	032 033 036 044 074 134 222
16 Master Dist. Lists	034 035
17 Check In/ Out	008 090 091
18 Super User	021 122 068 120 123 141 147 152 174 178 186 187 189 229 234
19 Msg Wait Ind.	079 080 134 182 183 205 228 234
20 NuPoint Fax	090 191 192 193 194 195 196 197 198 199 200 203 206 207 230
21 Paging	077 124 168 169 171 172 173 181 188 208 209 210 211 212 213 219
22 E-mail	054 170 184 205 217 220 221 224 225
23 Network/ NP Forms	135 139 149

26.51.6 LCOS Worksheet

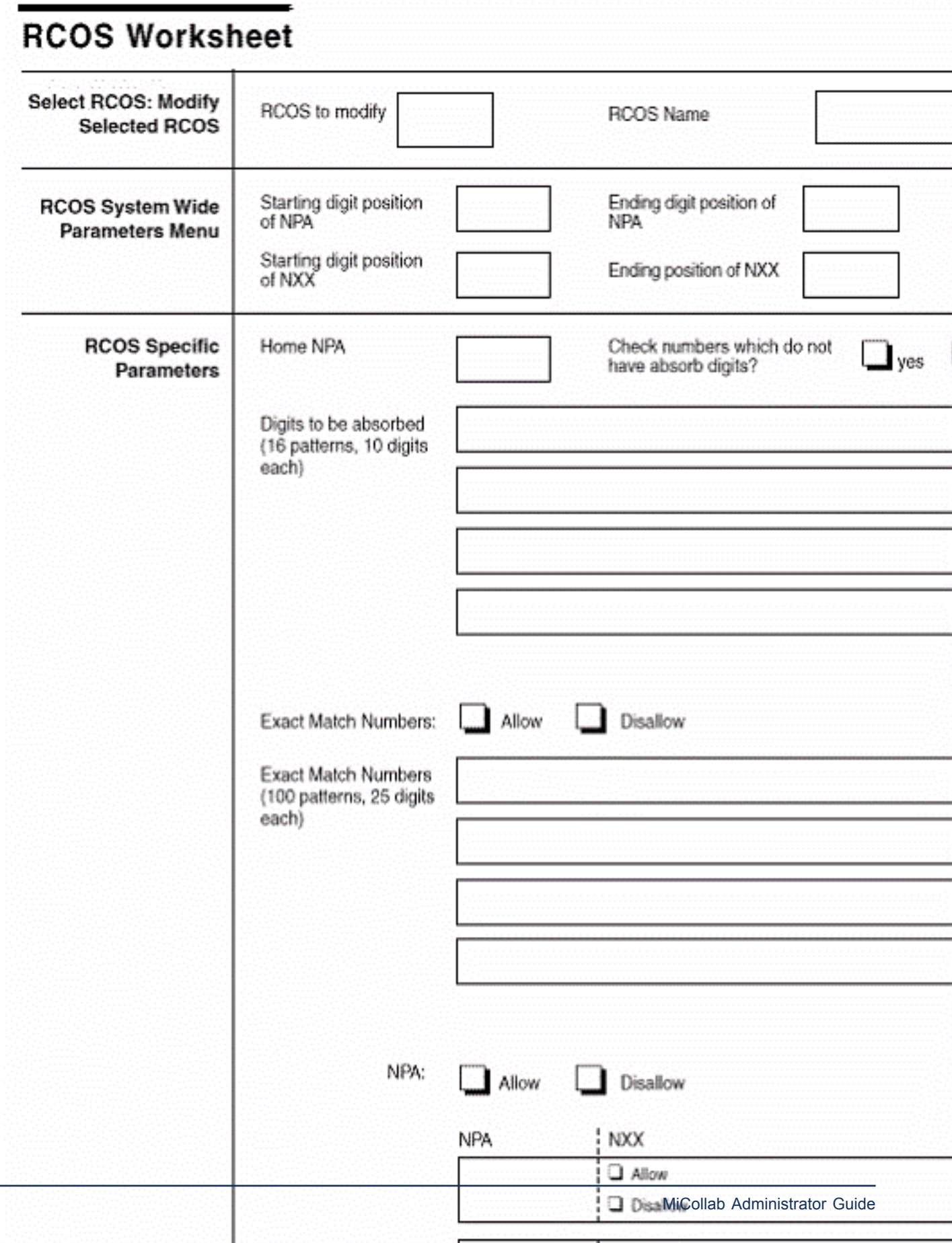
LCOS Worksheet

Limits Class of Service Menu	Limits COS		Name selected LCOS	
Limits Parameter Menu	Greeting length		User message length	
	User name length		Caller message length	
	Message count		Maximum login time	
	Messages per billing		Network queue message count	
More Limits Parameters Menu	Auto wakeup - phone length		Maximum days -future delivery	
	Paging - phone length		Maximum family member or guest	
	Message delivery - phone length		Message waiting indicator - msg. length	
	Future delivery - message count		Minimum message length	
Even More Limits Parameter Menu	Maximum days - auto wakeup		Maximum destinations per reminder call	
	Maximum days - reminder call		Maximum members per distribution list	
	Maximum reminder calls per billing		Maximum recipients count	
Call Placement Menu	RNA retry limit		Busy retry interval	
	RNA retry interval		Message phone length	

26.51.7 GCOS Worksheet



26.51.8 RCOS Worksheet



RCOS Worksheet

Select RCOS: Modify Selected RCOS

RCOS to modify

RCOS Name

RCOS System Wide Parameters Menu

Starting digit position of NPA

Ending digit position of NPA

Starting digit position of NXX

Ending position of NXX

RCOS Specific Parameters

Home NPA

Check numbers which do not have absorb digits? ❑ yes

Digits to be absorbed (16 patterns, 10 digits each)

Exact Match Numbers: ❑ Allow ❑ Disallow

Exact Match Numbers (100 patterns, 25 digits each)

NPA: ❑ Allow ❑ Disallow

NPA | NXX

❑ Allow

❑ Disallow

26.51.9 Billing Worksheet (1 of 2)

Billing Worksheet, Page 1 of 2

	RATE		
Messages Received	**Low Usage**	**Boundary**	**H**
Messages received from users			
Messages received from callers			
Messages future deliveries			
Call placement per minute rate (Connect Time)			
Call placement per call rate			
Urgent messages received from callers			
Auto wakeups or TAS messages			
Receipt requests			
Disk usage (Disk Usage)			
Network Billing			
Network messages sent			
Network urgent messages sent			
Network messages received			
Network urgent messages received			
Number of network nodes sent to			
Number of network nodes sent urgent			
Number of remote network recipients			
Number of remote network recipients urgent			
Message length network sent			
Message length urgent network sent			
Message length network received			
Message length urgent network received			
Message length, number of nodes sent			
Msg. length, number of nodes sent urgent			
Message length, number of remote recipients			
Message length, number of remote recipients urgent			
Messages Received (fax)			
Number of fax messages received			

26.51.10 Billing Worksheet (2 of 2)

Billing Worksheet, Page 2 of 2

Mailbox Accesses

Connect Time

	Greeting Rate			Login Rate			User Connect Time			
Line Group	Low	Bound	High	Low	Bound	High	Low	Bound	High	Low
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

Pager Billing

Pager No.	Low	Bound	High	Pager No.	Low	Bound	High
0				8			
1				9			
2				10			
3				11			
4				12			
5				13			
6				14			
7				15			

Base Rates

FCOS	Rate	FCOS	Rate	FCOS	Rate	FCOS	Rate
1		17		33		49	
2		18		34		50	
3		19		35		51	

26.51.11 Outdial Line Group Worksheet

Outdial Line Group Worksheet

Pager Systems Index Plan

Pager System	Pager Name	Access Code	Hold Time
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Offline Parameters

Define Line Groups

Current group

Add lines to current group

Name of current group

Line Group Only Applications

Group selected

Select application

Online Parameters

VoiceMemo Configuration Online Menu

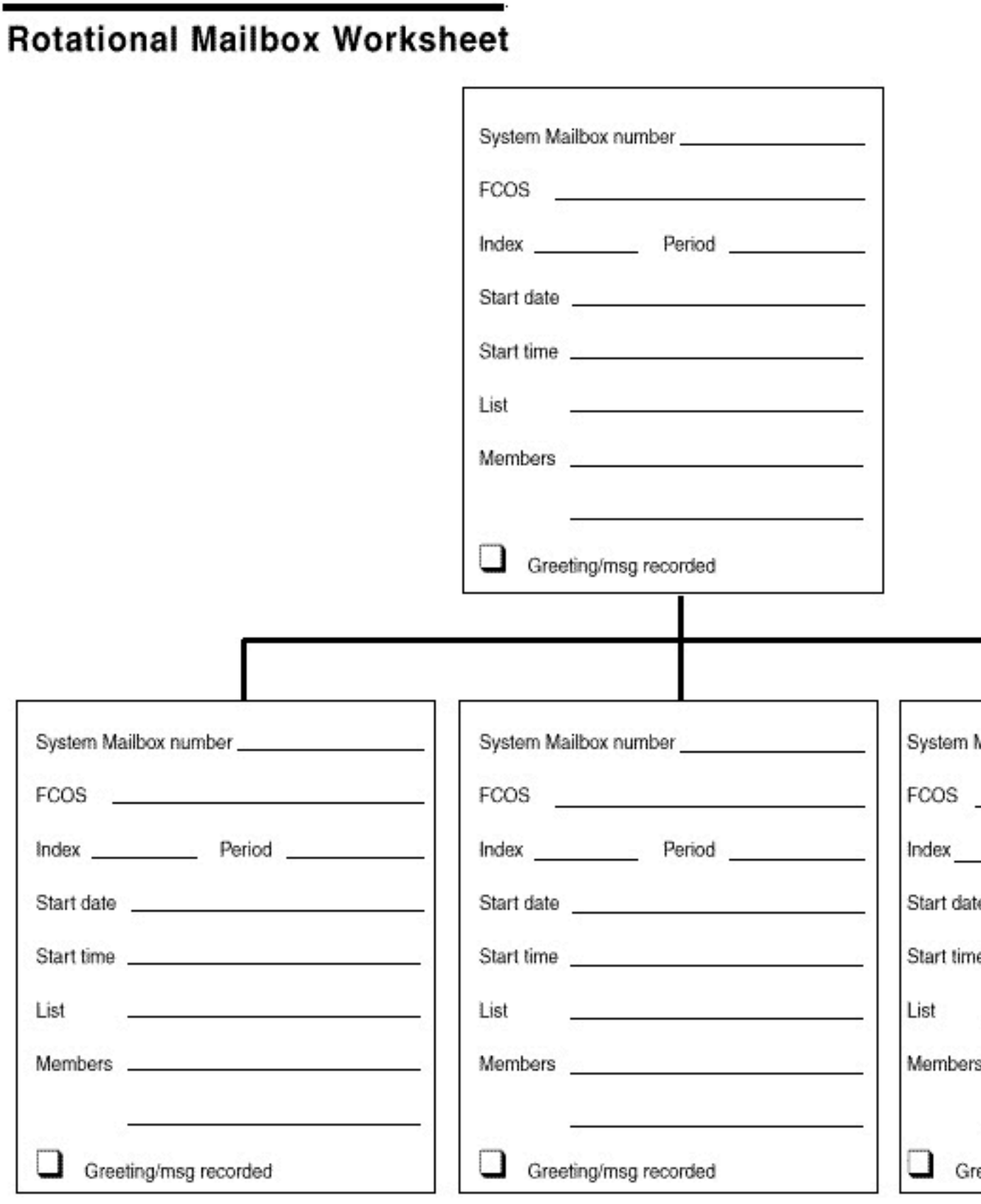
Group selected

Pagers

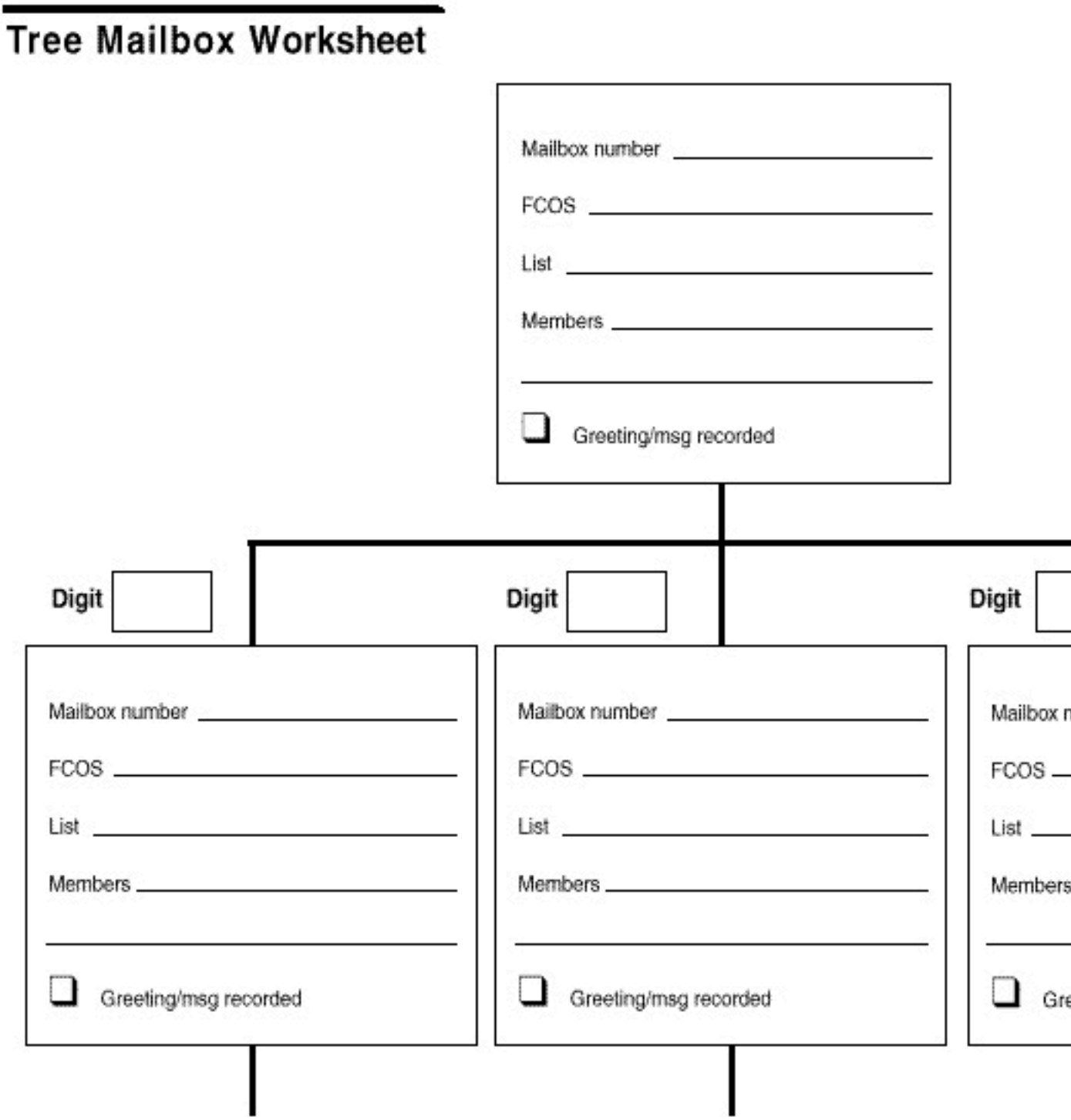
Pager systems supported (from Pager Systems Index Plan, above)

NP00

26.51.12 Rotational Mailbox Worksheet



26.51.13 Tree Mailbox Worksheet



26.51.14 DTMF-to-PBX Worksheet

DTMF-to-PBX Message Lights Worksheet

Offline Parameters

Define line groups

Current group

Add lines to current group

Name of current group

DTMF Applications

Group selected

Select application

Online Parameters

DTMF to PBX

Initial dial tone detect? ☐ yes ☐ no

PBX special access code

Dial tone confirmation? ☐ yes ☐ no

Pre-DN ON dial string

Pre-DN OFF dial string

Suppress updates to MWL? ☐ yes ☐ no

Pre-DN ON dial string

Pre-DN OFF dial string

Wait for dial tone? ☐ yes ☐ no

NP01

Enable alternate code? ☐ yes ☐ no

26.51.15 RS-232 Message Waiting Lights Worksheet

RS-232 Message Waiting Indicators Interface Worksheet

RS-232 Only Applications

Serial Port Selected

Serial port index ☐ Serial port type ☐ Serial port number ☐

Select Application

- ☐ AC Message Waiting Lights (BSR)
- ☐ BBL Pager
- ☐ Centigram Standard Interface
- ☐ Hyatt Encore PMS Integration
- ☐ PMS Integration
- ☐ HIS PMS Integration
- ☐ Hitachi PMS Integration
- ☐ Hitachi DX
- ☐ Programmable
- ☐ SL-1 Background Terminal Facility
- ☐ SL-1 Multiple Message Waiting Se
- ☐ Tip & Ring Message Waiting Lamp
- ☐ Video Dispatch
- ☐ Citywide SMDI
- ☐ Fujitsu 960

AC Message Waiting Lights

- ☐ AC Controller I
- ☐ AC Controller II

Programmable

Initialize string ☐ RS- 232 reply string ☐

Delay between requests ☐

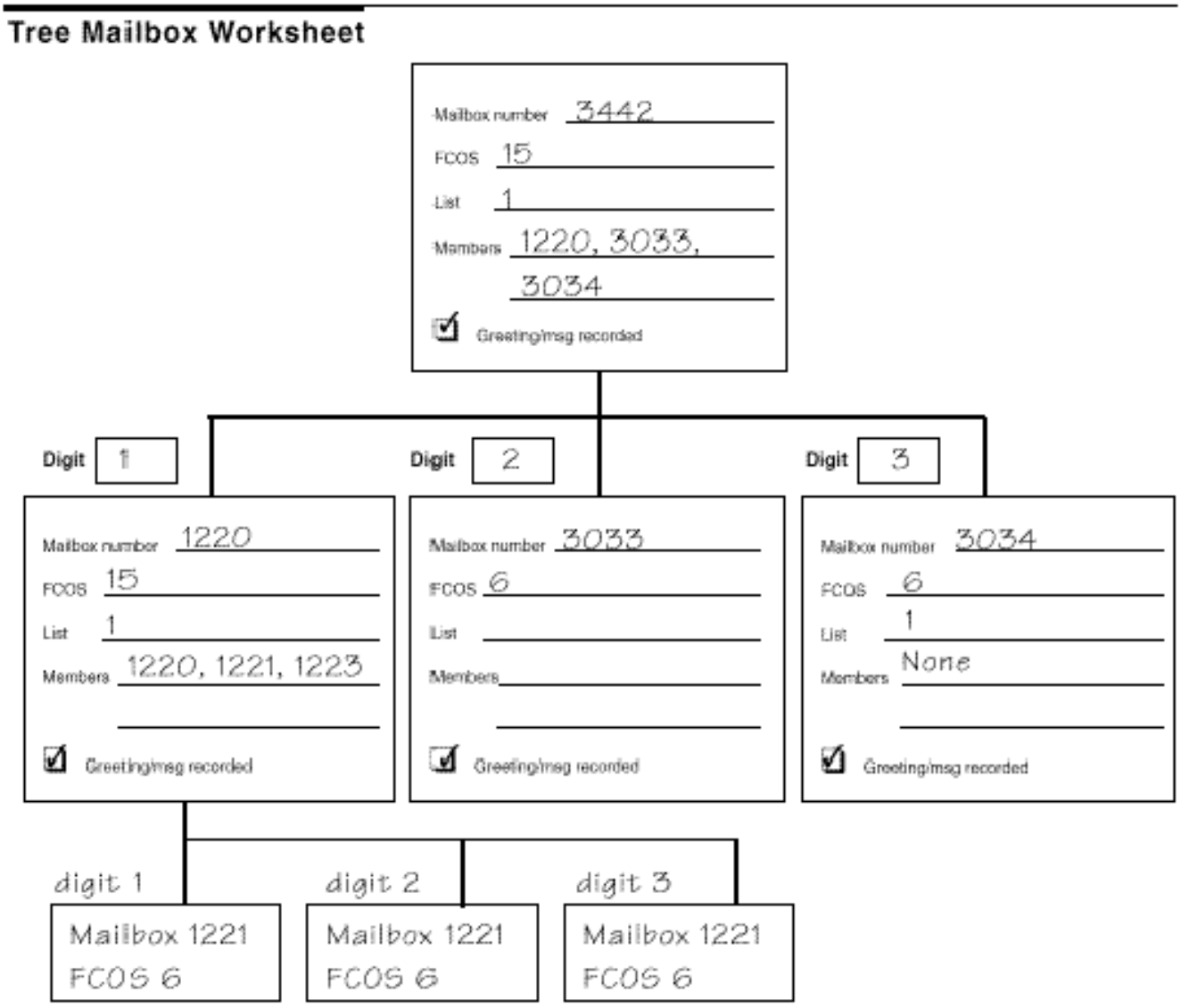
Pre-DN ON string ☐ Pre-DN OFF string ☐

Post DN-ON string ☐ Post-DN OFF string ☐

Department code ☐ yes ☐ no Unplayed number ☐

26.51.16 Mailbox Worksheet Examples

Sample Mailbox Individual Worksheet



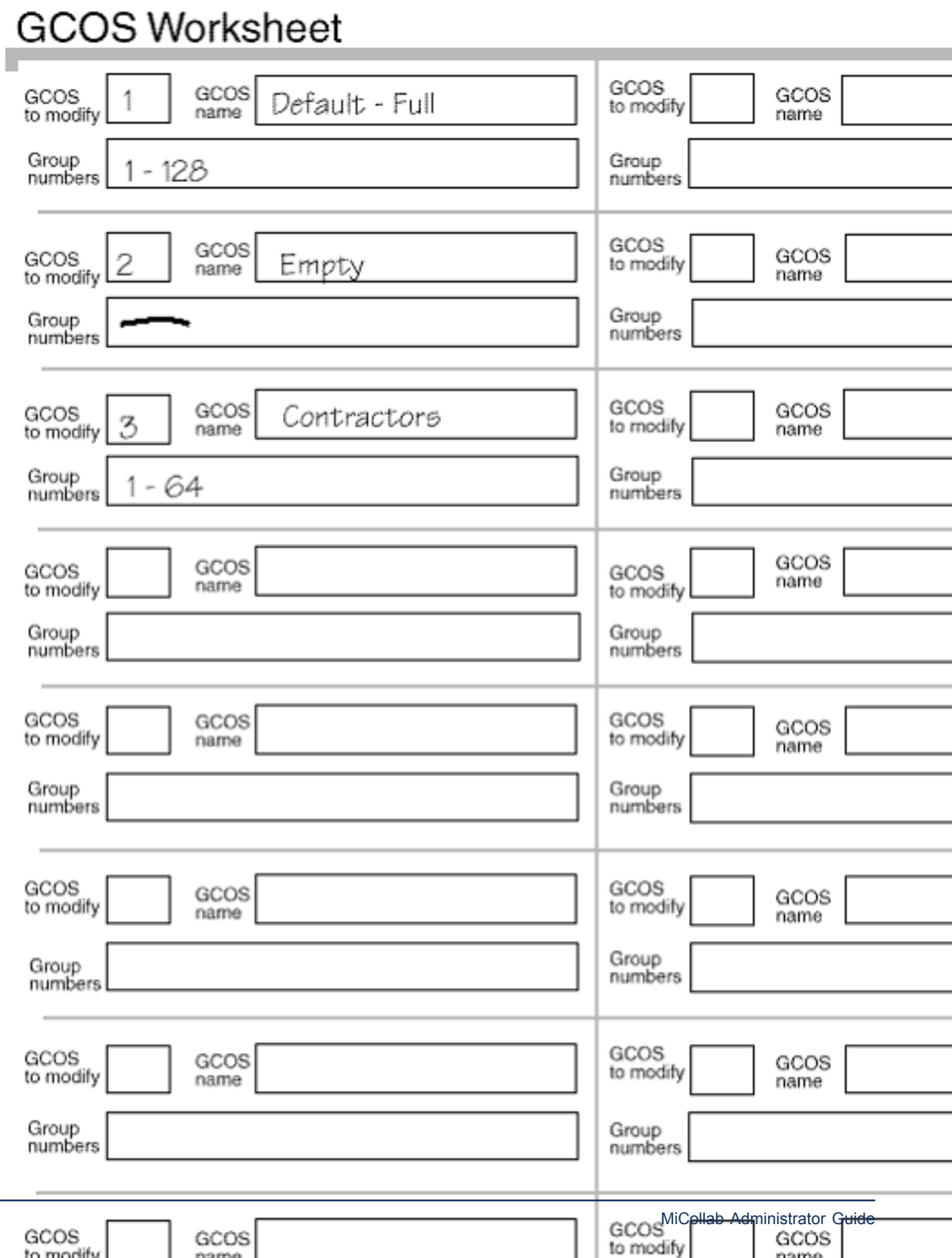
Mailbox Group Worksheet

26.51.17 Sample LCOS Worksheet

LCOS Worksheet

Limits Class of Service Menu					
	Limits COS	4	Name selected LCOS	Contractors only	
Limits Parameter Menu	Greeting length	1	User message length	ok	Maximum atta per message
	User name length	ok	Caller message length	ok	Maximum atta per network m
	Message count	50	Maximum login time	50	
	Messages per billing	200	Network queue message count	ok	
More Limits Parameters Menu	Auto wakeup - phone length	ok	Maximum days -future delivery	ok	Maximum pag billing cycle
	Paging - phone length	ok	Maximum family member or guest	3	Maximum wak billing
	Message delivery - phone length	ok	Message waiting indicator - msg. length	0	
	Future delivery - message count	50	Minimum message length	0	
Even More Limits Parameter Menu	Maximum days - auto wakeup	365	Maximum destinations per reminder call	ok	Maximum num distribution list
	Maximum days - reminder call	365	Maximum members per distribution list	ok	Minimum numb recipients for r summary
	Maximum reminder calls per billing	100	Maximum recipients count	ok	Minimum billed length
Call Placement Menu	RNA retry limit	ok	Busy retry interval	ok	Maximum mes length
	RNA retry interval	ok	Message phone length	ok	
	Busy retry limit	ok	Message count	50	
FaxMemo Limits Menu	Maximum number of digits for telephone number	NA	CNG tone detection length	NA	Fax delivery re interval
	FaxMemo message count	NA	Fax delivery retry frequency	NA	
Message Retention	Cut-through paging	0	Urgent message	172	Fax receipt rete

26.51.18 Sample GCOS Worksheet



GCOS Worksheet

GCOS to modify	GCOS name	Group numbers
1	Default - Full	1 - 128
2	Empty	
3	Contractors	1 - 64

26.51.19 Sample RCOS Worksheet

RCOS Worksheet

Select RCOS: Modify Selected RCOS

RCOS to modify: 2

RCOS Name: Westregion

RCOS System Wide Parameters Menu

Starting digit position of NPA: 10

Ending digit position of NPA: 8

Starting digit position of NXX: 7

Ending position of NXX: 5

RCOS Specific Parameters

Home NPA: 408

Check numbers which do not have absorb digits? ☑ yes ☐ no

Digits to be absorbed (16 patterns, 10 digits each):

- 9
- 1
- 91
-

Exact Match Numbers: ☐ Allow ☑ Disallow

Exact Match Numbers (100 patterns, 25 digits each):

- 5551212, 411, 0
-
-
-

NPA: ☑ Allow ☐ Disallow

NPA	NXX
408	☐ Allow ☑ Dis-allow 662, 684, 728
415	☐ Allow ☑ Dis-allow 493
510	☐ Allow ☑ Dis-allow 424
	☐ Allow

26.52 Overview

The system administrator creates and maintains software files for all mailboxes on the system (the server). You perform the following functions:

- Creating and modifying mailboxes
- Deleting and reassigning mailboxes
- Performing routine maintenance of software files
- Changing the system time and date
- Establishing system security

Additional administrative responsibilities may include the following activities:

- Billing clients
- Running reports
- Building classes of service
- Establishing programming for pagers
- Setting up system-wide distribution lists
- Creating messages, greetings, and tutorials

This online help system contains instructions for performing these functions.

Most administration is performed using either the Web console or the Text console, but some administration tasks can also be performed using the telephone.

26.52.1 System Maintenance - Overview

System maintenance for NuPoint UM is performed automatically. This section describes utilities you can use to perform optional maintenance procedures:

- Verify
- Passcode Maintenance
- Alarm Management
- Message Purge
- Backup
- System Shutdown
- Fax Download Settings

26.52.2 Passcode Maintenance

You can perform the following passcode maintenance:

- Set up temporary mailbox passcodes for new mailbox owners so they can access their mailboxes.
- Enforce a passcode change so users are prompted to change the password at their first login.

- Configure an expiry period for mailbox passcodes so that users are prompted to change passcodes periodically.

26.52.3 Alarm Manager

The alarm management system monitors system devices and applications and provides alarm notification and management abilities. Administrators can configure alarm management to send alarm messages ("traps") to an SNMP agent, or to send alarms as email messages to one or more selected email accounts. You can choose to receive each individual alarm as one message, or to receive all alarms of one type as one message. The second choice is more effective when multiple alarms are caused by a single error.

Administrators of systems that do not have an SNMP management system can use the Web Console for alarm management. Alarms can be acknowledged and/or deleted. Acknowledged alarms do not appear in the active alarm list.

The log-in page of the Web Console displays alarm status and a link to the Alarm Management page.

Alarm Messages

The alarm management system supports the following NuPoint alarm messages:

Alarm Type ID	Default Severity	Alarm Class	Type Name	Prescription	Cause of Alarm
1001	Minor	PORT	RNA		The port is experiencing a ring-no-answer condition.
2001	Warning	LICENSE	MBOX		Not in use.
2002	Informational	LICENSE	No more WebView licenses	Upgrade the WebView license of your system.	Not in use.
2003	Minor	LICENSE	Speech AA corporate list license exceeded	Upgrade the Speech AA license of your system.	The maximum number of Speech Auto Attendant users has been exceeded.

Alarm Type ID	Default Severity	Alarm Class	Type Name	Prescription	Cause of Alarm
3001	Warning	ERROR	Gather schedule	Re-activate NuPoint system to re-enable gathering.	The system is experiencing a problem gathering billing data, so the service has been suspended. To fix the problem, check that the gathering schedule is valid and make corrections if necessary. .
3002	Informational	ERROR	Speech AA rejected entries	Make sure all entries have a first and last name, as well as a phone number.	Entries for the Speech Auto Attendant have been rejected due to invalid data.
3003	Major	ERROR	Speech AA data source error	Make sure the Speech Auto-Attendant Data Source is configured properly.	Entries for the Speech Auto Attendant have been rejected because the data source is improperly configured.
4001	Warning	SECURITY	Failed login	Track the source IP address to determine where the requests come from.	The system has rejected a login attempt to the Web Console interface.

Alarm Type ID	Default Severity	Alarm Class	Type Name	Prescription	Cause of Alarm
4002	Informational	SECURITY	Failed WebView login	Track the source IP address to determine where the requests come from.	The system has rejected a login attempt to the Web View interface.
5001	Major	NODE	Failover		A failover has occurred from one NuPoint 640 server to another.
5002	Critical	NODE	Critical process		A critical process has crashed.
5003	Warning	NODE	Restore warning or error	Check log files for details.	A warning or error has occurred during the restore process.
5008	Informational	NODE	Socket for UMPro services either failed, disconnected, or is timed out.	Automatic retry by the system to reconnect.	The system has experienced a problem with the socket used for creating a session with the Mail servers; and reading and writing of data using these sockets.

Alarm Type ID	Default Severity	Alarm Class	Type Name	Prescription	Cause of Alarm
6001	Warning	NETWORK	Cannot connect to mail server	Make sure that the mail server is reachable from the NuPoint system.	The system cannot access the mail server.
6002	Minor	NETWORK	Unable to access Superuser account	Verify Superuser configuration.	The system cannot access the superuser account for Advanced UM.
7001	Major	TRANSACTION	No More SpinVox transcription credits (Speech To Text)	Buy more credits and activate the SpeechToText Feature.	The Speech to Text account credits are depleted. To fix the problem, purchase additional credits from your Authorized Mitel Reseller and then re-activated the feature.
7002	Warning	TRANSACTION	Invalid credentials for SpinVox transcription (Speech To Text)	Enter valid credentials.	Incorrect Speech to Text credentials have been provided. To fix the problem, re-enter the credentials (username, password, account ID, application ID).

Alarm Type ID	Default Severity	Alarm Class	Type Name	Prescription	Cause of Alarm
7003	Warning	TRANSACTION	Near end of credits for SpinVox transcription (Speech To Text)	Please buy additional credits.	The Speech to Text account credits are almost depleted. To fix the problem, purchase additional credits from your Authorized Mitel Reseller.
8001	Major	ERROR	SAA misconfiguration or missing language	Make sure SAA language installed and configuration is correct.	The Speech Auto Attendant has one of the following problems: • Incorrect configuration • Missing language • Mismatch of NuPoint database restore

Note:
Enterprise Manager does not support NuPoint UM and will not receive/display alarm messages.

26.52.4 Message Purge - Overview

A message purge clears the hard disk of unplayed, urgent, and played messages; it frees disk space for other tasks. Purging can be done in one of two ways: automatically or manually.

Automatic purges run daily at the default time of midnight. Deletion is controlled by the message retention settings in the LCOS of each mailbox.

Manual purges do not rely on LCOS settings but on parameters entered by the administrator at the time of the purge. Deletion can be limited by settings like mailbox number, class of service, or age of message. Manual purges must be done using the **Text Console**.

26.52.5 Backup and Restore

The following backup options are supported:

- LAN Backup to:
- an FTP Server
- a network share using Microsoft Networking
- a USB Memory Device

Restore procedures for LAN- and USB-based backups are supported for the following configurations:

- Standard and Active/Passive
- Active/Active

Requirements

Backing up NuPoint UM data can take a few seconds or up to several hours and should be performed during off-peak periods when traffic is at a minimum. Factors that influence the duration include:

- The nature of the files to be backed up and the amount of information being transferred. Messages, names, and greetings are large files and significantly increase the backup duration.
- The network speed: the throughput of the network between the NuPoint UM system and the storage server.
- The processing speed of the storage server.

The backup process saves all of the data to a single, large compressed file and is therefore limited by the destination file system:

File system	Maximum File Size
FAT32	4 GB
NTFS	2 TB
ext3	16 GB to 16 TB*
* Depends on the system block size but is typically 2 TB.	

For example, if you are backing up data to a Windows client that uses the FAT32 file system (the default for many older versions of Windows), you are limited to a maximum file size of 4 GB; newer Windows

operating systems that use the NTFS file system have a much larger capacity. If the backup file exceeds the maximum file size of the client operating system, it cannot be properly restored.

Web Console or Text Console?

You can perform all of the backup and restore procedures using Text console and some of the backup and restore procedures using Web console, as illustrated in the following table.

Procedure	Text console	Web console
Configure login, network, and backup settings for the destination server	Y	Y
Configure scheduled (automatic) LAN backups	Y	Y
Perform manual backups	Y	N
Back up data to USB memory devices	Y	During scheduled backups only
Restore data	Y	N

LAN Backup

NuPoint Unified Messaging supports backups of all data from the NuPoint server(s) using Microsoft Networking or an FTP server on the customer's Local Area Network (LAN), and provides system restore capability from the LAN archive to the server. You can restore data using FTP / MS Networking interchangeably, provided that you use the same directory path for both. The format of backed up data is the same, regardless of whether you backed it up using FTP or MS Networking.

Microsoft Networking enables NuPoint Unified Messaging to mount a remote driver or folder on a Microsoft Windows PC. The supported Windows operating systems include:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2012

A LAN backup and restore involves the following procedures:

- Configure the FTP server/MS Network Share for LAN backup and restore.

- Back up all configuration settings, mailbox names, messages, greetings, and billing information.
- Schedule automatic daily, weekly, monthly or delayed LAN system backups that occur once or repeatedly at specified times or dates.
- Activate inactive configurations after scheduling backups.
- Restore systems to retrieve backed-up content from the LAN archive.

USB Backup

You can back up to USB memory devices. It is the responsibility of the administrator to ensure that the memory device can accommodate the size of the backup as backing up a large number of recordings to such a device may fail if there is inadequate storage.

Many memory sticks will work but the following two brands are officially supported:

- Sandisk Cruzer flash drive
- Lexar Jumpdrive flash drive

Restore Data

Using Text console, you can perform the following data restore operations:

- LAN Restore using FTP
- LAN Restore using MS Networking
- USB Restore

Note:
FPSA user information is not included in a NuPoint backup. If it is necessary to perform a restore procedure, FPSA user information will not be included.

26.52.6 Configuring the Microsoft Network Share for LAN Backups and Restores

Before you back up the LAN, you must configure the backup data store. Ensure the folder or drive to be used for LAN backups is shared with Read/Write permission to the "userid" configured in the NuPoint UM menu.

Note:
To configure the network share for LAN backups and restores refer to in a Windows environment go to http://support.microsoft.com/kb/304040.

To configure the Microsoft Network Share

1. On the target drive, set up the root directory for the NuPoint UM backup (for example, NUPOINT\SiteA) and click **I Agree** to continue.
2. Right-click the root folder and select **Properties**.
3. On the **Sharing** tab, select **Share this folder**.
4. After **Share name**, type the name of the root directory for the NuPoint UM backup (in this example, type **NUPOINT\SiteA**) and click **OK**.
5. Click **Permissions**. The Share Permissions window appears.
6. Under **Group or user names**, add the user ID/group that will need to access the NP-Backup directory.
7. Under **Permissions for Everyone**, after **Allow**, select the **Full Control**, **Change**, and **Read** check boxes to grant everyone full control of the NUPOINT\SiteA directory and click **OK**.
8. On the **Security** tab, add the user ID/group (the same group you selected in Step 6) that will need to access the NUPOINT\SiteA directory.
9. Under **Permissions for Everyone**, after **Allow**, select the **Full Control**, **Modify**, **Read & Execute**, **List Folder Contents**, **Read**, and **Write** check boxes to grant everyone full control of the NP-Backup folder and click **OK**.

26.52.7 System Shutdown

Note:
This option is only available through the **Text console**.

System shutdown is an orderly shutdown procedure that warns callers when the system terminates call processing. You should run this program before turning off the power to a NuPoint UM node. We recommend that you perform this procedure during periods of low-call traffic.

What Happens When I Give the System Shutdown Order?

- The system asks for permission to shut down the node (module).
- The node's phone lines are displayed with their state indicated ("active", "idle", or "stopped")
- Phone lines that are carrying calls at the time you give the shutdown command are taken offhook when the caller who leaves a message, or the user who is logged into a mailbox, either presses a key or allows a silence timeout.

  - The caller or user hears the shutdown warning and is disconnected:

    "I'm sorry, the system is currently shut down for maintenance. Please call back later."

    EXAMPLE:If the shutdown occurs while a user is making a message for another system user, he can continue to record the message. But when he presses a key to review the message, or stops recording for the silence timeout interval, the system interrupts the call, plays the shutdown warning, sends the message, and logs out the user.

    - Phone lines taken offhook by the system are listed as **idle** in the line states display (prevented from answering new incoming or outgoing calls).

    - Phone lines with interrupted calls are listed as **stopped** in the line states display.

- All message-waiting indicator requests are canceled. Message lights are turned off even when there are unplayed messages in mailboxes.

  - Pager/message delivery calls and re-pages are not made during shutdown or afterward.
  - Message Indicator Request Queue Length shows how many message requests were lost on shutdown.
  - The system displays the status of each line and the lengths of the message indictor and paging request queues.
  - Lights are not turned on until new messages are received after shutdown.
- Callers who try to access the shutdown lines will hear a busy signal until the system is completely rebooted.

26.52.8 Auto Purge

An automatic message purge can be run daily without input from the administrator. A time for the automatic purge can be configured using Offline Configuration.

Configure Auto Purge

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. Click **Auto Purge**. The Auto Purge configuration screen is displayed.
4. In the **Time to run purge** field, select the hour at which you want to run the daily purge. By default, this value is set a 00 (midnight).
5. In the **Delay after Message Waiting Off Request** field, enter the amount of time to delay after the "message waiting off" request is sent. By default this value is set to 0. Enter any valid value between 0 and 50 (increments are .1 seconds so a setting of 10 = 1 second). Use this value when slower MWI methods like DMTF-to-PBX are used.
6. Click **Save**.
7. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.52.9 Auto Backup

You can use the Auto Backup option to schedule automatic backups and to specify details for the backup file destination. For more information about backups, see Backup and Restore.

Note: When you are finished making offline changes, you are instructed to save (commit) the changes to make them permanent in the offline (inactive) configuration. To make the revised configuration take effect in your system, you must then activate the offline configuration.

Configuring Auto Backup

To use Web console to schedule automatic LAN backups (for backups that use either FTP or MS Networking)

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Auto Backup**. The Auto Backup configuration screen is displayed.
4. Select **Turn on auto backup**.
5. In the **Frequency** list, select the frequency in which the system the system will perform backups.

   - If you selected **Daily**, select the **Hour of Day** to perform the backup. (The default is 0, midnight.)
   - If you selected **Weekly**, select the **Day of the Week** and the **Hour of Day** to perform the backup.
   - If you selected **Monthly**, select the **Day of Month** and the **Hour of Day** to perform the backup.
   - If you selected **Delayed**, enter a **Year**, and select a **Month**, **Day of Month** and **Hour of Day** to perform the backup.
6. In the Backup Details section, select a **backup type** and configure its parameters:

   - FTP
   - USB
   - Hard Disk
   - MS Networking
7. Click **Save**.
8. In the navigation tree, select **Commit Changes, X** (Exit), and **Y** (Yes).
9. Activate the configuration.

Turning Off Auto Backup

To turn off Auto backup

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. After **Duplicate Active Configuration**, select **Yes**.
3. In the navigation tree, click **Auto Backup**. The Auto Backup configuration screen is displayed.
4. Clear the **Turn on auto backup** check box.
5. In the navigation tree, select **Commit Changes, X** (Exit), and **Y** (Yes).
6. Activate the configuration.

26.52.10 Backup Parameters

FTP Backup

Parameter	Description	Value
FTP Server IP Address/ hostname	Enter the IP address of the FTP server to which you are backing up the data.	Valid IP address or hostname

Parameter	Description	Value
FTP Server User ID	Enter your FTP server user ID.	Max 15 characters
FTP Server Password	Enter your FTP server password.	Max 15 characters
Backup Path	Enter the path to the location on the FTP server where you want to back up the data.	
Backup Messages	Select this check box to back up the mailbox messages.	
Backup Names and Greetings	Select this check box to back up names and greetings.	
Back up Fax Cover Pages	Select this check box to back up fax cover pages.	

USB Backup

Parameter	Description	Value
USB Drive Path	Select the USB path from the list of installed USB devices.	
Backup Path	Enter the path to the location where the backed up data is to be stored.	
Backup Messages	Select this check box to back up the mailbox messages.	
Backup Names and Greetings	Select this check box to back up names and greetings.	
Back up Fax Cover Pages	Select this check box to back up fax cover pages.	

Hard Disk Backup

Parameter	Description	Value
Backup Path	Enter the path to the location on the hard disk where you want to back up the data.	
Backup Messages	Select this check box to back up the mailbox messages.	
Backup Names and Greetings	Select this check box to back up names and greetings.	
Back up Fax Cover Pages	Select this check box to back up fax cover pages.	

MS Networking Backup

Parameter	Description	Value
MS Network Destination Hostname	Enter the IP address of the PC where the data will be backed up.	
MS Network Domain	Enter the name of the domain to connect to the MS Network-enabled server.	
MS Network Shared Path	Enter the path to the shared directory on the PC where the data will be backed up.	
Backup Path	Enter the path to the directory where the backup data will be stored.	
MS Network User ID	Enter the user name for the local account on the PC where the data will be backed up.	

Parameter	Description	Value
MS Network Password	Enter the password for the local account on the PC where the data will be packed up.	
Backup Messages	Select this check box to back up the mailbox messages.	
Backup Names and Greetings	Select this check box to back up names and greetings.	
Back up Fax Cover Pages	Select this check box to back up fax cover pages.	

26.52.11 Perform System Shutdown and Startup

You can shut down NuPoint in order to perform offline maintenance. Two shutdown option are available. The first automatically restores the NuPoint services when you reboot the machine. The second requires you to restore the services manually.

System Shutdown

To perform a system shutdown:

CAUTION:
CAUTION: You should follow the policies of your site to warn users prior to the system shutdown, because this process removes the server from call processing.

1. From the navigation tree, click **Utilities** > **Stop NuPoint**.
2. Select a shutdown option:

- **Stop services and restart when machine reboots**

  If you select this option, the NuPoint services will remain stopped until you reboot the machine, at which time they are restarted automatically. For instructions to reboot the machine, see Shutdown or Reconfigure.
- **Stop services and do not restart when machine reboots**

  If you select this option, the NuPoint services will remain stopped even after you reboot the machine. You must then restart the services manually. For instructions to restart the services, see System Startup (below).

3. Click **Stop NuPoint**, and then click **OK**. You will be redirected to the MSL Server Manager, where you may perform maintenance and then reboot the machine.

System Startup

If you have selected the second shutdown option (Stop services and do not restart when the machine reboots), use the following procedure to restart the NuPoint services manually from the MSL Server Manager.

To perform a system startup:

1. From the MSL Server Manager, select **Applications > NuPoint Web Console**.
2. Select **Start NuPoint**, and then click **OK**.

26.52.12 Fax Download Settings

The NP Fax feature enables users to receive faxes in their mailboxes as electronic documents. Users can then send the faxes from their mailboxes to an actual fax machine, forward them to other mailboxes, send over the network or view then in the Web View interface.

Use this procedure to define the format you wish to receive, store and print faxes on the NuPoint UM system:

- TIFF (Tagged Image File Format): a computer file format for storing raster graphics images.
- PDF (Portable Document Format): a file format used to present documents in a manner independent of application software, hardware, and operating systems.

To configure the FAX download settings:

1. From the navigation tree, click **Utilities** > **Fax Download Settings**.
2. Choose one of the following:
   - For PDF format, select **Download Fax as PDF**.
   - For TIFF format (default), clear **Download Fax as PDF**.
3. Click **Save**.

26.52.13 Enable Alarm Management

You can configure the system to send alarm notifications (traps) to an SNMP agent or an email account. You can also specify whether a notification is generated for each alarm, for all alarms of a particular type (Information, Warning, etc.), or for all alarms together. The first option results in the most notifications; the last option results in the fewest notifications.

Configure Alarm Management on NuPoint

To configure alarm management:

1. From the navigation tree, click **Alarm Manager** > **Configuration**.
2. Select a notification method: **SNMP Notification** or **Email Notification**, or both.
3. For each method, select the frequency of notification:

   - **Every Alarm** to receive notification for each and every alarm
   - **Every Kind** to receive notification for each **type** of alarm
   - **Once** to receive one notification for any and all alarms.
4. Select the **Severity Level** that will trigger an alarm (Information, Warning, Minor, Major, Critical).
5. If you selected Email notification, enter the email addresses to which you want to send the alarm messages. Enter each email address and then click **Add**.
6. Click **Save**.

Note:
Alarm management emails received in the Outlook environment may not have the proper heading format because the "Auto Remove Line Breaks" feature in Outlook is enabled. To correct this problem, search for article # 287816 at http://support.microsoft.com/

Configure SNMP on MSL

If you selected SNMP Notification, you must configure the SNMP service on the Mitel Standard Linux (MSL) server.

To configure the SNMP settings:

1. Log in to the MSL Server Manager as "admin."
2. From the navigation tree, click **Configuration**, and then click **SNMP**.
3. For Service Status, select **Enabled**.
4. Enter the following settings:

   - **Community string**: Enter the address that SNMP clients use to monitor the server. The default string is “public”. For security, chose a non-default string.
   - **System contact address**: Enter the administrator's email address. If this field is left blank, the local administrative account is used y default.
   - **System location**: Enter the name of the system (for example, New York admin server).
   - **Network access setting**: Select one of the four available settings to permit access to SNMP information for the localhost only, immediate local networks only, all configured local networks, or all local networks and remote networks.
   - **SNMP Trap host or address**: Type the IP address where trap messages will be sent.
   - For all other fields, accept the default values.
5. Click **Save**.

Note:
For detailed instructions on how to configure SNMP on the MSL server, refer to the *NuPoint UM Technician's Handbook* and the *Mitel Standard Linux Installation and Administration Guide*.

Manage Alarms

To manage alarms:

1. From the navigation tree, click **Alarm Manager** and then click **View.**
2. From the alarm display list, select the alarms to display (All Alarms, Active Alarms, or Acknowledged Alarms). Click **Refresh** at any time to update the list.
3. Do one or more of the following:
   - to acknowledge an alarm, select the alarm check box and then click **Acknowledge**.
   - to delete an alarm, select the alarm check box and then click **Delete**.
   - to export an alarm to a .csv file, select the alarm check box and then click **Export to CSV**.
4. To determine the alarm category, click **Description**.

Note:
You cannot acknowledge an alarm that has previously been deleted. If you attempt to do so, you will *not* receive a notification of any sort from the system.

26.52.14 Automatic Message Purge

You can purge message storage automatically by programming a daily time for the purge to run (the default setting is '0' or midnight). Message disposal parameters are dictated by the LCOS settings for each mailbox.

To configure automatic message purge:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, **(G) Offline Menu**, and then **(B) Duplicate Active Configuration**
2. Select **(S) Auto Task Menu** and then **(B) Auto Purge**.
3. Select **(A) Hour to Run Purge=** and enter the hour at which you want the purge to start. (**0** is midnight.)
4. Select **(B) Delay after Message Wait Off Request** and enter the amount of time to delay after the "message waiting off" request is sent. By default this value is set to **0**. Enter any valid value between 0 and 50 (increments are .1 seconds so a setting of 10 = 1 second). Use this value when slower MWI methods like DMTF-to-PBX are used.

5. Exit to the main menu to save the changes to the offline configuration. You will need to activate the inactive configuration before your changes take effect.

26.52.15 Manual Message Purge

The parameters that you enter in the Manual Purge menu control which messages will be deleted.

To perform a manual message purge:

1. Notify users about the purge beforehand by sending a Message of the Day, to inform users which types of messages will be purged. See Recording Messages/Greetings/Tutorials, for instructions.
2. From the Main menu, select **(S) System Maintenance** and then **(M) Manual Message Purge**.
3. At the **Range of extensions to purge? (first-last)** prompt, enter the numbers of the first and last mailboxes in a range, separated by a hyphen (for example, 100-399) OR press <Enter> to check ALL mailboxes for old messages.
4. At the **Feature Classes to purge** prompt, enter one of the following:

   - **o** = odd numbered only
   - **e** = even numbered only
   - **u** = upper half only
   - **l** = lower half only
   - **x-y** to enter a range (x and y are numbers between 1 and 640)
   - **x, y, z** to enter individual classes
   - **x** to enter a single class of service
   - **Enter** = purge all mailboxes or purge all classes of service
5. At the **Group Classes to purge** prompt, enter o/e/u/l, the number(s), range, or press **Enter** for all (as in step 4).

6. The system now offers a series of age prompts. Select one of the following parameters or press **Enter** to move to the next prompt without selecting:

   - **Age, in hours, of played messages to purge? [<CR> for no purge]:**The age of a played message indicates the number of hours it is stored on the hard disk after it was played and kept.
   - **Age, in hours, of unplayed messages to purge?** This value indicates the number of hours an unplayed message is stored on the hard disk.
   - **Age, in hours, of urgent messages to purge?** This value indicates the number of hours an urgent message is stored.
   - **Age, in hours, of cut-through receipts to purge?**
   - **Age, in hours, of receipts to purge?**
   - **Age, in hours, of played fax messages to purge?**
   - **Age, in hours, of unplayed fax messages to purge?**
   - **Age, in hours, of urgent fax messages to purge?**
   - **Age, in hours, of fax receipts to purge?**
   - **Age, in absolute hours, of messages to purge?**
   - Purge Distribution Lists (Enter 'Y' or <CR> for no purge]. Purge searches distribution lists for all mailboxes. If a mailbox is in a distribution list, but that mailbox does not exist, Purge removes it from the distribution list. (When this mailbox is the last one in a list, the list is deleted.)
   - **Age, in hours, of NIB copy lists to be purged?** Enter a value between 1 and 999.

The system displays the conditions you specified for the messages to purge.

1. If the conditions are correct, type **purge** (lower-case) to activate the purge. If the conditions are NOT correct, press Enter and start the procedure again.

Purging is complete when the system displays the shortened version of the System Maintenance Menu.

26.52.16 Perform a USB Backup

You can back up to USB memory devices. It is the responsibility of the administrator to ensure that the memory device can accommodate the size of the backup as backing up a large number of recordings to such a device may fail if there is inadequate storage.

Before You Begin

- Ensure that the USB memory device can accommodate the size of the backup.

- Before the USB device can be used for backup it must be formatted with a file system. Any USB storage device that is formatted as FAT32 (DOS) or ext3 (Linux), or NTFS (Windows and Linux) is compatible.
- The file size limit for USB backups is set by the destination file system: 4 GB for a FAT32, 2 TB for NTFS, and 16 GB to 16 TB for ext3 (depending on file system block size). The current MSL ext3 block size is 4096 bytes which allows file sizes of 2TB.

To perform the backup

1. Insert the USB device (in the master node for systems with multiple nodes).
2. In Text Console, select **S (System maintenance)**, **L (NPM Backup**), and **U (USB Backup)**.
3. Select **A (USB Drive Path)** and then select the USB device to use.
4. Configure the following USB backup settings:
   - **(D) Backup Path** = [enter the **path** to the location where the backed up data is to be stored]
   - **(M) Backup Messages (Y/N)** = [enter **Y** to backup mailbox messages or **N** to skip]
   - **(N) Backup Names and Greetings (Y/N)** = [enter **Y** to backup names and greeting or **N** to skip]
   - **(F) Backup Fax Coverpages (Y/N)** = [enter **Y** to backup Fax coverpages or **N** to skip]
   - Select **B (Perform Backup)**. The device configuration is always backed up.
5. Return to the **Main Menu** and quit Text console.

26.52.17 Configure the FTP Server for LAN Backups and Restores

Before you back up the LAN, you must configure the backup data store. You can use any properly configured FTP server for LAN backups. The configuration requirements vary across FTP server types. The following example details how to configure an open source Server on a Windows operating system.

Note:
The configuration requirements and procedures vary across FTP server types.

Configuring the FTP Server for LAN Backup and Restore

To configure the backup data store on the FTP server

1. Set up the root folder for the NuPoint UM backup (for example, NUPOINT\SiteA) and click **I Agree** to continue.
2. Double-click the executable file to download the server software.
3. On the **Licence Agreement** window, click **I Agree** to proceed with the installation.

4. On the **Choose Components** window, click **Next** to install the default installation options:
    a. Server (Service)
    b. Administration Interface
    c. Start Menu Shortcuts
    d. Desktop Icon
5. On the **Choose Install Location** window, click **Next** to accept the default location to install the server software: **C:\Program Files\Backup Server**.
6. On the **Startup Settings** window
    a. Click **Next** to accept the default startup settings for the Backup Server: **Install as service, started with Windows (default**).
    b. Click **Next** to accept additional default startup settings for the Backup Server: Start if user logs on, apply to all users (default).
7. On the **Installation Complete** window, click **Close**.
8. On the **Connect to Server** window, click **OK** to accept the default server IP address and port and click **OK**. The Backup server console opens.
9. In the **Backup Server Console**, on the **menu bar**, click the **Groups** (double headed) icon. The Groups window appears.
10. To create a group for backing up data, under **Groups**, type a name and click **Add**.
11. Set up shared folders for the group:
    a. Under **Page**, click **Shared folders**.
    b. In the center pane, click **Add** and add the NuPoint UM backup root folder (you created in Step 1) as the shared folder.
    c. Under **Files and Directorie**s, select all of the check boxes to enable all of the file and directory options.
    d. Click **Set as home directory** to make the directory the home directory for the group and click **OK**.
12. In the **BackupServer Console**, on the **menu bar**, click the **Users** (head) icon. The Users window appears.
13. Set up a user account:
    a. Under **Users**, enter a password and click **Add**.
    b. Under **Account settings**, ensure **Enable account** and **Password** are enabled.
    c. After **Group membership**, select the **group** you created in Step 10.
    d. After **Maximum connection** count, enter **0**.
    e. After **Connection limit per IP**, enter **0**.
    f. Under **Page**, click S**hared folders** to continue.

14. Set up shared folders for the user account:

    a. Under **Page**, click **Shared folder**s.
    b. In the center pane, click **Add** and add the NuPoint UM backup root folder (you created in Step 1) as the shared folder.
    c. Under **Files and Directories**, select all of the check boxes to enable all of the file and directory options.
    d. Click **Set as home directory** to make the directory the home directory for the user and click OK. The Backup server console opens.
    e. Log on to the FTP server to test the network share.

26.52.18 Back up the LAN using FTP

NuPoint UM supports manual and scheduled backups of all application data from the NuPoint UM server(s) using Microsoft Networking or a FTP server on the customer's LAN. Each backup is a full and independent backup of NuPoint UM data, and does not include existing MSL configuration data. You perform backups over the LAN to an FTP server or a Microsoft network share.

NuPoint UM provides a system restore capability from the LAN archive to the server. You can restore data using FTP / MS Network interchangeably, provided that you use the same directory path for both. The format of the backed up data is the same, regardless of whether you backed it up using FTP or MS Networking.

Backing up NuPoint UM data can take a few seconds or up to several hours. Factors that influence the duration include

- The nature of the files to be backed up and the amount of information being transferred. Messages, names, and greetings are large files and significantly increase the backup duration.
- The network speed: the throughput of the network between the NuPoint UM system and the storage server.
- The processing speed of the storage server.

Before You Begin

- For the LAN backup to function, you must enable write access on the customer's FTP server before you perform the backup. Failure to do so will result in errors.
- Ensure the Windows PC has sufficient disk space available for the backup.
- If you have added local host names for VPIM servers to the MSL server, the host names are not backed up by the LAN backup procedure. To back up local host names for VPIM servers on the MSL server, you must back up the MSL server settings before you perform the LAN backup procedure. For information on backing up the MSL server, refer to the Mitel Standard Linux Technician's Handbook on the Mitel Customer Documentation site.
- Ensure the network connection is functioning and is stable.
- For Active/Active and Active/Passive systems, ensure the backup is restored to the correct server (for example, the server1 backup must be restored to server1) in order to maintain cluster and ILO information.

- Configure the FTP Server for LAN backups and restores.

To specify network, login, and default backup settings for the FTP destination server

1. Access **Text console** and connect to the **NuPoint UM node**.
2. Log in as **root** and type the **root** password.
3. Access the FTP Backup menu: select **S (System Maintenance)**, **L (NPM Backup Menu)**, and **L (Lan Backup using FTP)**.
4. In the FTP Backup menu, configure the following settings:

1.
   - **(I) FTP Server IP Address/host name** = [enter the **IP address** of the FTP server to which you will back up the data (for example, 10.32.63.100)]
   - **(U) FTP Server User ID** = [enter the **FTP server user ID**]
   - **(P) FTP Server Password** = [enter the **FTP server password**]
   - **(D) Backup Path =** [enter the **path** to the location on the FTP server where the data will be backed up.] You specified the name of the root folder in Step 1 of Configuring the FTP Server for LAN Backups and Restores.
   - (M) **Backup Messages (Y/N)?** = [enter **Y** (yes) or **N** (no) to indicate if mailbox messages will be backed up]
   - (N) **Backup Names and Greetings (Y/N)**? = [enter **Y** (yes) or **N** (no) to indicate whether mailbox names and greetings will be backed up]
   - (F) **Backup Fax Coverpages (Y/N)** = [enter **Y** (yes) or **N** (no) to indicate whether Fax cover pages will be backed up] The system configuration is automatically backed up the FTP server.

1. Type **B** (Perform Backup) to begin the backup process.
2. When the backup is complete, under **General information** the **Status** line confirms if the backup was completed successfully.
3. Return to the **Main Menu** and quit Text console.

26.52.19 Perform a LAN Backup using MS Networking

NuPoint UM supports manual and scheduled backups of all application data from the NuPoint UM server(s) using Microsoft Networking or a FTP server on the customer's LAN. Each backup is a full and independent backup of NuPoint UM data, and does not include existing MSL configuration data. You perform backups over the LAN to an FTP server or a Microsoft network share.

NuPoint UM provides a system restore capability from the LAN archive to the server. You can restore data using FTP / MS Network interchangeably, provided that you use the same directory path for both. The format of the backed up data is the same, regardless of whether you backed it up using FTP or MS Networking.

Backing up NuPoint UM data can take a few seconds or up to several hours. Factors that influence the duration include

- The nature of the files to be backed up and the amount of information being transferred. Messages, names, and greetings are large files and significantly increase the backup duration.
- The network speed: the throughput of the network between the NuPoint UM system and the storage server.
- The processing speed of the storage server.

Before You Begin

- Ensure the folder or drive to be used for LAN backups is shared with Read/Write permission for the userid configured in the NuPoint Unified Messaging menu. Failure to do so will result in errors.
- Ensure the Windows PC has sufficient disk space available for the backup.
- If you have added local hostnames for VPIM servers to the Mitel Standard Linux server, the hostnames are not backed up by the LAN backup procedure. To back up local hostnames for VPIM servers on the Mitel Standard Linux server, you must back up the Mitel Standard Linux server settings before you perform the LAN backup procedure. For information about backing up the Mitel Standard Linux server, refer to the *Mitel Standard Linux Installation and Maintenance Guide* available at Mitel OnLine.
- Ensure the network connection is functioning and is stable.
- The file size limit for LAN backups is set by the destination file system: 4 GB for a FAT32, 2 TB for NTFS, and 16 GB to 16 TB for ext3 (depending on file system block size). The current MSL ext3 block size is 4096 bytes which allows file sizes of 2TB.
- For Active/Active and Active/Passive systems, ensure the backup is restored to the correct server (for example, the server1 backup must be restored to server1) in order to maintain cluster and ILO information.
- Configure the MS Network Share for backups and restores.

To specify network, login, and default backup settings for the Microsoft Network destination server

1. Access Text console and connect to the NuPoint UM node.
2. Log in as "root" and type the admin password.
3. To access the MS Networking Backup menu, select **S (System Maintenance)**, **L (NPM Backup Menu**), and **M (Lan Backup using MS Networking**).
4. In the MS Networking Backup Menu, configure the following settings:

   - **(I)** MS Network Destination Hostname = [enter the **IP address** of the server to which you will back up the data (for example, 10.33.63.111).]
   - **(A)** MS Network Shared Path = [enter the **path** to the shared folder on the PC where the data will be backed up]
   - **(U)** MS Network User Id = [enter the **user name** for the local account on the PC where the data will be backed up.]
   - **(P)** MS Network Password = [enter the **password** for the local account on the PC where the data will be packed up.]
   - **(D)** Backup Path = [enter the **path** to the folder where the data will be backed up.] You specified the name of the root folder in Step 1 of Configuring the MS Network Share for backups and restores.
   - **(M)** Backup Messages (Y/N)? = [enter **Y** (yes) or **N** (no) to indicate whether you want to restore the mailbox messages.]
   - **(N)** Backup Names and Greetings (Y/N)? = [enter **Y** (yes) or **N** (no) to indicate whether you want to restore the mailbox names and greetings.]
   - **(F)** Backup Fax Coverpages (Y/N) = [enter **Y** (yes) or **N** (no) to indicate whether you want to restore the Fax cover pages.]

Note:
The system configuration is automatically backed up to the MS Networking server.

5. Select **B (Perform Backup)** to begin the backup process. When the backup is complete, under **General information** the **Status** line confirms if the backup was completed successfully.
6. Exit to the **Main Menu** and quit Text console.

Troubleshooting a LAN Backup (MS Networking)

- If the backup fails (times out, broken connection), you are given a choice to either start it again from beginning or to resume the last backup. The time-out value in case of a broken LAN connection is 1 minute.
- The following scenarios are possible during a LAN Backup/Restore:
- LAN connection failure - The backup stops after a time-out of 1 minute. In this case, you must restart the backup manually. The system prompts you to either resume the backup or restart it from the beginning. The log file will specify the error encountered.
- Windows server share not available - This scenario is same as LAN connection failure. See above.
- Remote disk full - The backup process can not find out if the disk space is full or not. The processes will simply log the error that it could not copy the file(s). Attempts to resume the backup may continue failing. Ensure that enough disk space is available on the remote server.
- Login failure - Backup will stop immediately, indicating the appropriate error in the log file.

26.52.20 Configure Scheduled LAN Backups

You can schedule automatic daily, weekly, monthly or delayed LAN system backups that occur once or repeatedly at specified times or dates.

Before You Begin

Manually back up the LAN to confirm it is configured properly before you schedule automatic backups.

Note:

- If Auto Backup is interrupted, it will not resume from where it was interrupted—it will always start at the beginning.
- After you schedule the automatic LAN backup, you *must* activate the configuration.

To schedule automatic LAN backups (for backups that use either FTP or MS Networking)

1. Access Text console and connect to the NuPoint UM node.

2. Log in as **root** and type the **root** password.
3. Select **S (System Maintenance)**, **R (Reconfiguration)**, **R (Reconfigure System)**, and **G (Offline Menu)**.
4. In the Offline menu, select **B** to duplicate the active configuration and then select **S (Auto Task Menu)**.
5. In the Auto Task menu, select **D (Backup Menu)**. The NPM Backup menu appears.
6. Select **T (Backup Type)** and then select **F (FTP)** or **M (Microsoft Networking)**.
7. Select **E (Enable Regular Backup)** and then select **D (Daily)**, **W (Weekly)**, **M (Monthly)**, **or O (Delayed)**.
8. Configure a daily, weekly, monthly, or delayed LAN backup (Refer to the procedures below.)
9. Select **B (Backup Messages)** and then select **Y**.
10. Select **N (Backup Names and Greetings)** and then select **Y**.
11. Select **F (Fax Cover Pages)** and then select **Y**.
12. Exit to the **Main Menu**.
13. Activate the inactive configuration.

Schedule a Daily LAN Backup:

1. From the NPM Backup Menu, select **D (Daily Backup Menu)**.
2. Select **H (Hour to do Backup)** and enter the number (from zero (midnight) to 23 hours) that corresponds to the hour at which the backup will begin.
3. Exit to the **Main Menu**.

Schedule a Weekly LAN Backup:

1. From the NPM Backup Menu, select **W (Weekly Backup Menu)**.
2. Select **D (Day to do Backup)** and enter the letter that corresponds to the day of the week on which the backup will occur: (M - Monday, T - Tuesday, W - Wednesday, TH - Thursday, F - Friday, S - Saturday, SU - Sunday).
3. Select **H (Hour to do Backup)** and enter the number (from zero (midnight) to 23 hours) that corresponds to the hour at which the backup will begin.
4. Exit to the **Main Menu**.

Schedule a Monthly LAN Backup:

1. From the NPM Backup Menu, select **M (Monthly Backup Menu)**.
2. Select **M (day of Month to Do Backup)** the enter the number (from 1 to 28) that corresponds to the date/day of the month on which the backup will occur.
3. Select **H (Hour to do Backup)** and enter the number (from zero (midnight) to 23 hours) that corresponds to the hour at which the backup will begin.
4. Exit to the **Main Menu**.

Schedule a Delayed LAN Backup:

1. From the NPM Backup Menu, select **O (Delayed Backup Menu)**.
2. Select **Y (Year to do Backup)** and specify the year during which the scheduled backup will occur, (for example, type 2005).

3. Select **M (Month to do backup)** enter type the number (from 1 to 12) that corresponds to the month in which the backup will occur.
4. Select **D (Day to do backup)** and enter the number (from 1 to 28) that corresponds to the date/day of the month on which the backup will occur.
5. Select **H (Hour to do Backup)** and enter the number (from zero (midnight) to 23 hours) that corresponds to the hour at which the backup will begin.
6. Exit to the **Main Menu**.

26.52.21 Restore Data

CAUTION:
Partial restore is not supported. Ensure that all data you want to keep is backed up before restoring.

Use this procedure to perform any of the following data restore operations:

- LAN Restore using FTP
- LAN Restore using MS Networking
- USB Restore

Message waiting indicators will automatically refresh following a restore. Time required for MWI restore is dependent upon the number of mailboxes in the system.

This procedure requires you to shut down the system and disable the module(s). All modules of a system must be both stopped and disabled before restoring the database.

Note:
Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

Standard and Active/Passive Systems

To restore previously backed-up data:

1. Shut down the system and disable all the modules. See Shutting Down the System. The module will reboot automatically as part of the system shutdown.
2. At the # prompt, enter **startnpm**. A list of commands is displayed.
3. At the **Enter one of the names:** command, type **system.restore**, and then press **Enter**. The Restore Menu is displayed.
4. Select one of the following restore options from the menu:

   - USB Restore
   - LAN Restore using FTP
   - LAN Restore using MS Networking

5. Modify the parameters in the restore menu as follows:

   In the USB Restore Menu:

   - (D) Backup Path = [enter the path to the backup folder]
   - (R) Restore From = [enter the number that corresponds to the date of the backup you want to restore]
   - (C) Restore System Configuration (Y/N) = [enter Y (yes) or N (no) to indicate whether you want to restore the system configuration.]
   - (M) Restore Messages (Y/N) = [enter Y (yes) or N (no) to indicate whether you want to restore the mailbox messages.]
   - (N) Restore Names and Greetings (Y/N) = [enter Y (yes) or N (no) to indicate whether you want to restore the mailbox names and greetings.]
   - (F) Restore Fax Coverpages (Y/N) = [enter Y (yes) or N (no) to indicate whether you want to restore the Fax coverpages.]

   In the FTP Restore Menu:

   - (A) FTP Server IP Address = [enter the IP address of the FTP server from which you are restoring the data, for example, 192.168.1.101]
   - (U) FTP Server User Id = [enter your FTP server user ID, for example, anonymous]
   - (P) FTP Server Password = [enter your FTP server password, for example, ftp1001]
   - (D) Backup Path = [enter the LAN Backup path from which you are restoring the data, for example, NUPOINT\SiteA]
   - (R) Restore From = [enter the number that corresponds to the date from which you would like to restore the archived system backup]

Note:
A maximum of 20 of the most recent backup dates are listed.

- (C) Restore System Configuration (Y/N)? = [enter Y (yes) or N (no) to indicate whether you want to restore the system configuration.]
- (M) Restore Messages (Y/N)? = [enter Y (yes) or N (no) to indicate whether you want to restore the mailbox messages.]
- (N) Restore Names and Greetings (Y/N)? = [enter Y (yes) or N (no) to indicate whether you want to restore the mailbox names and greetings.]
- (F) Restore Fax Coverpages (Y/N) = [enter Y (yes) or N (no) to indicate whether you want to restore the Fax coverpages.]

In the MS Networking Restore Menu:

- (I) MS Network Destination Hostname = [enter the IP address of the PC to restore the data to.]
- (A) MS Network Shared Path = [enter the path to the shared folder on the PC where the data will be restored]
- (U) MS Network User Id = [enter the user name for the local account on the PC.]
- (P) MS Network Password = [enter the password for the local account on the PC.]
- (D) Backup Path = [enter the path to the folder that contains the backup data you want to restore.]
- (R) Restore From = [enter the number that corresponds to the date from which you would like to restore the archived system backup]
- (C) Restore System Configuration (Y/N)? = [enter Y (yes) or N (no) to indicate whether you want to restore the system configuration.]
- (M) Restore Messages (Y/N)? = [enter Y (yes) or N (no) to indicate whether you want to restore the mailbox messages.]
- (N) Restore Names and Greetings (Y/N)? = [enter Y (yes) or N (no) to indicate whether you want to restore the mailbox names and greetings.]
- (F) Restore Fax Coverpages (Y/N) = [enter Y (yes) or N (no) to indicate whether you want to restore the Fax coverpages.]

6. Select **(S) Perform Restore** to begin the restore process. If you are restoring messages and/or names, the following message may appear: "Speech Allocation Manager (SAM) Initialization is in progress. This can take maximum 15 minutes. Do you want to continue [yes/no]"
7. Select **yes** to continue with the system restore. (If you select no, the system restore process is aborted.) The restore process begins.
8. When the system restore process has completed, the LAN Restore Menu will reappear. Exit from this menu by selecting **(X) Exit**. The system updates the configuration records.
9. At the prompt, type host.status, and then press Enter. The Module Maintenance Menu is displayed.
10. Select **(E)** to enable a module, or type **all** to enable all the modules.
11. If you are enabling a specific module, type the number of the module at the Which Module? prompt.
12. At the # prompt, type **console** to return to the Main Menu.
13. Reboot the system to restore FPSA functionality. For more information see FPSA.
14. Log into each of the other modules and start up NuPoint Unified Messaging manually.

The data restore is now complete.

Active/Active Systems

To restore data on an Active/Active system

1. Log into the master node using the cluster IP address.
2. Shut down the NuPoint Unified Messaging system by accessing the System Maintenance Menu and selecting the **(S) System Shutdown** option.
3. Answer **N** to the **Transfer mastership to another node?** prompt that appears if you are on a master node.
4. Answer **All** to the **Modules to shutdown** prompt, and then type **Y** to confirm.
5. Type **shutdown** to reconfirm and start the shutdown process.
6. Answer the questions to the **MWI** and **Paging** prompts.
7. Answer **Y** to the **Enable or disable modules?** prompt.
8. From the Module Maintenance Menu that appears, select **D** to disable a module (you then need to enter the specific module to disable), or type **all** to disable all the modules.
9. NuPoint Unified Messaging is now completely stopped.
10. Type **startnpm** to start NuPoint Unified Messaging.
11. When the NuPoint Unified Messaging system has started, type **system.restore** to start the data restore process.
12. The data restore process for the Active/Active system is the same as for the Standard platform, steps 4 through 13, above.
13. NuPoint Unified Messaging will start on a local node, and you then need to access the second active node to invoke the **startnpm** command manually.

The data restore is now complete.

26.53 Hard Disk Utilities

Information about the hard drives in your system can be obtained from the Hard Disk Utilities menu.

Information for All Disks

1. From the Main menu, select **(S) System Maintenance** and then **(H) Hard Disk Utilities**.
2. Select **(I) Information for all Disks**.
3. The system displays disk size, type and status information:

```
================================================================================

* * * M O D U L E # 1 D I S K I N F O R M A T I O N * * *

Disk Size Rev. Disk Type Redund Status Errors

---- --------- ---- --------- ------ ------ ------

0:0 139GB PRIMARY 0:0 ENABLED

1:1 139GB REDUNDANT* 0:0 ENABLED

================================================================================

'*' : Probably not working.

Press any key to continue...
```

Physical Table Display

To display physical information about the disks in your system:

1. From the Main menu, select **(S) System Maintenance** and then **(H) Hard Disk Utilities**.
2. Select **(P) Physical Table Display**.
3. The system displays the physical characteristics of the system disk:

```
>>> Physical Characteristics Table <<<

1 Disk

DISK ID CAPACITY SERIAL NUMBER DISK TYPE REDN ID STATUS

------- -------- ------------- --------- ------- ------

0, 0 78156225 1234 PRIMARY 0, 0 ENA

(END)
```

Virtual Table Display

To display information about the virtual disks in your system:

1. From the Main menu, select **(S) System Maintenance** and then **(H) Hard Disk Utilities**.
2. Select **(V) Virtual Table Display**.
3. The system displays the characteristics of all virtual drives:

```
>>> Virtual Drive Characteristics Table <<<

VID DISK ID TYPE OFFSET SIZE FLAGS

--- ------- ---- ------ ---- -----

000 0,0 QNX 00080325(0x000139c5) 02040255(0x001f21bf)

001 0,0 PROMPT 00000154(0x0000009a) 00530048(0x00081680) P

002 0,0 PROMPT 00530202(0x0008171a) 00530048(0x00081680) P

003 0,0 PROMPT 01060250(0x00102d9a) 00530048(0x00081680) P

004 0,0 PROMPT 01590298(0x0018441a) 00530048(0x00081680) P

005 0,0 PROMPT 02120346(0x00205a9a) 00530048(0x00081680) P

006 0,0 PROMPT 02650394(0x0028711a) 00530048(0x00081680) P

007 0,0 PROMPT 03180442(0x0030879a) 00530048(0x00081680) P

008 0,0 PROMPT 03710490(0x00389e1a) 00530048(0x00081680) P

009 0,0 ACCOUNT 04240538(0x0040b49a) 00032834(0x00008042)

010 0,0 ACCOUNT 04273372(0x004134dc) 00032834(0x00008042)

011 0,0 ACCOUNT 04306206(0x0041b51e) 00032834(0x00008042)

012 0,0 ACCOUNT 04339040(0x00423560) 00032834(0x00008042)

013 0,0 ACCOUNT 04371874(0x0042b5a2) 00032834(0x00008042)
```

26.54 Change Text Console Password

The password for the 'admin' and 'root' users is the same password, and is set when the MSL operating system is installed and configured. We recommend that you do not change the root password, as it will not make a corresponding change to the 'admin' password and they will be out of synch.

If it is your intention to have different passwords for the 'admin' and 'root' users, then you can use the following procedure to do so.

To change the console password:

1. From the Main menu, select **(S) System Maintenance** and then **(P) Passwords/Security**.

2. Select **(C) Change Password** and enter the new 'root' password. The console passcode may be 6 to 30 alphanumeric characters. The letters may be upper or lower-case.
3. When prompted, re-enter the new password. The system confirms the password change.

Note:
Administration by phone requires a different phone passcode. Instructions for setting a passcode for phone administration are provided in Administration by Phone. When FPSA is activated, additional restrictions apply to console passcodes. See Functionally Partitioned System Administration (FPSA).

26.55 Set System Time and Date

This option allows you to reset the system time and date. You can also review the time and date without changing it by pressing **Enter** in response to the prompts.

1. From the Main menu, select **(S) System Maintenance**, **(O) Additional Options**, and then **(T) Time and Date**.
2. When prompted, enter the new date in the format mm-dd-yy where:

   - **mm** = two-digit month code
   - **dd** = two-digit day code
   - **yy** = two-digit year code (for example, enter **12-27-09**)
   - OR press **Enter** to skip this prompt
3. When prompted, enter the new time in the format hh:mm [am/pm] where:

   - hh = two digit hour code (1-12)
   - mm = two digit minute code
   - [am/pm] = AM or PM setting (For example, enter **03:29 pm**)
   - OR press **Enter** to skip this prompt

26.56 Lights Test

The lights test is used to test the function of message-waiting indicators (usually lights). Depending on the programming of the mailbox being tested, the lights test can also activate pagers and provide stutter dial tone.

To Perform a Lights Test

1. From the Main menu, select **(S) System Maintenance**, **(O)Additional Options**, and then **(L) Lights Test**.

2. At the Mailbox to light (1 - 99999999999) prompt, enter the *number* of the mailbox associated with the light to be tested OR enter a range of mailboxes to test; separate the first and last mailbox numbers in the series with a hyphen (for example, 100-399).
3. At the **Light off/on/existing value (0/1/2)** prompt, enter one of the following:

   - Enter **0** (zero) to turn the message waiting indicator(s) OFF
   - Enter **1** to turn the indicator(s) ON
   - Enter **2** to update the indicator(s) to the current correct state(s).

> **Note**:
> The "correct state" is ON if there is at least one unplayed message in the mailbox, and OFF if no unplayed messages reside in the mailbox.

4. At the **Message waiting type (0 or <CR> for all)** prompt, press Enter to test any message waiting type(s) associated with the test mailbox(es) OR enter a number (from 2 through 28) to test a specific message waiting indicator.
5. Check the state of the indicator(s) for proper functioning. To return the indicators to their correct states, repeat Steps 2 through 4 using the same mailbox number(s) and enter **2** at Step 3.

> **Note**:
> Pagers must be set to OFF before they can be reactivated a second time.

6. At the **Mailbox to Light (1 - 99999999999)** prompt, press **Enter** to return to the Additional Options Menu.

26.57 Enable Alarm Management

You can configure the system to send alarm notifications (traps) to an SNMP agent or an email account. You can also specify whether a notification is generated for each alarm, for all alarms of a particular type (Information, Warning, etc.), or for all alarms together. The first option results in the most notifications; the last option results in the fewest notifications.

Configure Alarm Management

To enable alarm management:

1. From the Main Menu, select (**S**) **System Maintenance**, and then (**T**) **Alarm Setting and Management.**
2. Select **(A) Alarm Setting**.

3. Select a notification method:

   - For SNMP notification, select **(A) SNMP Settings**.
   - For Email notification, select **(B) Email Settings**. **Note**: You can configure both methods.

4. In the Alarm SNMP Setting or Alarm Email Setting menu, select option **(A)**to enable notification and enter:

   - **1** to enable OR
   - **0** to disable

5. Select option **(B)** to set the **Sending Option** and enter one of the following:

   - **0** to report every alarm type
   - **1** to report only once (if an alarm is raised when there is no existing active alarm)
   - **2** to report every alarm individually

6. Select option **(C)** to set **Sending Severity** and enter one of the following:

   a. **1** for Informational alarms
   b. **2** for Warning alarms
   c. **3** for Minor alarms
   d. **4** for Major alarms
   e. **5** for Critical alarms

7. For Email notification, select option **(D)** to set **Email Addresses** for alarm messages. Enter one or more email addresses separated by commas.
8. Exit to save your changes.

Note:

- Alarm management emails received in the Outlook environment may not have the proper heading format because the "Auto Remove Line Breaks" feature in Outlook is enabled. To correct this problem, search for article # 287816 at http://support.microsoft.com/.
- If you enable SNMP Notification, you must configure the SNMP service on the Mitel Standard Linux (MSL) server. For instructions, see Configure SNMP on MSL. For additional information, refer to the *Mitel Standard Linux Installation and Administration Guide* .

Report and Manage Alarms:

You can manage alarms and produce reports for active alarms, cleared alarms, or all alarms.

To manage alarms:

1. From the Main Menu, select **(S) System Maintenance**, and then **(T) Alarm Management.**
2. Select **(B) Alarm Report and Management**.

3. Select one of the following options:

   - Option (**A**) to Report and Manage **Active** Alarms
   - Option (**B**) to Report and Manage **Acknowledged** Alarms
   - Option (**C**) to Report and Manage **All** Alarms
   - Option (**D**) to report Alarm status

4. Do one or more of the following:

   - Select Option (**A**) to display a report of each alarm category
   - Select option (**B**) to acknowledge a selected alarm or option (**C**) to acknowledge all alarms, as required
   - Select option (**D**) to delete a selected alarm or option (**E**) to delete all alarms, as required

26.58 Perform System Shutdown and Startup

To perform a system shutdown:

CAUTION:
You should follow the policies of your site to warn users prior to the system shutdown, because this process removes the server from call processing.

1. From the Main menu, select **(S) System Maintenance** and then **(S) System Shutdown**.
2. Type **shutdown** (lowercase).
3. At the **Modules to shutdown?** prompt, enter **1**.
4. The system displays a warning about call processing being terminated. Enter **Y** to continue. The system displays the status of each line of the module as "idle," "active" or "stopped," and updates the status every minute until all lines are stopped. The system stops any calls still in progress after five minutes.
5. At the **Wait for message waiting queues to clear?** prompt, enter **Y** to wait or **N** to proceed without waiting.
6. At the **Wait for paging queues to clear?** prompt, enter **Y** to wait or **N** to proceed without waiting.
7. At the **Do you want to enter the menu to enable or disable modules?** prompt, enter **Y** if you want to leave a server disabled after the shutdown/reboot (possibly for some offline maintenance) OR enter **N** to continue with shutdown (skip to step 10).
8. If you entered **Y** in step 7, module status is displayed. Enter **(D) to disable** a module or **(E) to enable** a previously-disabled module.
9. When prompted to **select a module ID**, enter **1**. The module state is changed to your selected state.
10. Press **Enter** to return to the root # prompt.
11. Type **startnpm**.

    - If you have disabled the module, the system warns you and offers a menu of offline maintenance choices (for example, system.restore, console). Select a maintenance procedure as required. To re-enable the module, type **host.status** and select **(E)** to enable.
    - If you have just changed the module state to "enabled", the node reboots.

12. The screen displays startup messages and then returns to the root prompt. Type**console**to return to the Main menu.

26.59 Adjust Audio Stream

Automatic Gain Control (AGC) is a MiVoice Business ICP, MiVoice Business feature that adjusts the volume of audio streams of individual calls so they are neither too loud nor too faint. You enable or disable AGC on a system wide basis. The default setting is Disabled. AGC settings are maintained during system reboots and are backed up.

To enable automatic gain control functionality:

1. Access Text console and connect to the NuPoint UM node.
2. Log in as "root" and type the admin password.
3. Exit to the Linux prompt and enter **touch /usr/vm/config/AGCon**
4. Restart the server.

To disable automatic gain control functionality:

1. Access Text console and connect to the NuPoint UM node.
2. Log in as "root" and type the admin password.
3. Exit to the Linux prompt and enter **rm -f -r /usr/vm/config/AGCon**

26.60 Security - Overview

Server security refers to protecting your NuPoint Unified Messaging server from abuse, both from outside callers and from mailbox owners. Outside callers can attempt to “take over” mailboxes that can be reached through the public switched telephone network and use them for their own applications. Mailbox owners can make inappropriate use of server resources by placing long distance calls through the server, overusing available storage, or sending messages to mailboxes that should be “off limits.”

The server has many features that are designed to provide security at the server level and at the mailbox level. These features address server administration, mailbox usage, and access to facilities, applications, and information.

This section describes the following features:

- Protecting your server from outside abuse
- Protecting your server from abuse by mailbox owners and users
- Protecting the server maintenance and administration functions
- Security reports and audit trails
- Functionally Partitioned System Administration (FPSA)

26.60.1 Protection From Outside Abuse

Mailboxes that can be reached through the telephone network are seen as the primary entry point for “hostile invasion” of a communications server such as the NuPoint Unified Messaging server. Service providers and corporate telecommunications managers alike are concerned about hackers taking over mailboxes for their own applications, or using mailboxes for toll fraud by calling through long-distance facilities accessible from the server.

You can configure your server to require access codes or passcodes before callers can reach various functions, and you can configure mailboxes to automatically perform certain functions, such as hanging up after playing a greeting.

Existing Mailboxes

The first level of security is protection of the mailboxes by **passcodes**. By default, the server requires passcodes on all mailboxes. You can turn this feature off using feature bit 218 for direct calls, but you should do so with caution. Mailbox owner passcodes can be up to 10 digits in length, and users can change their passcodes at any time (feature bit 073).

The server administrator typically sets a temporary passcode for new mailboxes, but the user is forced to enter a permanent passcode during the interactive tutorial. Using FCOS settings, you can prevent users from setting a passcode that is the same as the mailbox number (feature bit 130), or from using trivial passcodes, such as 1234 or 8888 (feature bit 201).

If a caller enters the wrong passcode when trying to get into a mailbox, the server requires the caller to enter the correct passcode twice, or the server hangs up. Callers are not told whether the mailbox number or the passcode was incorrect; hackers do not know if they have even half of a valid combination. (You can use feature bit 081 to set the server to only require a single correct passcode after an incorrect attempt, but this reduces the effectiveness of the security feature.)

The server tracks bad passcode attempts for each mailbox and compares the number to the parameters set for the line group. If the bad passcode attempts for a mailbox exceeds the number allowed in the passcode trip period, the server plays a bad passcode warning at the next login so that the mailbox owner knows that someone may have tried to gain unauthorized entry.

Feature bit 132 allows you to enable a bad passcode lockout, in which a mailbox is locked when the threshold of bad passcode attempts is reached. Only the server administrator can unlock the mailbox, set a new temporary passcode, reset the tutorial, and require re-initialization from the integrated telephone number (feature bit 142).

New Mailboxes

When you create a new mailbox, you can designate a temporary passcode for that mailbox, either by making up a passcode, or using the server’s random passcode generation program.

Note:
When you choose the random passcode generation program, you must make note of the number generated and provide that number to the mailbox user so that they can log in to their new mailbox.

If you have created mailboxes but have not yet assigned them to users, you can use an FCOS to deny login (feature bit 001).

To ensure that a new mailbox, once assigned, is not used until the owner accesses it, you can require initialization from the integrated telephone number (feature bit 142). You can also set the FCOS to prevent messages from being received until the mailbox has been initialized (feature bit 127).

Note:
Feature bit 142 (Must run tutorial from own phone) is not supported for all integrations.

Line Groups

By dividing the total number of ports in your server into line groups, you can increase the security for specific applications. You can configure each application to be on a different line group, and enable an appropriate level of security for each application.

Separating the applications by line group can help prevent certain types of abuse, such as connecting from one application to another. Incoming and outgoing calls occur on separate line groups in a server. This keeps hackers from reaching the server and then dialing out through the NP Receptionist or another application.

You can restrict access to certain line groups, like a toll-free dial-in line group, by setting the FCOS to require callers to enter an access code before hearing the regular line group greeting (feature bit 160). If a caller exits one mailbox, the server requires reentry of the access code before allowing further progress through the server. You can also use FCOS to completely deny login on specific line groups (feature bits 101-109), or ensure that mailboxes cannot receive messages when the call is received on a specific line group (feature bits 111-119).

Telephone Answering

Outside callers can abuse access to a server during a telephone answering call by trying to break into the dialed mailbox or access other features. By correctly setting the line groups and FCOS in your server, you can control the feature set available during an answering session.

You can force the termination of telephone answering sessions after callers leave a single message by setting the line group to not allow multiple messages for outside callers. For Greeting-Only mailboxes, you can have the server hang up immediately after playing the greeting (feature bit 062), call the mailbox attendant after the greeting (bit 063), or call the mailbox user after the greeting (bit 064).

By customizing an FCOS to contain feature bit 004 (Outside caller functions) but not feature bit 005 (Play outside caller menu prompts), you can allow knowledgeable users to access server functions, while not letting other callers know that the functions are available.

Feature bit 137 (Caller must enter access code) can restrict outside callers from leaving messages in high security mailboxes. You set the access codes when configuring each individual mailbox.

You can further ensure the privacy of mailbox users by not putting them in the Dial-by-Name database (feature bit 092), or by not allowing the mailbox name or extension number to be played (bit 202). This latter feature can be especially important in hotel or dormitory situations.

Audiotext (Tree Mailboxes)

You can protect audiotext applications by requiring callers to enter an access code (feature bit 137) before hearing the information. Because you can design audiotext applications as a series of mailboxes, each with individual information, you can set a unique access code for each piece of information to ensure corporate security.

You can configure audiotext applications to hang up after playing the greeting (feature bit 062), or transfer to the mailbox attendant (bit 063) or mailbox extension (bit 064). You can also deny login from within the tree (bit 152).

26.60.2 Protection From Mailbox Owner Abuse

The corporate telecommunications manager must control use and potential abuse of corporate resources to provide the best service while controlling costs and maintaining security. Likewise, the revenue of a service bureau is dependent on being able to bill mailbox owners for use of the server. The NuPoint UM server allows you to place controls and limits in the server to ensure that mailbox owners use the server appropriately.

Line Groups

Service bureaus can provide mailbox owners with certain line groups for receiving messages, while having them pick up their messages on other line groups, either to control costs or to control call flow. To enforce this type of usage, you can use feature bits 101-109 to deny login on specific line groups; callers can leave messages, but are not able to log into a mailbox. In this way, you can also restrict access to certain information to internal ports only, or to “800” number ports where the server owner must pay for connect time.

Mailbox Usage

Depending on the number of phone lines or the storage hours available on your server, or on the levels of service that mailbox owners pay for, you can set LCOS parameters to control certain aspects of mailbox usage, such as connect time, number of messages stored, or storage duration.

If the number of phone lines to your server is limited, you can limit call duration by setting the Maximum login time parameter in each LCOS to a few minutes. On the other hand, if disk storage is a limiting factor, you can lower both the Caller message length and User message length, and set the Message count limit to a number that is equitable to all users assigned to each LCOS.

The amount of storage used on your server is the result of the number of messages stored and the length of storage time. You can control the storage times for played and unplayed messages by setting the two LCOS parameters: Played message retention and Unplayed message retention.

Besides setting limits on server usage, you must ensure that your mailbox listings are current—remove mailboxes that are no longer being used. Once you have removed a mailbox, the server automatically removes it from the Dial-by-Name database and from all distribution lists.

Messaging

Messaging between mailbox owners is the primary purpose of many voice mail systems, but you must use GCOS and FCOS settings to enforce restrictions on which mailboxes can exchange messages.

The primary tool for controlling messaging between mailboxes is the GCOS. Correct GCOS settings can effectively partition a server so that separate user groups are not aware of one another, or so that certain mailboxes can only receive or send messages to other specific mailboxes, such as in dispatcher situations.

GCOS structures also create partitioned Dial-by-Name. A mailbox owner cannot use Dial-by-Name to address a message to a mailbox that is not accessible due to GCOS restrictions; the server does not match or play inaccessible mailbox names.

You can also use FCOS settings to control the sources and destinations for messages. Feature bits 040 through 045 control a mailbox's ability to receive messages from various sources, such as other users, outside callers, or distribution lists. Feature bits 020 through 035 control the ability to make or give messages to users and distribution lists.

Outdials

Depending on the optional features purchased with your server, mailbox owners can send a variety of outdial calls, including call placement, message delivery, auto wakeup, and paging. To prevent abuse and to provide better call traffic, you can restrict different outgoing call types to specific line groups and set appropriate restrictions and limits on each line group. This prevents users from accessing other services on dedicated line groups and allows you to monitor resource usage.

Mailbox owners can use the message delivery feature for message waiting, in which the server calls a specified number when the mailbox owner receives a new message. The person who answers the phone must enter the correct passcode to access the mailbox, thus ensuring that only the mailbox owner can listen to the message.

Mailbox owners can use call placement to record a message and send it to a telephone number (as opposed to a mailbox). The message sender can record the name of the intended recipient and can optionally require a passcode before the message is played.

The FCOS and LCOS settings provide a tool for the administrator to control access to outdial services. Various feature bits enable use of the different features, and LCOS limits control the number of digits that a mailbox owner can enter for a target telephone number. You can set the message delivery, paging, and message phone lengths to seven digits to limit calls to the local service area, or 10 (or 11) digits to allow for long distance calls.

26.60.3 Security for System Administration

In the hands of a trained and responsible administrator or technician, server administration functions can be used to provide convenient and full-featured service to mailbox owners and callers, and to keep the server functioning smoothly. In the wrong hands, the same functions can be used to take over mailboxes, disrupt service, and even shut down the server. Security for the administration function is extremely important. However, when Functionally Partitioned System Administration (FPSA) is employed, server security is assured because access can be restricted to authorized persons only.

System Maintenance Console (Text and Web Consoles)

The system maintenance console—the main point of entry for configuration and administration—is one of the most critical factors in security. Console access is protected by a login sequence of **User ID** and **Passcode** to verify a user before allowing access to menus.

FPSA User ID

The FPSA user ID is a unique representation of a person's identity within the system, consisting of up to 14 alphanumeric characters. Each user ID is associated with one real name, although a single real name can be assigned multiple user IDs.

During the login sequence, you are identified by your user ID, the terminal device, and the module where you log in. Each subsequent activity you perform during a session at a server maintenance console can be recorded in the audit trail.

An FPSA user can perform the following tasks:

- Log in/out of Web or Text Console
- Change password in Web or Text Console
- Display privileges in Web Console

System Superuser

The system superuser (a system administrator who logs in as "root" or "admin") can display, on a system maintenance console, all current user IDs, along with the names, passcodes, permission categories, and other statistics associated with the IDs.

The system superuser can perform following user-maintenance tasks:

- Configure FPSA parameters in Web or Text Console
- Add, delete and unlock FPSA users in Web or Text Console
- Modify FPSA user permission categories in Web or Text Console
- Reset FPSA user passwords in Web or Text Console
- Display a list of FPSA users in Web or Text Console
- Start an audit trail in Web or Text Console
- Generate an audit trail report in Web or Text Console

Note:
The system superuser's login user IDs ("root" and "admin") cannot be changed.

Console Passcode

A user ID can be verified by entering an optional passcode consisting of a mix of alphabetic, numeric and punctuation characters. The same passcode can be used with different user IDs. The system superuser and FPSA users each have their own passcode.

FPSA Passcode Restrictions

FPSA passwords:

- must contain at least one alphabetic, one numeric and one punctuation character (3!CALDA@) in the first eight characters.
- must be between six and 64 characters log for Web Console access, and between six and 30 characters long for Text Console access.
- cannot be reused.
- cannot contain accented characters.
- cannot contain a substring (four or more characters) of the user ID. For example, the user ID "mark61" cannot have the console passcode "**mark**ey4!" or "n=**ark6**0" because each contains a substring that is part of the user ID (indicated in bold characters).

Each time you log in the system displays the date and time of your last login and the number of unsuccessful attempts, if any, since your last login.

Modem

A modem on a serial port of the system can be used by you, or anyone else, to gain access to all system maintenance and configuration capabilities. You must protect this access point from abuse. The same login sequence described in the previous section applies to any remote access that uses the modem.

Administrator's Mailbox

The administrator's mailbox can be used to perform several administration functions, including the creation and deletion of mailboxes.

To protect the administrator's mailbox:

- **Change the mailbox number** to any number up to 11 digits (you do not have to keep the default setting). If you do change the administrator's mailbox to a number with several digits, be sure the Dial Plan allows it (or change the plan).

- Make a passcode a condition for successful login.
-

Note:
The administrator's mailbox **must** have a passcode; it cannot be the same as the mailbox number, and it cannot be a trivial passcode (such as, 1234 or 8888).

- Set the FCOS to **require an access code** before callers can leave a message. If the administrator's mailbox number is not an integrated extension number, you must access the mailbox by calling the system: press the * key (star) at the first greeting, enter the administrator's mailbox number, press the * key (star), and enter the passcode.
- If the FCOS requires an access code, you must enter it before you can press the second * (star), thus adding a second level of passcode-type protection.
- Use FCOS settings to further **restrict mailbox access to certain ports**, or to deny login to the mailbox (FCOS Category 2).

- **Note**:
  If you deny login to the mailbox, you must use the system console to allow login prior to performing any administration by phone.

26.60.4 Security Reports and Audit Trails

Several reports available from the **Text Console** can indicate breaches in system security or potential security abuse or concerns.

Mailbox Reports

Use the following reports and options to review security issues. For details on specific reports see Reports Overview.

- The **Mailbox Dump Report** can be run for specific mailboxes to obtain information about mailbox activity, including login status and usage statistics.
- The **Idle Mailboxes Report** lists mailboxes with no activity. This listing contains any unassigned or non-initialized mailboxes in the server.
- The **Mailbox Totals Report** gives the same type of information as the Idle Mailboxes Report, except that it covers all mailboxes in the system.
- The **Mailbox Data Inquiry Report** provides summary statistics for a single mailbox or a range of mailboxes.
- The **Mailbox Data Report** contains information on the number of recent failed login attempts and on the date of the last mailbox owner login. Because this report covers all mailboxes and contains extensive information, it is the last report used to examine potential abuse problems.
- **Mailbox searches** can locate mailboxes that meet certain criteria (such as those with a specific FCOS or GCOS, or those without a passcode, or with the tutorial enabled). If you suspect system abuse, you can identify the mailboxes involved by performing a search with the right criteria.

Audit Trail

If you are the system administrator, you can obtain an Audit Trail Report of all users logged in during a specified period. After logging in, each subsequent activity performed during a session at a maintenance console is recorded in the audit trail.

Recorded information includes:

- User ID
- Time and date of activity
- Menus reached
- Actions taken
- Additional details you specify

Only the system administrator can configure and manage an audit trail. Audit trail options include:

- Start and stop the audit trail
- Review the audit trail report; each activity is recorded as a separate numbered entry
- Specify the maximum entries (up to 999,999) in an audit trail
- Specify the type of information that comprises an entry (entry details)
- Specify a range of entries to report

The audit trail resembles the system Logfile, but it does not need to be cleared. When the specified maximum number of entries is reached, the server continues to record new information, overwriting the oldest information and beginning again at entry 1. The system issues a warning, in the error log, when the number of entries reaches 85%, 90% and 95% of the maximum.

26.60.5 Configure Mailbox Passcode Parameters by FCOS

You can modify FCOS settings to control how mailbox owners can set their passcodes, including:

- Allow mailbox owners to change their passcodes
- Prevent the use of trivial passcodes
- Lock the owner out of the mailbox when there are too many invalid passcode entries.

To configure passcode parameters:

1. Customize an FCOS to include feature bit **70** (User Options Menu) and the following bits as applicable:
   - **73** (enter and change mailbox passcode)
   - **81** (only require one correct passcode for login)
   - **93** (deny change of passcode in first tutorial)
   - **130** (passcode cannot be same as mailbox)
   - **132** (bad passcode lockout if over limit)
   - **201** (deny trivial passcode)
   - **218** (passcode not needed on direct calls)
2. Assign the FCOS containing these bits to each mailbox that requires these passcode settings.

26.60.6 Restrict Line Group Access

This procedure describes how to restrict line group access in a variety of ways. Select those methods that are appropriate for your server and users.

Require Callers to Enter a Line Group Access Code

1. Customize an FCOS to include feature bit **160** (Caller must enter line group access code).
2. Set the Access Code in the Administrator's Mailbox for each line group that requires an access code. The Department Code is the line group access code. Callers do not have to enter an access code on line groups with no department code in the Administrator's Mailbox.

Deny Login on Specific Line Groups

- Customize each FCOS to include feature bit **101-109** (Deny login on line groups 1-9, respectively).

Force the Termination or Transfer of Calls to Greeting-only Mailboxes

- Customize an FCOS to include one of the following feature bits:
  - **62** (Hang up immediately after greeting)
  - **63** (Call mailbox attendant after greeting)
  - **64** (Call mailbox user extension after greeting)
- Assign the FCOS containing these bits to each greeting-only mailbox that requires these passcode settings.

26.61 List of Current Users

You can view a list of FPSA users who are currently logged into the Web Console.

Note:

- Only the system superuser can perform this procedure.
- The list includes FPSA users who have been added in both the Text Console and the Web Console.

To display a list of current users:

1. In the navigation tree, click FPSA Management >Who is online.

   The Administrators Online page displays the list of FPSA users who are currently logged in to the Web Console. The User ID, Name, and Login Time is provided for each user.
2. To update the page, click **Refresh**.

26.61.1 Start an Audit Trail

This procedure describes how to start the NuPoint Unified Messaging audit trail that creates a record of users logged in at a Web Console.

Note:
Only the system superuser (root) can perform this procedure.

To start an audit trail:

1. In the navigation tree, click Report Generation >**Start Audit Trail**.

   The Start Audit Trail page displays.
2. Enter a number from 1 to 999999 as the **Maximum Audit Trail Entries** to record. If you leave the current number of trail entries set to 0, the audit trail will remain empty even after being started.

Note:
The system issues a warning in the error log when the number of entries reaches 85%, 90% and 95% of the maximum. To ensure that this process functions properly, enter values in multiples of 100 (in other words, enter 200 or 2000, but do not enter 201 or 2222).

3. To start the audit trail, click **Start**.

The audit trail starts and continues running until it has recorded the number of events you specified or the system capacity is exceeded. If there is a capacity problem, a series of alarms are issued until the capacity limit is reached, at which time older audit trail entries will be overwritten.

Note:
Once you have started an audit trail, you cannot stop it. However, when you Export an Audit Trail all data is deleted, enabling you to start a new audit trail.

26.61.2 Export an Audit Trail

Use this procedure to download the audit trail and delete all existing entries. It is important to clear the data in this manner if your system has limited storage capacity.

Note:
Only the system superuser (root) can perform this procedure.

To export an audit trail:

1. In the navigation tree, click Report Generation >**Export**.

   The Export Audit Trail page displays.
2. Click **Export**.
3. Depending on which type of browser you are using, the download may begin automatically or the File Download dialog may display. If the File Download displays, navigate to the place where you wish to store the audit trail and click **Save**.

The report is exported in CSV format and data for the current audit trail is deleted. To resume the audit trail, you must Start an Audit Trail.

26.61.3 Generate an Audit Trail Report

Use this procedure to generate the current NuPoint Unified Messaging audit trail report and display it in the Web Console.

Note:
Only the system superuser (root) can perform this procedure.

To generate a report of the audit trail:

1. In the navigation tree, click Report Generation >**Report**.

   The Generate Audit Trail Report page displays.
2. Use the screen tools to select the **Time Range** (start and end date/time).
3. Use the **Include Data** check boxes to select which data columns and records numbers to include in the report.
4. Select the report format:
5. **Printer Friendly Version**: The report is opened in a web page which you can print.
6. **Export to CSV File**: The report is downloaded to your system in CSV format. Depending on which type of browser you are using, the download may begin automatically or the File Download dialog may display. If the dialog displays, navigate to the place where you wish to store the audit trail and click **Save**. No data is deleted when you perform this function.

Note:
Generating an audit trail report in printer friendly or CSV format *does not* delete any data, unlike when you Export an Audit Trail.

26.62 List of Authorized Users

You can view a list of FPSA users who have access to the server.

Note:

- Only the system superuser can perform this procedure.
- The list includes FPSA users who have been added in both the Text Console and the Web Console.

To display a list of authorized users:

- From the Main menu, select **(S) System Maintenance**, **(P) Passwords and Security**, and then **(L) List Users**.

Sample List of Authorized Users

```
User ID----------UID------Real Name----------Last Login------Has Password---Locked---Perm---

cmartin 5001 christal martin <none> Yes No .23456

jsmith 5003 Jeff smith <none> Yes No .2....

mjones 5002 melanie jones Aug 25 2011 Yes No ...45.
```

26.62.1 Configure Mailbox Passcode Parameters by Line Group

This procedure describes how to:

- Set a minimum and maximum passcode length
- Set the number of incorrect passcode attempts that will trigger a warning
- Set the period for counting incorrect passcode attempts

To configure mailbox passcode parameters by line group:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(R) Reconfigure System**.
2. Do one of the following:
3. Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it

4. Otherwise, select **(E) Modify Active Configuration**.
5. Select **(G) Group Selected** and enter the **number** of the line group (1-24) that you want to modify.
6. Select **(M) Modify Application** and then **(P) Passcode Menu**.
7. Select **(M) Minimum Passcode Length** and enter a **number** (4-10). This is the minimum number of digits that constitute a valid passcode for all users in the current line group.
8. Select **(N) Maximum Passcode Length** and enter a **number** (4-10). This is the maximum number of digits that constitute a valid passcode for all users in the current line group.
9. Select **(C) Passcode Trip Count** and enter the **number** of times (1-255) someone can attempt to use an incorrect passcode during a passcode trip period before a warning is issued, or enter **0** (zero) to disable the passcode trip count function.
10. Select **(P) Passcode Trip Period** and enter the **number** of hours (1-240) for the time limit for a passcode trip count, or **enter 0** (zero) to disable the passcode trip period function.
11. Save the parameter settings by exiting to the NuPoint Voice Configuration Main Menu.
12. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.62.2 Prevent Multiple Message In an Answering Session

Prevent Multiple Message In an Answering Session

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:
3. Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
4. Otherwise, select **(E) Modify Active Configuration**.
5. Select **(G) Group Selected** and enter the **number** of the line group (1-24) to modify.
6. Select **(M) Allow Multiple Messages for Outside Caller** and enter **N** to prevent outside callers from leaving more than one message with a single call-in.
7. Save the entry by exiting to the Main Menu. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.62.3 Set Site Name, Site Banner, or Site Code

To set the site name, site banner, and the site code:

Changing Site Name and Code

1. From the Main Menu, select **(S) System Maintenance**, and then **(N) Site Name, Code, Banner**. The server displays the current site name, code and banner.
2. Select **(N) Change Site Name** and then enter **Y** to change the site name, or **N** to keep the current site name.
3. If you entered Y, enter a descriptive site **name**, up to 60 characters.
4. Select **(C) Change Site Code** and enter a site code, up to 10 characters.
5. Exit the site name menu.

Changing the Site Banner

1. From the Main Menu, select **(S) System Maintenance**, and then **(N) Site Name, Code, Banner**. The server displays the current site name, code and banner.
2. Select **(B) Change Site Banner** and enter **Y** to change the site banner, or **N** to keep the current site banner.
3. If you entered Y, enter a **banner**, up to 240 characters, 65 characters or fewer per line. Terminate text by entering a **period** (.) on a new line and press **Enter**.
4. Exit the site name menu.

Reverting to the Previous or Default Site Banner

1. From the Main Menu, select **(S) System Maintenance**, and then **(N) Site Name, Code, Banner**. The server displays the current site name, code and banner.
2. Select **(P) Revert to Previous Site Banner** and enter **Y** to reset the site banner to the previous text, or **N** to keep the current site banner.
3. To change the banner back to the default setting, select **(D) Revert to Previous Site Banner** and then **Y** to reset the site banner to the default text, or **N** to keep the current site banner.
4. Exit the site menu.

26.63 Start or Stop an Audit Trail

This procedure describes how to start or stop the audit trail that creates a record of users logged in at a server text console.

Note: Only the system superuser (root) can perform this procedure.

Starting the Audit Trail

To start an audit trail:

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(T) Audit Trail Menu**.
3. Select **(A) Max. Number of Audit Trail Entries** and enter a **number** from 1 to 999999 for the maximum number of entries to record in the audit trail. If you leave the current number of trail entries set to 0, the audit trail will remain empty even though you start it.

Note:
The system issues a warning in the error log when the number of entries reaches 85%, 90% and 95% of the maximum. To ensure that this process functions properly, enter values in multiples of 100 (in other words, enter 200 or 2000, but do not enter 201 or 2222).

4. Select **(B) Start Audit Trail**. The audit trail begins.

Stopping the Audit Trail

To stop an audit trail:

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(T) Audit Trail Menu** and then select **(C) Stop Audit Trail**.

26.63.1 Format an Audit Trail Report

To format a report of the audit trail at the server console:

Note:
Only the system superuser (root) can perform this procedure.

To format an audit trail:

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(T) Audit Trail Menu** and then **(D) Audit Trail Report Menu**.
3. Select **(A) Details** and enter one of the following:

- **A** for all details
- A single field **number** for a single detail, for example, 5
- A range of field **numbers** for a continuous range of details, for example, 5-10
- A comma-separated list of field **numbers**, for example, 4,5,8. This list can also include a range, for example 4-8,9.
- Enter a question mark (**?**) to see a list of the details available:

Field Number	Abbrev.	Description
1	TEN	Trail entry number
2	DATE	Date of the entry
3	TIME	Time of the entry
4	PORT	TTY Port number
5	SVID	Server identifier
6	USER	ID of user logged in
7	PROG	Application or menu invoked
8	ACT	Action taken (start, stop, delete, c onfigure, etc.
9	SMBX	Starting mailbox number
10	EMBX	Ending mailbox number

4. Select **(B) Field Delimiter** and enter **0** to make the field delimiter a space, **1** to make the field delimiter a tab, or enter any printable character.
5. Select **(C) Starting Trail Entry Number** (to specify the first entry to be reported) and enter a trail entry **number** from 1 to 999999.
6. Select **(D) Ending Trail Entry Number** and enter an ending trail entry **number** from 1 to 999999.
7. Select **(E) Report's Width** and enter the **number** of characters, from 40 to 160, in a displayed line of the report

26.63.2 Generate an Audit Trail Report

Note: Only the system superuser (root) can perform this procedure.

To generate a report of the audit trail at a server text console:

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(T) Audit Trail Menu** and then **(D) Audit Trail Report Menu**.
3. Ensure that you have completed the Format an Audit Trail Report procedure before proceeding.
4. Select **(F) Generate Report**.

The server displays the report, formatted as specified, at the server console. When the end of the report is displayed, you can continue in the Audit Trail Menu or exit.

26.64 Functionally Partitioned System Administration

Functionally Partitioned System Administration (FPSA) is a standard software feature that requires you to enter your user identifier (user ID) and password for verification before you can reach any of the system maintenance console menus. Access to the menus is based on the authorization level of your user ID and password.

FPSA allows access to menus only to persons who are authorized through permission categories. In addition, FPSA requires passwords for all users logging in.

FPSA Permission Categories

Six permission categories are available. The first is applicable only to the system superuser. The remaining five can be applied to FPSA users to establish their privileges. The categories are described in the following table.

Category #	Category Name	Description
1	System Superuser	**Unlimited access to all Text and Web Console features and server resources. Can perform FPSA management activities such as adding users, unlocking users, changing permission categories, resetting passwords and starting audit trails.** **Two superusers ("admin" and "root") are created when the system is originally installed. You can reset their password, but you cannot change or delete them. If you forget the superuser password, you can contact Mitel assistance for assistance or reset it yourself using a Unix Shell command.**
2	NuPoint Voice Superuser	Access to all Text and Web Console features and server resources with t he exception of FPSA management.
3	System Configuration	**Access only to system configuration and network features in the Text and Web Console .** **For example, see Features Class of Service.**
4	Mailbox Maintenance	Access only to mailbox maintena nce features in the Text and Web Console .
5	Inquiry/Report Only	Access only to inquiry features such as Reports, Statistics, and Dump in the Text and Web Console .
6	Network Configuration	Access only to network and network-related features in the Text and Web Console .

After logging in as an FPSA user, you can perform menu-based procedures described in this section ONLY if you have the appropriate permission category or categories.

FPSA limits access to menus based on a permission category or categories assigned to each user ID. If you attempt to reach an unauthorized menu, the server responds with a “Permission denied” message. Each server menu also has one or more permission categories associated with it.

When you assign permission categories to each user, make sure that the combination is sensible. For example, category 1 gives access to the entire server, so there is no need to assign any other permission categories in addition. Categories 3 and 6 together give permission for all system configuration menus.

Using FPSA

FPSA is activated by default on the NuPoint UM system. Prior to using it, the administrator needs to configure the FPSA parameters and add up to 500 new users in the Text or Web Console. When these steps are complete, the users can reach console menus only if they have the proper permission category (or categories). Every console menu is associated with one or more permission categories.

Password Restrictions

The following restrictions apply to FPSA passwords:

- Passwords must contain at least one letter, one digit, and one punctuation mark. For example, **o;ster1**.
- Users must change their passwords periodically (default is 30 days). The new password must be different from the old one. The server issues a reminder notice at login warning that the password must be changed; the default reminder period is seven days. If the password is not changed before the expiration date, the server forces the user to change passwords after logging in. The system superuser can set the period between password changes and the period for displaying warnings.

The above-noted restrictions do not apply to the system superuser ("admin" and "root").

Login and Usage Errors

If a user enters an invalid or incorrect ID or password, the server displays “login incorrect” and the login sequence halts. If a user attempts to reach a menu outside the user's permission category or categories, the server displays "permission denied" and prohibits access.

After three unsuccessful login attempts, the user will be locked out and must contact the system superuser to have his or her password reset. If you are the system superuser and forget your password or become locked out, contact Technical Support for assistance or reset the password using a Unix Shell command.

Login Restrictions (Web Console only)

An FPSA user can only have one login session. If a user opens a second session on the same or another PC, the first session will be terminated.

A client can support only one login session. If an FPSA user opens a second session, the first session will be terminated.

FPSA users are automatically logged out after five minutes of inactivity.

Up to five users of any type (FPSA, "admin," or "root") can be logged in to Web Console simultaneously. If a sixth user attempts to log in, access will be denied.

Configuration

Configuration involves the following steps:

- Configure password parameters

- Add FPSA users to the Web or Text Console
- Set up an audit trail if desired

Note:
FPSA user information is not included in a NuPoint backup. If it is necessary to perform a restore procedure, FPSA user information will not be included.

NuPoint Feature Examples

The following table provides examples of how NuPoint features can be accessed with FPSA permission categories.

Feature	Permission Category				
1	2	3	4	5	6
Change Password and Security Settings	*				
Configure NP-UM Wake Up	*	*			
Configure Remote Modem Connection	*	*			
Resynchronize HIS PMS	*	*			
Manually Purge Messages	*	*			
Perform System Shutdown	*	*			
Set Site Name, Site Code, or Site Banner	*	*			
Perform Backup/Restore	*	*			
Manage Class of Service	*	*	*		
Edit/Activate Offline Configuration	*	*	*		
Configure Speech Auto Attendant	*	*	*		
Configure Unified Messaging	*	*	*		
Configure Call Director	*	*	*		
Enable Alarm Management	*	*	*		

26.64.1 Configure FPSA Password Parameters

This procedure describes how the system superuser can configure password parameters.

Note:
Only the system superuser can perform this procedure.

To configure FPSA password parameters:

1. In the navigation tree, click FPSA Management >Password Parameters.

   The Password Parameters page is displayed.
2. In the **Password Expiration Period** field, enter the number of days, from 1 to 365, preceding the expiration of a password that the server issues a warning to change the password. The default is 30 days.
3. Click **Save**. The setting change takes effect immediately.

26.64.2 Log In or Log Out of the Text Console

This procedure describes how to log in to or log out of a server through the NuPoint Unified Messaging Text Console. The login steps described below become the first steps in every procedure that requires access to a menu, even though they are not described in every procedure.

Logging In

To log in as an FPSA user:

1. Activate the NuPoint Unified Messaging Text Console.
2. At the Login prompt, enter your **user ID.**
3. **When prompted, e**nter your **password** or your temporary **password**. It does not display.
4. At your first login, you must change your temporary **password** to a personalized password. Your password:

   - must contain at least one alphabetic, one numeric and one punctuation character (3!CALDA@).
   - must be between six and 30 characters long.
   - cannot contain a substring (four or more characters) of your user ID.

When you have successfully logged in, the server displays a message such as the following:

****Last successful login: 12/24/10 9:41 a.m.

Login Incorrect

If "login incorrect" displays, one of the following may have occurred:

- You typed your user ID incorrectly
- You typed your password incorrectly
- Your user ID has been locked

Try again, being careful to enter the user ID and password correctly. If you are still unsuccessful, contact your system administrator to have your password reset. If you are the system superuser ("root" or "admin" user), contact Technical Support for assistance.

Warning About Password Expiration

If a warning about password expiration displays, you can continue logging in but you should change your password without delay, through the Passwords/Security Menu. If your password expires, you are forced to change it as soon as you log in.

Permission Denied

If a user does not have the correct permission categories to access a menu option, the server prompts "Permission Denied." To change your permission categories, contact your system administrator.

Logging Out

You can perform a routine logout from the Main Menu, or you can take a shortcut from any related menu.

- To log out routinely, return to the Main Menu, then press (**X**) to exit.
- To take a shortcut, press **Ctrl-C**.

In either method, when logout is completed, the server displays the login prompt on the main console only.

26.64.3 Add, Delete, Lock, or Unlock a User ID



These procedures describes how to manage user IDs with the Web Console.

Note:
Only the system superuser can perform the following procedures.

Adding a User ID

To add an FPSA user:

1. In the navigation tree, click FPSA Management >Administrators.

   The Administrators page is displayed.
2. Click **Add**.
3. Enter a unique **User ID** of up to 14 alpha-numeric characters.
4. Enter the user's actual **First Name** and **Last Name**. Each field can contain up to 50 alphabetic characters.
5. Select the password **Type**:
6. User Specified: If you select this option, you must manually configure the password by entering it twice. It must contain at least one alphabetic, one numeric and one punctuation character in the first eight characters, and be between six and 64 characters long. It cannot contain accented characters.
7. **System Generated**: If you select this option, the system will automatically generate the password.
8. Select the permission categories; for example: 4, 5, 6. At least one permission category is required. Refer to the table below for descriptions.

Category	Description
1	**System Superuser. Unlimited access to all features and server resources. Can perform FPSA management activities such as adding users, unlocking users, changing permission categories, resetting passwords and starting audit trails.** This category is created when the system is installed; therefore, it cannot be set through the console.
2	**NuPoint Voice Superuser. Access to all features and server resources with the exception of FPSA management.**
3	**System Configuration. Access only to system configuration and network features.**
4	**Mailbox Maintenance. Access only to mailbox maintenance features.**
5	**Inquiry/Report Only. Access only to inquiry features such as Reports, Statistics, and Dump.**
6	**Network Configuration. Access only to network and network-related features.**

9. Click **Save**. The settings take effect when you see the confirmation "<user ID> added."
10. Record the password and give it to the user.

Locking a User ID

While users are "locked," they cannot log in to the system. The system administrator can lock a user using the procedure outlined below, or a user may become locked by entering incorrect login credentials three times in a row.

To manually lock an FPSA user:

1. In the navigation tree, click FPSA Management >Administrators.

   The Administrators page is displayed.
2. Specify the users you wish to lock by selecting the check boxes next to their User IDs.
3. Click **Lock**.

A lock icon displays next the name of each user who is locked.

Unlocking a User ID

The system administrator can unlock users who have a "lock" icon next to their names on the Administrators page.

To unlock an FPSA user:

1. In the navigation tree, click FPSA Management >Administrators.

   The Administrators page is displayed.
2. Specify the users you wish to unlock by selecting the check boxes next to their User IDs.
3. Click **Unlock**.

Note:
You can also unlock a user by clicking the lock icon next to the user's name.

Deleting a User ID

To delete an FPSA user:

1. In the navigation tree, click FPSA Management >Administrators.

   The Administrators page is displayed.
2. Select the check boxes to the left of the ID column to choose one or more users, or all users.
3. Click **Delete**, and then confirm that you wish to proceed.

   The deletion takes effect and future login attempts will be prevented.

26.64.4 Modify Permission Categories for Current User IDs

This procedure describes how to add or delete permission categories for a current user ID. Assigning permission categories to a **new** user is covered in Add, Delete, or Unlock a User ID.

Note:
Only the system superuser can perform this procedure.

To modify permission categories for an FPSA user ID:

1. In the navigation tree, click FPSA Management >Administrators.

   The Administrators page is displayed.
2. Specify the user you wish to modify by selecting the check box next to the User ID.
3. Click **Edit**.
4. Enter up to five **categories**, numbers 2 - 6, each separated by a comma. You must enter all the categories desired, not just the category that you are adding or deleting. For example, to add category 6 to categories 4 and 5, enter 4,5,6.

Category	Description
1	System Superuser. Unlimited access to all features a nd server resources. Can perform FPSA management activities such as adding users, unlocking users, chang ing permission categories, resetting passwords and s tarting audit trails. This category is created when the system is installed; therefore, it cannot be set through the console.
2	NuPoint Voice Superuser.Access to all features and server resources with the exception of FPSA manag ement.
3	System Configuration.Access only to system configura tion and network features.
4	Mailbox Maintenance. Access only to mailbox main tenance features.
5	Inquiry/Report Only. Access only to inquiry features such as Reports, Statistics, and Dump.
6	Network Configuration. Access only to network and ne twork-related features.

5. Click **Save**. The category modification takes effect when you see the message "<User ID> modified.

26.64.5 Reset a Password

This procedure describes how the system superuser can reset an FPSA user password.

Note:
Only the system superuser can reset a user's password.

To reset an FPSA password:

1. In the navigation tree, click FPSA Management >Administrators.

   The Administrators page is displayed.
2. Specify the user you wish to reset by selecting the check box next to the User ID.
3. Click **Reset**.
4. Select the password **Type**:
5. User Specified: If you select this option, you must manually configure the password by entering it twice. It must contain at least one alphabetic, one numeric and one punctuation character in the first eight characters, and be between six and 64 characters long. It cannot contain accented characters.
6. **System Generated**: If you select this option, the system will automatically generate the password.
7. Click **Save**. The password change takes effect when you see "Password reset for user ID <user ID>. Password expiration date reset."

26.64.6 Configure FPSA Password Parameters

This procedure describes how the superuser can configure password parameters.

Note:
Only the system superuser can perform this procedure.

To configure FPSA password parameters:

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(P) Configure Password Parameters** and specify the **number** of days, from 1 to 365, before a password expires. The default is 30 days.
3. These settings take effect immediately.

26.64.7 Add, Delete, or Unlock a User ID

This procedure describes how to add or delete a user ID, and how to unlock the ID of a user. Adding a user ID involves specifying a user ID, the actual (real) name, a password, and permission categories. Only the server superuser can perform this procedure.

Adding a User ID

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.

2. Select **(A) Add User** and enter a unique **user ID** of up to 17 letters.
3. Enter the **real name**, up to 25 letters, of the person to be associated with this user ID.
4. Enter the permission categories; a **digit** from 2 through 6, or any combination of these digits, separated by commas. For example: 4,5,6. Refer to the table below for a description of permission categories.

Category	Description
1	Unlimited access to all console menus and all server resources (synonymous with server superuser access). This category cannot be set through the console.
2	Unlimited access to all console menus and Linux shell, except security features limited to the server superuser
3	Access only to system configuration menus except network configuration (see Features Class of Service)
4	Access only to mailbox maintenance menus
5	Access only to inquiry menus (read-only menus such as Reports, Statistics, and Dump)
6	Access only to network and network-related menus

1. The system assigns a temporary password that is valid for 30 days. Write it down and give it to the user.
2. These settings take effect when you see the confirmation "<user ID> added."

Unlocking a User ID

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(U) Unlock User** and enter the User ID of the locked user.
3. Unlocking takes effect when you see the confirmation "<user ID> unlocked."

Deleting a User ID

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.

2. Select **(D) Delete User** and enter the **user ID** to be deleted. Check the User ID and real name displayed to ensure it is the correct one to delete.
3. Enter Y to delete the user or **N** to keep the user.
4. The deletion takes effect when you see the confirmation "<user ID> deleted.

26.64.8 Modify Permission Categories for Current User IDs

This procedure describes how to add or delete permission categories for a current user ID. Assigning permission categories to a **new** user is covered in Add, Delete, or Unlock a User ID.

Note:
Only the system superuser can perform this procedure.

To modify permission categories for an FPSA user ID:

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(M) Modify User Data** and enter the **user ID** to be modified.
3. Press **Enter** until you are prompted to **Enter the permission categories (separated by commas)**.
4. Enter up to five **categories**, numbers 2 - 6, each separated by a comma. You must enter all the categories desired, not just the category that you are adding or deleting. For example, to add category 6 to categories 4 and 5, enter 4,5,6.

Category	Description
1	System Superuser. Unlimited access to all features and server resources. Can perform FPSA management ac tivities such as adding users, unlocking users, changing permission categories, resetting passwords and starting audit trails. This category is created when the system is i nstalled; therefore, it cannot be set through the console.
2	NuPoint Voice Superuser. Access to all features and ser ver resources with the exception of FPSA management.
3	System Configuration. Access only to system configurati on and network features.
4	Mailbox Maintenance. Access only to mailbox maintena nce features.
5	Inquiry/Report Only. Access only to inquiry features such as Reports, Statistics, and Dump.
6	Network Configuration. Access only to network and n etwork-related features.

The category modification takes effect when you see the message "<User ID> modified. Press any key to continue."

26.64.9 Reset a Password

This procedure describes how the superuser can reset a password for users.

Note:
Only the server superuser can reset a password.

1. From the Main Menu, select **(S) System Maintenance**, and then **(P) Passwords/Security**.
2. Select **(R) Reset** user password and enter the **user ID** to be modified.
3. Note the new temporary password assigned by the server.
4. The password change takes effect when you see "Password reset for user ID <user ID>.
5. Password expiration date reset."

26.64.10 List of Authorized Users

You can view a list of FPSA users who have access to the server.

Note:

- Only the system superuser can perform this procedure.
- The list includes FPSA users who have been added in both the Text Console and the Web Console.

To display a list of authorized users:

- From the Main menu, select **(S) System Maintenance**, **(P) Passwords and Security**, and then **(L) List Users**.

Sample List of Authorized Users

```
User ID----------UID------Real Name----------Last Login------Has Password---Locked---Perm---

cmartin 5001 christal martin <none> Yes No .23456

jsmith 5003 Jeff smith <none> Yes No .2....

mjones 5002 melanie jones Aug 25 2011 Yes No ...45.
```

26.65 Log In or Log Out of the Web Console

This procedure describes how to log in to or log out of a server through the NuPoint Unified Messaging Web Console. The login steps described below become the first steps in every procedure that requires access to a menu, even though they are not described in every procedure.

Logging In

1. Activate the NuPoint Unified Messaging Web Console.
2. At the Login prompt, enter your **user ID.**
3. **When prompted, e**nter your **password**. It does not display.

After you have successfully logged in, the server displays your User ID.

Login Incorrect

If "login incorrect" displays, one of the following may have occurred:

- You typed your User ID incorrectly
- You typed your password incorrectly
- Your User ID has been locked

Try again, being careful to enter your user ID and password correctly.

After three unsuccessful login attempts, you will be locked out. To regain access to the system, contact your system administrator to have your password reset. If you are the system superuser ("root" or "admin"), contact Technical Support for assistance.

Password Expiration

By default, FPSA user passwords expire after 30 days. The expiry interval can be changed by the system administrator to anything from one to 365 days.

One day before your password is due to expire, you will receive a warning message instructing you to change it. If you fail to do this and allow your password to expire, you will be prompted to configure a new password the next time you attempt to log in.

*P*ermission Denied

If you do not have the correct permission categories to access a menu option, the server prompts "Permission Denied." To change your permission categories, contact your system administrator.

Logging Out

You can log out while you are viewing any Web Console screen.

- To log out, click **Logout** in the upper right corner of the Web Console interface.

When logout is completed, the server displays the login prompt.

26.66 Change a Password

This procedure describes how users with any permission category can change their passwords.

NOTE: Change Password option is available for FPSA users only if the user is logged in through npm-admin.

Changing a Password

To change an FPSA password:

1. In the navigation tree, click **Utilities**>**Change Password**.

   The Change Password page is displayed.
2. Enter the following fields:

   - Enter old password
   - Enter new password
   - Confirm new password

> **Note**:
> Your new password:
>
> - must be different from the old password
> - must contain at least one alphabetic, one numeric and one punctuation character (3!CALDA@) in the first eight characters.
> - must be between six and 64 characters long.
> - cannot contain accented characters.
> - cannot contain a substring (four or more characters) of the user ID

3. Click **Save**. Your new password takes effect when you see the message "Password changed. Password expiration date reset."

26.67 Change Text Console Password

The password for the 'admin' and 'root' users is the same password, and is set when the MSL operating system is installed and configured. We recommend that you do not change the root password, as it will not make a corresponding change to the 'admin' password and they will be out of synch.

If it is your intention to have different passwords for the 'admin' and 'root' users, then you can use the following procedure to do so.

To change the console password:

1. From the Main menu, select **(S) System Maintenance** and then **(P) Passwords/Security**.
2. Select **(C) Change Password** and enter the new 'root' password. The console passcode may be 6 to 30 alphanumeric characters. The letters may be upper or lower-case.
3. When prompted, re-enter the new password. The system confirms the password change.

Note:
Administration by phone requires a different phone passcode. Instructions for setting a passcode for phone administration are provided in Administration by Phone. When FPSA is activated, additional restrictions apply to console passcodes. See Functionally Partitioned System Administration (FPSA).

26.68 Display Administrator Privileges

MITEL

This procedure describes how users can check which features they may access in the Web Console.

Note:
Feature access is determined by the permission categories you have been assigned by the system superuser.

To display administrator privileges:

- In the navigation tree, click Utilities >My Admin Privileges.

  The Administrator Privileges page displays a list of the features you may access on the Web Console:

- Mailbox Maintenance
- Report Generation
- Audit Trail
- Class of Service
- Active Configuration
- Offline Configuration
- Auto Attendant
- FPSA Management
- Utlities

26.69 Overview

This section describes the billing function and gives the requirements for configuring the billing function. Billing reports are summarized in this section, but the Reports section has more complete information about them. Information covered in this section includes:

- Setting rates
- Gathering billing data
- Billing reports
- Configuration requirements

About Billing

The billing function collects statistics about NuPoint Unified Messaging server usage and calculates charges for that usage. You can set a low-usage rate and a high-usage rate for each statistic. This rate-setting arrangement gives you the option to charge fixed rates, give volume discounts, or charge for heavy use. During day-to-day server operation, over 120 different statistics can be kept for each mailbox, grouped into these six categories:

- Mailbox access
- Base rates
- Connect time
- Disk usage
- Messages received
- Network rates
- Pager calls

You can configure the server to perform a gather of these statistics, then obtain billing reports generated by the server from the resulting information.

Billing Reports

After the server performs a gather, the statistics and charges that are calculated go into four types of billing reports that the server can generate. Each report gives a breakdown of charges for individual mailboxes by statistics, then calculates the total amount that is due. Each report has a different purpose. Samples of these reports and explanations of their contents are contained in the Reports section.

26.69.1 Configuration Requirements for Billing

Configuring for billing involves obtaining a report of current rates, using a Billing Worksheet, and adjusting rates, if necessary.

Current Billing Rates

You can use Text console reports to see what the current rates are for various statistics, such as base rates and pager calls. In the Web console, you can view all current rates on the Billing Rates page.

Use these options to see what the low usage and high usage rates are and what the low/high boundary is for each statistic in the categories mentioned earlier. When configuring for billing, you should check these figures to help you determine which rates to set or adjust. If you are setting rates for many of the server usage activities, you should also use the report of current rates as an extension of the Billing Worksheet, marking it up to show the rates for all the various server usage activities desired.

Billing Worksheet

Complete one Billing Worksheet for each line group. For all rates except Base Rates, specify the Low rate, the High rate, and the Boundary (the point at which the High rate applies).

The Billing Worksheet has two pages. Be sure you complete both pages when working on Billing Rates. Blank worksheets are located in Worksheets section. A sample Billing Worksheet is shown here:

Billing Worksheet, Page 1 of 2

	RATE		
Messages Received	**Low Usage**	**Boundary**	
Messages received from users	0.500	20	
Messages received from callers	0.700	10	
Messages future deliveries			
Call placement per minute rate (Connect Time)			
Call placement per call rate			
Urgent messages received from callers			
Auto wakeups or TAS messages			
Receipt requests			
Disk usage, (Disk Usage)			
Network Billing			
Network messages sent	0.000	0	
Network urgent messages sent	1.000	5	
Network messages received			
Network urgent messages received			
Number of network nodes sent to			
Number of network nodes sent urgent			
Number of remote network recipients			
Number of remote network recipients urgent			
Message length network sent			
Message length urgent network sent			
Message length network received			
Message length urgent network received			
Message length, number of nodes sent			
Msg. length, number of nodes sent urgent			
Message length, number of remote recipients			
Message length, number of remote recipients urgent			
Messages Received (fax)			
Number of fax messages received	0.050	30	
Number of fax messages sent			
Number of fax retrieval			

Billing Worksheet, Page 2 of 2

Mailbox Accesses

Connect T

Line Group	Greeting Rate			Login Rate			User Connect Time			
	Low	Bound	High	Low	Bound	High	Low	Bound	High	
1	0.002	10	0.000	0.000	0	0.000	0.001	50	0.002	0
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

Pager Billing

Pager No.	Low	Bound	High	Pager No.	Low	Bound	High
0	0.050	10	0.120	8			
1	0.030	15	0.200	9			
2				10			
3				11			
4				12			
5				13			
6				14			
7				15			

Base Rates

FCOS	Rate	FCOS	Rate	FCOS	Rate	FCOS	Rate
1	0.200	17	0.050	33	0.100	49	0.250
2	0.200	18		34		50	
3	0.400	19		35		51	
4		20		36		52	

Mailbox Accesses

There are two types of mailbox access for which you can bill: logins and greetings (number of times greeting was played), and you can set a low usage rate, high usage rate, and a low/high boundary for each type. The two types are shown on the worksheet and in the Billing Categories table at the bottom of this page.

The rates you set for mailbox access apply to all calls through the specified port (line) group.

Base Rates

As mentioned earlier in this section, a base rate is a flat fee that is charged at every billing period. You must set a rate for each FCOS that you want to bill. You can only differentiate among the first 64 FCOS; any FCOS higher than 64 is billed at the rates for FCOS 64.

Connect Time

There are three connect time statistics that you can bill for: user connect time, caller connect time, and call placement connect time. These statistics are accumulated in the same way, but you can have a different set of rates for each port (line) group in the server. These statistics measure off-hook to on-hook phone line usage.

- **User connect time** is the time used by the mailbox owner to pick up messages and/or to make messages for other mailbox owners. The rates you set for user connect time apply to all calls through the specified port (line) group.
- **Caller connect time** is the time charged when outside callers leave messages in a mailbox or listen to the greeting of a Greeting-Only mailbox. The rates you set for caller connect time apply to all calls through the specified port (line) group.
- **Call placement connect time** is the amount of time required to place an off-server call, including any greeting a caller hears. The low-usage rate and high-usage rate applies to all line groups. The rates you set for call placement connect time apply to the entire server.

Measurement Method

Connect time other than call placement connect time is measured in tenths of minutes (6 seconds), rounded up if not exact. Call placement connect time is measured in one-minute units. This statistic can increment to about 109 hours before the accumulator restarts at zero. This is equivalent to about 3.5 hours per day for a month.

Calculation of Charges

When charges are calculated, they are based on minutes of connect time, rather than tenths of a minute. This is to allow rates, which are precise to $0.001, to be adjusted by small amounts.

Disk Usage

The disk usage statistic is calculated as follows: the message size multiplied by the time on disk.

Measurement Method

Message size is measured in tenths of a minute (6 seconds), rounded up if not exact. Time on disk is measured in hours, rounded up to the next hour, and is calculated when the message is deleted from the server.

The disk usage statistic resets to zero after 16,777,215 units of usage (one unit equals one-tenth of a minute multiplied by 1 hour of storage). This is equivalent to keeping three hours of speech for 1 year.

Calculation of Charges

Users typically accumulate several thousand units of disk usage per month, unless they delete messages immediately after they are received. If the rate were applied to the usage as accumulated, a rate of $.001 would be a significant charge, and the only way the rate could be changed would be to double it. Therefore, when charges are calculated, disk usage values are divided by one hundred, and the rate is specified to the nearest mil per minute of speech that has been kept for ten hours.

Other factors in the calculation of charges are:

- A user is not billed for messages that have not been deleted at the time that billing data are gathered. These messages are eventually deleted, however, and the charges are greater, since the time on disk has increased.
- No disk usage is accumulated for names or greetings. Charges for these can be included in the base rates.
- If a message is made with a distribution list, each mailbox that receives the message is charged for it.
- If a user gives a message, with comments, to another user, the sender is charged for the original message for as long as it remains on the server. The recipient is charged disk usage for both the original message, and for the comments, until each is deleted from the mailbox.

Messages Received

Every time a message is left in a mailbox, one of 14 statistics is incremented for that mailbox. Each message statistic can accumulate up to 4095 messages before it resets to zero. This is equivalent to 132 messages per day, for a month.

User message count increments in two ways:

- When a caller phones his/her own mailbox and “makes a message” for another mailbox, the recipient’s mailbox counter increases.
- When a user “gives” a message, with comments, to another mailbox, the counter of the recipient mailbox increases by one. (The message, plus the comments, are counted as one message.)

Caller message count increments in several ways:

- When a caller phones into the server directly and leaves a message.
- When a greeting is delivered for a Greeting-Only mailbox. This includes times when the mailbox owner logs into his mailbox by pressing the star (*) key while the greeting is playing.
- When a caller phones into the server directly and leaves an urgent message.
- When a caller phones into the server directly, leaves a message, and requests a receipt response.

Network Rates

Network rates that can be set are grouped as message counts and message lengths.

Network message counts include messages sent, messages sent urgent, messages received, and messages received urgent. Network message lengths include messages sent, messages sent urgent, messages received, and messages received urgent. See the table below for a complete list of network rate statistics.

Pager Calls

Pager call rates are set by pager system, not by individual pager. Pagers that have the same access code index are on the same pager system. In the Billing Report, charges for pager calls are listed by line group.

Each time a successful page is issued, a counter increments in the mailbox. This does not necessarily correspond to the number of messages received. If two messages are received at the same time, only one page is made. If a message is not picked up within a selected period (the pager interval, which was configured when the mailbox was created), the server re-pages, if the mailbox pager frequency (which also was configured when the mailbox was created) is greater than 1. Each re-page is counted as a separate page.

Unsuccessful re-pages are not counted in the mailbox statistics.

Adjusting Pager Call Rates in Mid-Cycle

The rate at which a page is billed depends on the access code index (the Pager System number) that is in the mailbox setup at the time the gather is done, not the one that is present at the time the page is made. If the access code index or the billing rate is changed in the middle of the billing period, all pages that were accumulated during the billing period are billed at the new rate.

Termination of Paging

When paging service is discontinued in the middle of the billing period, there is no access code index in the mailbox at the time of billing and, therefore, no pages are billed, even if some have accumulated. To avoid this situation, generate a Termination Report (described earlier) before modifying the mailbox. This calculates the amount due without changing the statistics in the mailbox; the other charges are correct at the regular billing.

Low Usage Rates, Low/High Boundary, High Usage Rate

The rates and boundary specified apply to all pagers in the specified pager system.

Message Delivery Billing Considerations

The server is capable of billing both paging and message delivery on a per-page basis. However, keep in mind that the server installation site, as the calling party, is responsible for any charges that accrue when paging or message delivery calls are made to the outside telephone network. While pager calls are usually very short, message delivery calls can be quite long. Since the cost of each call depends on the time of day that it was made, the duration of the call, the distance to the user, and the rates of the local telephone company, the server makes no provisions for this aspect of the billing.

The billing rates structure does allow you to specify an individual rate for each pager system. This rate is multiplied by the number of pages that are issued for the mailbox. If you put message delivery accounts and radio pager accounts on separate pager systems, you can increase the charges on the pager systems that service message delivery subscribers to compensate for any toll charges that the telephone company levies.

Adjusting Rates

You can set, adjust, or leave as is a low usage rate, low/high boundary rate, and high usage rate for each of the statistics in the billing categories on the worksheet. Billing categories are defined here:

Category	Statistics Calculated and Reported
Mailbox accesses	**Logins Greets**
Base rates	**FCOS usage by FCOS number (1-64 only)**
Connect time (by line group)	**User connect time Caller connect time Call placement connect time**
Disk usage	**Disk usage units (length of messages**x time on disk)
Messages received	**User messages Caller messages Call placement messages Future delivery messages Urgent messages Wakeup messages Receipt responses messages**
Network rates (applicable if the NP Net optional feature is installed)	**Network messages sent Network urgent messages sent Number of network nodes sent to Number of network nodes sent urgent to Number of remote network recipients sent to Number of remote network recipients sent urgent to Network messages received Network urgent messages received Message length for network messages sent Message length for network messages sent urgent Message length for network messages received Message length for urgent network received Message length for number of network nodes sent Message length for number of network nodes sent urgent Message length for number of remote recipients sent Message length for number of remote recipients sent urgent**

Category	Statistics Calculated and Reported
Network rates (applicable if the NP Net optional feature is installed)	**Network messages sent Network urgent messages sent Number of network nodes sent to Number of network nodes sent urgent to Number of remote network recipients sent to Number of remote network recipients sent urgent to Network messages received Network urgent messages received Message length for network messages sent Message length for network messages sent urgent Message length for network messages received Message length for urgent network messages received Message length for number of network nodes sent Message length for number of network nodes sent urgent Message length for number of remote recipients sent Message length for number of remote recipients sent urgent**
Pager Calls	**Successful pages issued**

26.69.2 Set Billing Rates

During day-to-day system operation, 120 different statistics are kept for each mailbox, including mailbox access counters, message counters, connect time accumulators, disk usage accumulation, and page counter. For each statistic, different rates can be set for high and low usage, and for a boundary. This tiered rate system gives you the option to charge set rates or to give volume discounts.

- **Low usage rate** is the rate charged, up to the boundary number. A 0 (zero) prevents this rate from appearing on the Billing Report.
- **High usage rate** is the rate charged after the boundary number is reached. If you want to use this rate, be sure to enter a boundary.
- **Boundary** is where the rate changes from the low usage rate to the high usage rate. A 0 (zero) means all usage is charged at the low rate.

If you need to enter new billing rates or adjust existing rates the system's various counters and accumulators determine the charges. A different billing rate can be set for each resource counter.

Set Billing Rates for Each Counter

You can set billing rates for each counter. With the exception of Base rates, which are flat fees, you can enter a separate high and low usage rate, along with a boundary rate, for each resource (See About Resource Counters).

To give volume discounts, enter a lower amount for the high usage rate than for the low usage rate. To penalize heavy usage, enter a higher amount for the high usage rate. Boundary values are charged at the lower rate. Each boundary value is set in the same unit as the individual resource. To charge a standard rate, enter 0 (zero) in the boundary number field.

You can also generate reports of the current rates. See the Reports section for more information.

26.69.3 About Resource Counters

Each mailbox has resource counters. The billing system allows you to charge a base rate and set two-tiered separate rates for each counter, if required. Rates for the following resources are discussed here:

• Base Rates • Mailbox Accesses • Logins • Greetings Accesses • Connect Times	• Disk Usage • Messages Received • Pager Calls • Network Rates

Base Rates

A base rate is a flat fee charged at every billing period. The system prompts you to set a base rate for each FCOS. The rate set for any FCOS can be any value between $0.00 and $327.67, precise to $0.01; it can be pro-rated for a portion of the billing cycle.

Mailbox Accesses

There are two different mailbox access counters: (a) login rates, and (b) greeting rates. Although each mailbox has mailbox access counters, these counters are designed specifically for billing Information-only mailboxes. Information-only mailboxes have an FCOS that **does not** allow them to receive messages (for example, chain and greeting-only mailboxes).

Other resource counters that may be increased for Information-only mailboxes are the "user connect" time and the "caller connect" time. A base rate can also be set.

Login Rates Counters

Login rates counters track the number of times the user logs into the mailbox. A different rate may exist for each port or line group on the system.

Greeting Rates Counters

Greeting rates counters track the number of times that the mailbox greeting plays (that is, the number of times that the mailbox is accessed by an outside caller). A different rate may exist for each port or line group on the system. **Note**: The caller does not have to listen to the entire greeting for this counter to be increased.

Connect Times

Two connect time accumulators measure phone line usage (off-hook to on-hook).

User Connect Rates

User connect rates measure the time used by the mailbox owner to pick up messages and make messages for other users. A different rate may exist for each port or line group on the system.

Caller Connect Rates

Caller connect rates measure the time charged when outside callers leave messages in a mailbox, or listen to the greeting of an Information-only mailbox.

Note:

- Counter is not increased when a message is left by a TAS (Telephone Answering Service) operator using the Message Attendant application. There is no way to associate TAS operator time with any particular mailbox—other than by the number of messages left by TAS operators.
- Different rates may exist for each port or line group on the system.

Measurement Method and Limitations of the "Connect Time" Counter

Connect time is measured in tenths of minutes (6 seconds), rounded up if not exact. Each counter allows 109 hours—about 3.5 hours per day for a month—before the accumulator restarts at zero.

Calculation of Charges

When charges are calculated, they are based on minutes of connect time (rather than tenths of a minute). This calculation allows rates (which are in mils) to be adjusted by small amounts.

Disk Usage

Disk usage is the size of the message, multiplied by the length of time the message stays on the system.

Measurement Method and Limitations of the "Disk Usage" Accumulator

Time on disk is measured in hours rounded up to the next hour, and is calculated when the message is deleted from the system. The disk usage accumulator resets to zero after 16,777,215 units of usage—equivalent to keeping three hours of speech for one year.

Calculation of Charges

Users typically accumulate several thousand units of disk usage per month, unless they delete messages immediately after they are received. If the rate is applied to the usage as accumulated, a rate of $.001 would be a significant charge, and the only way the rate could change would be to double it. Therefore, when charges are calculated, disk usage values are divided by one hundred, and the rate is specified to the nearest mil-per-minute of speech kept for 10 hours.

- Users are not billed for messages not deleted at the time billing data is gathered. These messages will eventually be deleted, however, and the charges will increase, because the time on the disk will have increased.

- Disk usage for names or greetings is not accumulated. Charges for these can be included in the base rates.

- If a message is made with a distribution list, each mailbox receiving the message is charged for it.
- If a user sends a message with comments to another user, the sender is charged for the original message for as long as it remains on the system. The recipient is charged disk usage for both the original message and for the comments until each is deleted from the mailboxes.

Messages Received

Every time a message is left in a mailbox, a counter is increased for that mailbox for each of the following categories:

• user messages • caller messages • call placement messages • future delivery messages • urgent messages • wakeup/tas messages • receipt response messages • fax received messages	• fax sent messages • fax retrieval non-billed messages • fax retrieval billed messages • fax undelivered messages • fax pages received messages • fax pages sent messages • fax pages retrieval non-billed messages • fax pages retrieval billed messages

User Messages Counters

User messages counters are increased in two ways:

- When a caller phones his or her own mailbox and "makes" a message for another mailbox, the recipient’s mailbox counter increases.
- When a user "gives" a message with comments to another mailbox, the recipient’s mailbox counter increases by one (message plus comments are counted as one message).

Caller Messages Counters

Caller messages counters are increased in several ways:

- When a caller phones into the system directly and leaves a message.
- When a caller leaves a message in the attendant’s mailbox and the attendant forwards the message.
- When a greeting is delivered for a Greeting-only mailbox. Including times when the mailbox owner logs into his mailbox by pressing the * key (star) while the greeting is playing.
- When a caller phones into the system directly and leaves an urgent message.
- When a caller phones into the system directly and requests a receipt response.

TAS Operator Messages Counters

TAS operator messages counters increase when a TAS operator leaves a message via one of the open ports set up by the Message Attendant application.

Limits of the "Messages Received" counter

Each message counter can accumulate up to 4,095 messages—132 messages per day for a month—before it resets to zero.

Pager Calls

Each time a successful page is issued, a counter is increased in the mailbox, however, this does not necessarily correspond to the number of messages received.

- If two messages are received at the same time, only one page is made.
- If a message is not picked up within the set pager **interval** (a selected amount of time programmed when the mailbox was created), the system re-pages.
- If the mailbox pager **frequency** (programmed when the mailbox was created) is greater than one, every re-page is counted as a separate page.

Pager call rates are set by the Pager System, not by an individual pager. Pagers with the same pager outdial index (also known as the access code index) belong to the same pager system. See Pagers and Message Delivery for more information.

Adjusting Pager Call Rates in Mid-cycle

The rate at which a page is billed depends on the pager outdial index—representing the pager system access code—programmed into the mailbox at the time the "Gather" is performed, and **not** the rate present at the time the page is made. If the pager outdial index or the billing rate are changed in the middle of the billing period, all pages accumulated during the billing period are billed at the new rate.

Termination of Paging

When paging service is discontinued in the middle of the billing period, an outdial index does not appear in the mailbox at the time of billing. Therefore, **no** pages are billed even if some have accumulated. To avoid this situation, run a Termination Report before modifying the mailbox. This report calculates the amount due without changing statistics in the mailbox. Other charges are corrected at the regular billing. See the Reports section for instructions to run the Termination Report.

Network Rates

Billing rates can be set for network usage, including the following:

Network Message Counters

- messages sent; urgent messages sent
- network nodes sent to; network nodes sent urgent to
- recipients sent to; recipients sent urgent to
- messages received; urgent messages received

Network Message Length Counters

- messages sent; urgent messages sent
- messages received; urgent messages received
- network nodes sent; network nodes sent urgent
- remote recipients sent to; remote recipients sent urgent to

Network rates can be set for any/each of the following categories:

• Network messages sent • Network urgent messages sent • Number of network nodes sent to • Number of network nodes sent urgent to • Number of remote network recipients sent to • Number of remote network recipients sent urgent to • Network messages received • Network urgent messages received	• All message length rates are per .1 minutes of messages • Message length for network messages sent • Message length for network messages sent urgent • Message length for network messages received • Message length for urgent network received • Message length for number of network nodes sent • Message length for number of network nodes sent urgent • Message length for number of remote recipients sent • Message length for number of remote recipients sent urgent

26.70 Gathering Data

Before the server can produce billing reports, data must be gathered from the statistics that have been specified. Gathering data is a three-step process:

1. The current billing data file, which was created during the last gather, becomes the new previous billing data file. The server issues a warning because this step overwrites (and thereby destroys) the previous billing data file, which was also created during the last gather.
2. The server scans the statistics in all the mailboxes. The data that is collected becomes the new current billing data file.
3. The data gathered in step 1 is subtracted from the mailbox statistics. This update zeros the statistics in all the mailboxes (unless there was mailbox activity between steps 2 and 3 to prepare them for the next billing cycle.

When you run a billing report, the value that is obtained during the gather for each statistic in a mailbox is multiplied by the billing rate that you assigned to that statistic. The server then adds the charges for all statistics with billing rates greater than zero, plus any base rate that you may have specified, to give a total charge for each mailbox.

All billing data older than the previous billing data file is available using the regular backup procedures.

26.70.1 Perform a Manual Gather

To perform a manual or single gather:

1. In the navigation tree, click Report Generation, then click Billing, and then click Billing Gather.

   The Billing Gather form opens.
2. Click Gather Now!.

26.70.2 Configure an Automatic Gather

Once the Automatic Billing Gather is configured and saved, you can close the Web Console session. The Automatic Gather will be performed as long as the Web Console application and the NuPoint Unified Messaging server are running.

To configure an automatic gather:

1. In the navigation tree, click Report Generation, then click Billing, and then click Billing Gather. The Billing Gather form opens.
2. Configure the Billing Gather form.
3. To save your Automatic Gather configuration, click Save.

26.70.3 Set Billing Rates

You must set Billing Rates before you can gather billing information and run a Billing Report.

You can configure billing for the following eight categories of billing rates:

- Mailbox Access
- Base Rates
- Connect Time
- Disk Usage
- Messages Received
- Fax Messages
- Network Rates
- Pager Calls

To set Billing Rates:

1. In the navigation tree, click Report Generation, then click Billing, and then click Billing Rates.
2. Configure rates for one or more of the billing categories in the Billing Rates form.
3. Click Save.

26.70.4 Billing Gather Form

You use the Billing Gather form to configure periodic, automatic billing gathers on the NuPoint Unified Messaging system.

Billing Gather Form Field Descriptions

Field	Description	Values/Notes
Automatic Gather		
Never	Disables automatic gather.	N/A
Weekly	Enables automatic gather to occur once a week at the times specified in the When to Gather section below.	The gather will occur once a week, at the selected Hour of Day, on the Day that is selected.
Twice Monthly	Enables automatic gather to occur twice a month at the times specified in the When to Gather section below.	The gather will occur twice a month, at the selected Hour of Day, on the days selected for the First Day and the Second Day. If you select a value for the first day, the GUI will automatically advance the Second Day setting by a day. You can then change the day.
Monthly	Enables automatic gather to occur once a month at the times specified in the When to Gather section below.	The gather will occur once a month, at the selected Hour of Day, on the Day selected.
When to Gather		
Hour of Day		Hour of Day range is from 01:00 - 12:00, AM and PM.
Weekday		For Weekly, select the day of the week from the drop-down list
First Day		For Monthly and Twice Monthly, Days are numbered 01-28.
Second Day		Same as First Day.

Billing Gather Form Button Actions

Button	Action
Save	Saves the configuration.
Gather Now!	Immediately gathers the data for the mailbox.

26.70.5 Billing Rates Form

You use the Billing Rates form to set mailbox billing rates.

There are eight tabs available on this form, one for each of the eight different billing categories:

- Base Rates
- Mailbox Accesses
- Connect Time
- Disk Usage
- Messages Received
- Fax Messages
- Network
- Pager Calls

Daily statistics are generated for each billing category. For each statistic, different rates can be set for high and low usage, and for a boundary. This tiered-rate system gives you the option to charge set rates or to give volume discounts.

- Low usage rate is the rate charged, up to the threshold number. A 0 (zero) prevents this rate from appearing on the Billing Report.
- High usage rate is the rate charged after the threshold number is reached. If you want to use this rate, be sure to enter a boundary.
- Threshold is where the rate changes from the low usage rate to the high usage rate. A 0 (zero) means all usage is charged at the low rate.

You can enter new billing rates or adjust existing rates, and the system determine the charges. A different billing rate can be set for each resource counter.

Base Rates Fields Description

The Base rates are flat fees that are charged at every billing period. The base rates are set for each FCOS. All named, programmed FCOS are displayed in the form with their base rates. You can only differentiate among the first 64 FCOS; any FCOS higher than 64 is billed at the rates for FCOS 64.

Fields	Values
FCOS	Max. 640 – only named FCOS are displayed (**Note**: You can create unnamed FCOS using the Text console but they are not supported in the Web console. If you encounter an unnamed FCOS, use the Text console to name it.)
Rates	Range ($0.00 - $654.99). Default value $0.00

Mailbox Accesses Fields Description

Although each mailbox has mailbox access counters, the login rates and greeting rates are designed specifically for billing information-only mailboxes. For each line group the Logins and Greets can be configured through this form. The rates you set for mailbox access apply to all calls through the specified port (line) group.

Login rates counters track the number of times the user logs into the mailbox. Greeting rates counters track the number of times that the mailbox greeting plays (that is, the number of times that the mailbox is accessed by an outside caller).

Fields	Values
Line Group Number	Max.24 – Only the ones that are programmed will be shown.
Logins	Low and High Usage: Range ($0.00 -$64.99). Default is $0.00. Threshold: 0 – 65535. Default is 0.
Greets	

Connect Time Fields Description

For each line group the User connect time, Caller connect time and Call placement connect time can be configured. There are three connect time statistics that you can bill for: user connect time, caller connect time, and call placement connect time. All these statistics are accumulated in the same way, but you can have a different set of rates for each port (line) group in the server. These statistics measure off-hook to on-hook phone line usage.

- User connect time is the time used by the mailbox owner to pick up messages and/or to make messages for other mailbox owners. The rates you set for user connect time apply to all calls through the specified port (line) group.

- Caller connect time is the time charged when outside callers leave messages in a mailbox or listen to the greeting of a Greeting-Only mailbox. The rates you set for caller connect time apply to all calls through the specified port (line) group.
- Call placement connect time is the amount of time required to place an off-server call, including any greeting a caller hears. The low-usage rate and high-usage rate applies to **all** line groups. The rates you set for call placement connect time apply to the entire server.

Measurement Method

Connect time other than call placement connect time is measured in tenths of minutes (6 seconds), rounded up if not exact. Call placement connect time is measured in one-minute units. This statistic can increment to about 109 hours before the accumulator restarts at zero. This is equivalent to about 3.5 hours per day for a month.

Calculation of Charges

When charges are calculated, they are based on minutes of connect time, rather than tenths of a minute. This is to allow rates, which are precise to $0.001, to be adjusted by small amounts.

Fields	Values
Line Group Number	Max.24 – Only the ones that are programmed will be shown.
User connect time	Low and High Usage: Range ($0.00 -$64.99). Default is $0.00. Threshold: 0 – 65535. Default is 0.
Caller connect time	
Call placement connect time	

Disk Usage Fields Description

Measurement Method

The disk usage statistic is calculated as follows: the message size multiplied by the time on disk. Message size is measured in tenths of a minute (6 seconds), rounded up if not exact. Time on disk is measured in hours, rounded up to the next hour, and is calculated when the message is deleted from the server.

The disk usage statistic resets to zero after 16,777,215 units of usage (one unit equals one-tenth of a minute multiplied by 1 hour of storage). This is equivalent to keeping three hours of speech for 1 year.

Calculation of Charges

Users typically accumulate several thousand units of disk usage per month, unless they delete messages immediately after they are received. If the rate were applied to the usage as accumulated, a rate of $.001 (one mil) would be a significant charge, and the only way the rate could be changed would be to double

it. Therefore, when charges are calculated, disk usage values are divided by one hundred, and the rate is specified to the nearest mil per minute of speech that has been kept for ten hours.

Other factors in the calculation of charges are:

- A user is not billed for messages that have not been deleted at the time that billing data is gathered. These messages are eventually deleted, however, and the charges are greater, since the time on disk has increased.
- No disk usage is accumulated for names or greetings. Charges for these can be included in the base rates.
- If a message is made with a distribution list, each mailbox that receives the message is charged for it.
- If a user gives a message, with comments, to another user, the sender is charged for the original message for as long as it remains on the server. The recipient is charged disk usage for both the original message, and for the comments, until each is deleted from the mailbox.

Fields	Values
Disk usage units (excluding Fax)	Low and High Usage: Range ($0.00 -$64.99). Default is $0.00. Threshold: 0 – 65535. Default is 0.
Fax disk usage units	

Messages Received Fields Description

Every time a message is left in a mailbox, one of 14 statistics is incremented for that mailbox. Each message statistic can accumulate up to 4095 messages before it resets to zero. This is equivalent to 132 messages per day, for a month.

User messages are incremented in two ways:

- When a caller phones his/her own mailbox and “makes a message” for another mailbox, the recipient’s mailbox counter increases.
- When a user “gives” a message, with comments, to another mailbox, the counter of the recipient mailbox increases by one. (The message, plus the comments, are counted as one message.)

Caller messages are incremented in several ways:

- When a caller phones into the server directly and leaves a message.
- When a greeting is delivered for a Greeting-Only mailbox. This includes times when the mailbox owner logs into his mailbox by pressing the star (*) key while the greeting is playing.
- When a caller phones into the server directly and leaves an urgent message.
- When a caller phones into the server directly, leaves a message, and requests a receipt response.

Fields	Values
User messages	Low and High Usage: Range ($0.00 -$64.99). Default is $0.00. Threshold: 0 – 65535. Default is 0.
Caller messages	
Call replacement messages	
Future delivery messages	
Urgent messages	
Wakeup messages	
Receipt responses	

Fax Messages Fields Description

Fields	Values
Received messages	Low and High Usage: Range ($0.00 -$64.99). Default is $0.00. Threshold: 0 – 65535. Default is 0.
Sent messages	
Retrieval non-billed messages	
Retrieval billed messages	
Undelivered messages	
Pages received	
Pages sent	

Fields	Values
Pages retrieved non-billed	
Pages retrieved billed	

Network Fields Description

Network rates that can be set are grouped as message counts and message lengths.

Network message counts include messages sent, messages sent urgent, messages received, and messages received urgent. Network message lengths include messages sent, messages sent urgent, messages received, and messages received urgent.

Fields	Values
Messages sent	Low and High Usage: Range ($0.00 -$64.99). Default is $0.00. Threshold: 0 – 65535. Default is 0.
Messages sent urgent	
Messages sent per node	
Messages sent urgent per node	
Messages sent urgent to remote recipient	
Messages received	
Message Length/Sent	
Message Length/Sent Urgent	
Message Length/Received Urgent	
Message Length/Sent per node	

Fields	Values
Message Length/Sent urgent per node	
Message Length/Sent to remote recipient	

Pager Calls Fields Description

Each time a successful page is issued, a counter is incremented in the mailbox.

Pager call rates are set by pager system, not by individual pager. Pagers that have the same access code index are on the same pager system. Once the Pager system number is selected it will show the related rates for successful pages for that Pager System. In the Billing Report, charges for pager calls are listed by line group. For more information about Pager Systems, see the *System Administration Help*.

Each time a successful page is issued, a counter is incremented in the mailbox. This does not necessarily correspond to the number of messages received. If two messages are received at the same time, only one page is made. If a message is not picked up within a selected period (the pager interval, which was configured when the mailbox was created), the server re-pages, if the mailbox pager frequency (which also was configured when the mailbox was created) is greater than 1. Each re-page is counted as a separate page.

Unsuccessful re-pages are not counted in the mailbox statistics.

Adjusting Pager Call Rates in Mid-Cycle

The rate at which a page is billed depends on the access code index (the Pager System number) that is in the mailbox setup at the time the gather is done, not the one that is present at the time the page is made. If the access code index or the billing rate is changed in the middle of the billing period, all pages that were accumulated during the billing period are billed at the new rate.

Termination of Paging

When paging service is discontinued in the middle of the billing period, there is no access code index in the mailbox at the time of billing and, therefore, no pages are billed, even if some have accumulated. To avoid this situation, run a Billing Report and check the Termination Data before modifying the mailbox. This calculates the amount due without changing the statistics in the mailbox; the other charges are correct at the regular billing.

Low Usage Rates, Low/High Threshold, High Usage Rate

The rates and boundary specified apply to all pagers in the specified pager system.

Message Delivery Billing Considerations

The server is capable of billing both paging and message delivery on a per-page basis. However, keep in mind that the server installation site, as the calling party, is responsible for any charges that accrue when paging or message delivery calls are made to the outside telephone network. While pager calls are usually very short, message delivery calls can be quite long. Since the cost of each call depends on the time of

day that it was made, the duration of the call, the distance to the user, and the rates of the local telephone company, the server makes no provisions for this aspect of the billing.

The billing rates structure does allow you to specify an individual rate for each pager system. This rate is multiplied by the number of pages that are issued for the mailbox. If you put message delivery accounts and radio pager accounts on separate pager systems, you can increase the charges on the pager systems that service message delivery subscribers to compensate for any toll charges that the telephone company levies.

Adjusting Rates

You can set, adjust, or leave as is a low usage rate, low/high threshold, and high usage rate for each of the statistics in the billing categories on the worksheet.

Fields	Values
Pager System Number	16 - one selected at a time
Low Usage and High Usage	Range ($0.00 -$64.99). Default is $0.00.
Threshold	Range is 0 – 65535. Default is 0.

26.71 Check Current Billing Rates

This procedure describes how to check the current rates for various statistics that the server uses to generate billing reports. These are:

• Base Rates	• Connect Time Rates
• Mailbox Access Rates	• Network Rates
• User and Caller Message Rates	• Call Placement, Future Delivery, Urgent, Wakeup Rates
• Disk Usage Rates	• Receipt Processing Rates
• Pager Call Rates	

To check current rates:

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, **(A) Adjust Rates**,and then **(R) Report Rates**.
2. Select the options for the statistics you want to check, as described in the following sections:

To Check Base Rates (Keyed to FCOS)

- Select **(B) Base Rates**. The server displays a list of all FCOS in numerical order and the current rate for each.

Note:
FCOS from 65 to 640 are billed and reported at the rates for FCOS 64.

To Check Connect Time Rates

1. To view rates for **caller connect** time, select **(C) Caller Connect Rates** and enter the port group number to report. The server displays the current low usage rate, low/high boundary, and high usage rate, by line (port) group.
2. To view rates for **user connect** time, select **(U) User Connect Rates**. No response is necessary. The server displays the current low usage rate, low/high boundary, and high usage rate, by line (port) group.
3. To view rates for **call placement connect** time, select **(O) Other Rates**. No response is necessary. The server displays the current low usage rate, low/high boundary, and high usage rate under "Connect Time."

To Check Mailbox Access Rates

1. To view rates for **greetings**, select **(G) Greeting Rates**. The server displays the current low usage rate, low/high boundary, and high usage rate, by line (port) group.
2. To view rates for **logins**, select **(L) Logins Rates**.

To Check Network Rates

- To check Network rates, select **(N) Network Rates**. The server displays the current low usage rate, low/high boundary, and high usage rate, by line (port) group, for Network message counts and Network message lengths.

To Check Rates for Pager Calls

- To view rates for pager calls, select **(P) Pager Calls**. The server displays the current low usage rate, low/high boundary, and high usage rate for supported pager systems by access code.

To Check Other Rates

To check any of the following rates, select **(O) Other Rates**:

- User and Caller Messages

- Call Placement, Future Delivery, Urgent, or Wakeup Messages
- Receipt Processing
- Disk Usage

26.71.1 Perform a Gather

Before the system can bill mailboxes, it must gather data from all mailbox counters. Gather is a three-step process that performs the following tasks:

1. The **current billing data file (**created during the last Gather), becomes the *new* **previous billing data file**. This step overwrites (and thus destroys) the *old* previous billing data file, also created during the last Gather; the system issues a warning.
2. The system scans the counters and accumulators in all mailboxes. The data collected becomes the *new* **current billing data file**.
3. The data gathered in Step 2 is subtracted from the mailbox counters. This update zeros the counters in all mailboxes to prepare them for the next billing cycle (unless mailbox activity occurs between Steps 2 and 3).

While the billing report is running,

- The value obtained during the Gather for each counter in a mailbox is multiplied by the billing resource rate you assigned to that counter.
- The system adds charges for all resources with billing rates greater than zero, plus any base rate you may have specified.
- A total charge for each mailbox is provided.

You can perform a Gather manually, or you can configure the system to perform a Gather automatically.

To Run a Single Gather (Manually)

1. From the Main menu, select select **(R) Report Generation**, and then **(B) Billing.**
2. Select **(G) Gather Data**. The system displays the date of the last Gather, and responds: **Warning!!** This will destroy previous billing data. Type "gather" if you really want to do this.
3. Type **gather; OR** press **Enter** to cancel. The system displays status messages: Please wait...gathering data... gathering complete... starting update... <number> mailboxes updated.

When the system displays the number of mailboxes updated:

- Gather is complete
- Counts of all statistics are set to zero (0)
- Any billing report you obtain is current, as of this Gather

Note:
If you did not receive both **gathering complete** and **<number> mailboxes updated** prompts, see "If Gather Fails", below.

If Gather Fails

It is possible for a Gather to be unsuccessful. The most likely cause is a power loss during the process because Gather can take several minutes to complete. If your Gather fails, use the following procedure to determine your billing:

1. Perform a backup. (See the NuPoint UM Technician's Handbook for instructions.)
2. Perform another Gather. The information needed for the current billing is now divided between the current and previous billing data files on the hard disk.
3. Run a Previous Billing Report. This report shows what was billed during the last billing cycle and gives a starting point for determining current charges.
4. Run a Billing Report and a Previous Billing Report from the **hard disk**. Manually determine which report has the correct bill for each mailbox.

26.71.2 Auto Gather

Auto Gather allows the system to be configured to automatically perform weekly, monthly, or bimonthly gathers.

To Configure Auto Gather

Note:
This procedure makes changes to the inactive configuration. You must activate the inactive configuration for the changes to take effect.

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, **(G) Offline Menu**.
2. Select **(B) Duplicate Active Configuration**. The system copies the current (active) configuration. Steps 3 through 7 and additional configuration entries affect only the copy; entries take effect **only after** you activate the configuration.
3. Select **(S) Auto Task Menu** and then **(A) Gather - System Billing**.
4. If you are enabling weekly gather, select **(W) weekly Gather menu** and configure **(D) Day to do Gather**, and **(H) Hour to do Gather** (0 = midnight, 12 = noon).

5. Select **(E) Enable Auto Gather (weekly/monthly/no) (W/M/N)** and enter
   - **W** to enable a weekly Gather
   - **M** to enable a monthly (or twice-monthly) Gather
   - **N** to disable Auto Gather
6. If you are enabling **monthly** (or bi-monthly) Gather, select **(M) Monthly Gather** menu and configure the following:
   - Day of month to do first gather (1-28)
   - Day of month to do second gather (1-28) (For bi-monthly gathers)
   - Hour to do gather (0-23)
   - Second auto gather enabled? Y/N (Enter **Y** to perform a bi-monthly gather)
7. Select **X** to exit. Select **X** again to save changes and return to the Main menu. For changes to take effect, you must activate the inactive configuration.

26.71.3 Set Base Rates

To set base rates for billing purposes:

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(B) Base Rates** and enter one or more FCOS numbers. Valid entries are:
   - A = all (1-64)
   - E = even
   - O = odd
   - L = lower half (1-32)
   - U = upper half (33-64)
   - A range of first-last, for example, 1-5
3. Individual numbers separated by commas, for example, 1,3,4,6
4. A single FCOS number, for example, 1
5. At the **base rate ($n.nn) ?** prompt, enter an **amount** from $0.01 through $654.99, **OR** enter **0.00** to clear the current rate (you must enter two digits after the decimal point when entering an amount or clearing the current rate), **OR** press **Enter** to keep the current setting.
6. Exit to the Main Menu to make your settings take effect.

Note:
FCOS from 65 to 640 are billed at the rates set for FCOS 64.

26.71.4 Set Billing Rates for Connect Time

This procedure describes how to set low usage rates, high usage rates, and a high/low boundary for user connect time, caller connect time, and call placement connect time. The server uses these rates to calculate charges when generating billing reports.

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(C) Connect Time** and enter the line group **number** (1-16) to which user and caller connect time rates will apply. Rates for call placement connect time apply to all line groups.
3. For each connect time category (user connect, caller connect, call placement), enter the following information as required, when prompted:

   - At the **low usage rate ($ n.nnn) ? $** prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
   - At the **low/high boundary (n) ?** prompt, enter a **number** from 1 through 65535 that represents the number of units (tenths of a minute) at which the low rate changes to a high rate (for example, 600 equals 1 hour), OR enter **0.00** to clear the current rate, OR press **Enter** to keep the current setting.
   - At the **high usage rate ($ n.nnn) ?** $ prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
4. Exit to the Main Menu to make your settings take effect.

26.71.5 Set Billing Rates for Messages Received

This procedure describes how to set low usage rates, high usage rates, and a high/low boundary for types of messages received. The server uses these rates to calculate charges when generating billing reports.

• User messages	• Wakeup messages
• Caller messages	• Receipt response messages
• Call placement messages	• Fax received, sent, retrieval, and undelivered mes sages
• Future delivery messages	• Fax pages received, sent, and retrieved messages
• Urgent messages	

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(M) Messages Received**.
3. For one or more message types (listed above), enter the following information when prompted (you can press **Enter** until you reach the message type you want to set/change.):

   - At the **low usage rate ($ n.nnn) ? $** prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
   - At the **low/high boundary (n) ?** prompt, enter a **number** from 1 through 65535 that represents the number of units (tenths of a minute) at which the low rate changes to a high rate (for example, 600 equals 1 hour), OR enter **0.00** to clear the current rate, OR press **Enter** to keep the current setting.
   - At the **high usage rate ($ n.nnn) ?** $ prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.

4. Exit to the Main Menu to make your settings take effect.

26.71.6 Set Billing Rates for Mailbox Accesses

This procedure describes how to set low usage rates, high usage rates, and a high/low boundary for the two types of mailbox access statistics: logins and greets. The server uses these rates to calculate charges when generating billing reports.

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(A) Mailbox Accesses** and enter the line group **number** to which these mailbox access rates will apply.
3. For each access category (logins and greets), enter the following information as required, when prompted:

   - At the **low usage rate ($ n.nnn) ? $** prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
   - At the **low/high boundary (n) ?** prompt, enter a **number** from 1 through 65535 that represents the number of units (tenths of a minute) at which the low rate changes to a high rate (for example, 600 equals 1 hour), OR enter **0.00** to clear the current rate, OR press **Enter** to keep the current setting.
   - At the **high usage rate ($ n.nnn) ?** $ prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
4. Exit to the Main Menu to make your settings take effect.

26.71.7 Set Billing Rates for Pager Calls or Message Delivery

This procedure describes how to set rates which the server can use to produce a report for billing message delivery usage or pager usage.

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(P) Pager Calls** and enter the index **number** (0-15) of the pager system (that includes message delivery), that you want to set rates for.
3. At the **low usage rate ($ n.nnn) ? $** prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
4. At the **low/high boundary (n) ?** prompt, enter a **number** from 1 through 65535 that represents the number of units (tenths of a minute) at which the low rate changes to a high rate (for example, 600 equals 1 hour), OR enter 0 to charge the same rate regardless of usage.
5. At the **high usage rate ($ n.nnn) ?** $ prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
6. Exit to the Main Menu to make your settings take effect, or enter the index number of the next pager system to continue.

26.71.8 Set Billing Rates for Disk Usage

This procedure describes how to set low usage rates, high usage rates, and a high/low boundary all disk usage. The server uses these rates to calculate charges when generating billing reports.

To set billing rates for disk usage:

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(D) Disk Usage**.
3. At the **low usage rate ($ n.nnn) ? $** prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
4. At the **low/high boundary (n) ?** prompt, enter a **number** from 1 through 65535 that represents the number of units (tenths of a minute) at which the low rate changes to a high rate (for example, 600 equals 1 hour), OR enter **0.00** to clear the current rate, OR press **Enter** to keep the current setting.
5. At the **high usage rate ($ n.nnn) ?** $ prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
6. Exit to the Main Menu to make your settings take effect.

26.71.9 Set Billing Rates for Network Usage

This procedure describes how to set low usage rates, high usage rates, and a high/low boundary for types of network usage. The NuPoint Unified Messaging server uses these rates to calculate charges when generating billing reports. Types of network usage are:

- Network messages sent
- Network urgent messages sent
- Number of network nodes sent to and sent urgent to
- Number of remote network recipients sent to and sent urgent to
- Network messages received and network urgent messages received
- Message length for network messages sent, sent urgent, received, and received urgent
- Message length for number of network nodes sent and sent urgent
- Message length for number of remote recipients sent and sent urgent

To set billing rates for network usage:

1. From the Main Menu, select **(R) Reports**, **(B) Billing**, and then **(A) Adjust Rates**.
2. Select **(N) Network Rates**.
3. For one or more network usage types (listed above), enter the following information when prompted (you can press **Enter** until you reach the usage type you want to set/change.):
   - At the **low usage rate ($ n.nnn) ? $** prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
   - At the **low/high boundary (n) ?** prompt, enter a **number** from 1 through 65535 that represents the number of units (tenths of a minute) at which the low rate changes to a high rate (for example, 600 equals 1 hour), OR enter **0.00** to clear the current rate, OR press **Enter** to keep the current setting.
   - At the **high usage rate ($ n.nnn) ?** $ prompt, enter an amount for the new usage rate ($0.01 through $64.99) OR enter **0.00** to clear the current rate OR press **Enter** to keep the current setting.
4. Exit to the Main Menu to make your settings take effect.

26.71.10 Bill Outdials to an Account or Long Distance Carrier

This procedure describes the steps for having an outdial billed to an account or a long distance carrier specified for the originating mailbox.

Configure an Access Code

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:

   - Select (F) Modify Inactive Configuration if you just made a change through the Offline Menu without activating it

   - Otherwise, select (E) Modify Active Configuration.
3. Select **(G) Group Selected** and enter *t*he **number** of the Pagers line group (1-24).
4. Select **(M) Modify Application** and then **(D) Define Pagers**.
5. Select **(P) Current Pager System** and enter the pager system index **number** representing the access code for the outdials.
6. Select **(D) Access Code** and enter the **code** (1-24 characters) that is common to mailbox owners using this outdial index. This code indicates what the server should dial before the destination telephone number. It comprises the first part of the dial string.
7. Save the parameter settings by exiting to the Main menu.
8. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear

Establish a Minimum Billed Number Length

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(L) Limits COS**.
2. Select **(C) Choose Limits COS to Modify** and enter the **n umber** of the LCOS you want to modify (1-640).
3. Select **(E) Set Even More Limits for Selected LCOS**.
4. Select **(I) Minimum Billed Number Length** and then enter the minimum **number** of characters in the outdial string required to activate call charges to an account or activate the specified carrier.
5. Select **(X)** to exit and save your changes.

Configure the Mailbox

1. From the Main Menu, select **(M) Mailbox Maintenance**.
2. Select **(C) Create New Mailboxes** or **(M) Modify Mailboxes** and enter the number of the mailbox to add or modify for outdial billing or for a specific carrier. (When you select "Modify", the word "New" precedes all prompts.)
3. Press **Enter** until the **Limits Class of Service** prompt appears and then enter the number (1-640) of the LCOS.
4. Press **Enter** until the **Enter Internal Outdial Index** prompt appears and then enter the index **number** (0-15) representing the access code for internal calls.

5. At the **Billed Outcall Index** prompt, enter the index **number** (0-15) representing the access code for outdials to be charged to a billing account.
6. At the **Non-Billed Outcall Index** prompt, enter the index **number** (0-15) representing the access code for outdials not charged to a billing account.
7. At the **Billing Number** prompt, enter the **number** of the account, up to 24 digits, that outdials are billed to.
8. At the **Billing Dialing Order** prompt, enter one of the following:

   - **BN** to require the billing number to be processed before the destination telephone number, OR
   - **NB** to require the destination telephone number to be processed before the billing number
9. At the **Message Waiting Type** or **# 1 Message Waiting Type #2** prompt, enter **5** (pagers).
10. At the **Pager access type** prompt, enter **B** for billed.
11. Set the other paging parameters as desired. (See Configure a Mailbox for Paging.)
12. Press **Enter** until the **Call Placement Pager Access Type** parameter displays and then enter **B** for billed.
13. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the server displays the mailbox configuration, then prompts for the next mailbox number. At this point, the parameter settings are saved and you can exit.

26.72 Overview

The system generates three types of reports.

- **System Information reports** provide specific information on how the system is configured or programmed. Information reports are discussed in System Information Reports.
- **Statistics reports** cover how system resources are used and are discussed in Statistics Reports.
- **Billing reports** provide a breakdown of charges for individual mailboxes by statistic and calculate the total amount due. These reports are discussed in Billing Reports.

The **Web Console** provides only a subset of these reports because much of the information is easily viewed in the Web Console interface. Web Console reports can be printed, or downloaded in text or .csv file format.

The **Text Console** provides numerous reports that can be viewed at the console or printed to a file.

Viewing Reports on the Text Console

Reports can be directed to the console or to a serial port; they can be displayed, saved, or printed. When you run each report, the system prompts you to choose a report destination. Choose from the following options:

REPORT OUTPUT ROUTING	
C	to display the report on the console without pausing.
P	to display the report on the console and pause as the sc reen fills.
1	(no longer used)

2	(no longer used)
F	to send the report to a file on the system.
A	to append the report to an existing file on the system.
X	to exit report output options (no report).

When displaying a report on the console, use the following commands to control scrolling:

- **CTRL-S** to stop scrolling.
- **CTRL-Q** to resume scrolling.
- **CTRL-C** to discontinue the report.

When viewing a report:

- **Press the space bar** to move ahead one page at a time.
- **Press <Enter>** to move ahead one line at a time.
- **Enter Q** when you reach the "END" of the report and want to exit the display.

26.72.1 View System Information

The System Information Report contains the serial numbers of all disks in the server, all optional features loaded, and the number of hours of speech storage. The hour, port, and link locks indicate the maximum number of hours, ports, and links that the current server can support. The UI (Unified Integration) lock lists the number of ports allowed.

To view system information:

1. In the navigation tree, click **Report Generation**, and then **System Information**. The system information report is displayed.
2. Click **Printer Friendly Version** to print the list, or click **Download** to save the list as a text file.

26.72.2 Configuration Report

Overview

The Configuration report provides a summary of all features programmed for the system. An excerpt from a Configuration report is shown here:

```
>>> Mitel Corporation <<<

SYSTEM CONFIGURATION

Tue Nov 10 14:16:07 20XX

Group #1: "voice1"

Module 1: Lines 0:0 0:1 0:2 0:3

Fax Conn: Fax Group 1 (1 channel shared w/ other line groups)

Voice Recognition Conn: <none>

Application = [NP RECEPTIONIST]

Dial plan = [4,4,4,4,4,4,4,P8,3]

Administrator mbox # = [998]

General Greeting mbox # = []

Attendant mbox # = [999]

Wait Prompt = [Y]

Caller multiple messages enabled = [Y]

KEY_0 for attendant transfer during greeting = [N]

Disconnect string = []

Pre-company name string = []

Pre-mailbox greeting string = []

Passcode Length Min = [4], Max = [10], Language = [English]

"6" Key Operator Transfer Dial String = []

Enter Group Number to Display (1-24) or <CR> for all: 01

"6" Key Operator Transfer pre-Dial String = []

Start of day = [08:00 AM], End of day = [05:00 PM], Days of Week = [DDDDDNN]

Passcode trip count = [5], Passcode trip period = [24]

Dial-by-name: Last First = [Y], Match Threshold = [3], Exact = [Y]

Suppress Number = [N], Single Digit Access = [N]
```

Run the Configuration Report

1. From the Main Menu, select **(R) Reports** and then **(C) Configuration**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server
3. Select a group number to display or press **Enter** for all groups.

26.72.3 Call Director Database Report

The Call Director Database report provides a list of all mailboxes that are licensed to have personal call flows. An excerpt from a sample report is shown here:

```
**********CALL DIRECTOR DATABASE REPORT**********

***Mailboxes Licensed to have personal call flows ***

Mailbox Number

1. 4095

2. 8888

3. 13215

4. 15152

5. 20105

6. 20225

7. 20228

8. 20239

9. 20240

10. 20242

11. 20293

12. 20311

13. 20364

14. 20418

15. 20469

16. 20592

17. 20704
```

Run the Call Director Database Report

1. From the Main Menu, select **(R) Reports** and then **(N) Call Director Database Report**.

2. Select an output routing for the report:

- **C** to send the report to the console without pausing
- **P** to send the report to the console, pausing as the screen fills
- **F** to send the report to a file on the server
- **A** to append the report to an existing file on the server

The system runs the report and returns to the Reports Menu.

26.72.4 Feature Class of Service (FCOS) Report

Overview

A Feature Class of Service (FCOS) is assigned to each mailbox when the mailbox is created. The FCOS feature bits grant privileges or impose restrictions on mailboxes.

The FCOS Report lists each FCOS and the numbers of the assigned feature bits. An excerpt from a sample FCOS Report is shown here:

```
>>> Mitel Corporation <<<

FEATURE CLASS OF SERVICE

Tue Nov 10 15:22:21 20xx

FCOS: UNLIMITED : 1

001 002 003 004 005 006 007 020 024 028 029 032 033 034 035 040 041 043 044 045

050 053 055 058 059 066 070 071 072 073 074 077 092 098 125 126 161

FCOS: FULL GUEST : 2

001 002 003 004 005 006 008 020 024 028 029 032 033 034 035 040 041 043 044 045

050 053 055 058 059 066 070 071 072 073 074 077 126

FCOS: RESTRICTED : 3

001 002 003 004 005 006 008 009 010 040 041 043 044 050 052 053 054 055 058 059

066

FCOS: CHECK IN : 4

001 004 005 066 070 071 072 090

FCOS: CHECK OUT : 5

001 004 005 066 070 071 072 091

FCOS: GREETING ONLY : 6

001 002 003 060 062 066 070 071 072 073

FCOS: TUI EMULATION : 7

/usr/vm/log/tmp_ShL.0A1 18%
```

Run the FCOS Report

1. From the Main Menu, select **(R) Reports** and then **(F) FCOS**.

2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

3. Refer to Feature Bit Descriptions for details.

26.72.5 Group Class of Service (GCOS) Report

Overview

The Group Class of Service (GCOS) provides a way to manage the mailboxes with which a particular set of system users can communicate. A GCOS must be included in every mailbox configuration for the mailbox owner to send and receive messages. The report lists the groups assigned to each GCOS. An excerpt from a sample GCOS Report is shown here:

```
>>> Mitel Corporation <<<

GROUP CLASS OF SERVICE

Tue Nov 10 15:30:25 20xx

GCOS: Default GCOS 1 : 1

001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019 020

021 022 023 024 025 026 027 028 029 030 031 032 033 034 035 036 037 038 039 040

041 042 043 044 045 046 047 048 049 050 051 052 053 054 055 056 057 058 059 060

061 062 063 064 065 066 067 068 069 070 071 072 073 074 075 076 077 078 079 080

081 082 083 084 085 086 087 088 089 090 091 092 093 094 095 096 097 098 099 100

101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120

121 122 123 124 125 126 127 128

GCOS: Contractors : 2

001 007 009 013 041 056 099

GCOS: <No name> : 3

GCOS: <No name> : 4

GCOS: <No name> : 5
```

Run the GCOS Report

1. From the Main Menu, select **(R) Reports** and then **(G) GCOS**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

The system runs the report and returns to the Reports Menu.

26.72.6 Limits Class of Service (LCOS) Report

Overview

A Limits Class of Service (LCOS) is assigned to each mailbox when the mailbox is created. LCOS allow you to control system resources, such as speech and message storage. LCOS are detailed in Mailbox Reference Guide.

The LCOS Report lists each LCOS and the limits that are set for each parameter. A sample LCOS Report is shown here.

```
>>> Mitel Corporation <<<

LIMITS CLASS OF SERVICE

Tue Nov 10 14:28:19 20xx

Max Netq Max User Callr Name Greet Max Msg Net MsgDl 1View

# Name Msgs Msgs Bill Len Len Len Len Log Sib Sib Delay Tmout

-------------------------------------------------------

1 Default 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

2 NYNEX-Basic 200 99 0 2.0 2.0 2 2.0 0 199 199 5 59

3 NYNEX-Advanced 200 99 0 2.0 2.0 2 2.0 0 199 199 5 59

4 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

5 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

6 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

7 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

8 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

9 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59

10 <No name> 200 99 0 5.0 5.0 2 2.0 0 199 199 5 59
```

Run the LCOS Report

1. From the Main Menu, select **(R) Reports** and then **(E) LCOS**.

2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

3. Refer to LCOS Parameter Descriptions for details on report categories.

26.72.7 Log File Report

Overview

The log file is a record of any detected module or system errors and the date and time of any system resets. An excerpt from a sample Log File Report for a single-module system is shown here.

Note:
Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

```
>>> Mitel Corporation <<<

SYSTEM ERROR LOGFILE

Wed Nov 11 12:32:52 20xx

1 16365(ipPhone ) (ip_phone_han 409 ) 11/11 10:54:51: Ch 49 extension

147321224: Error receiving data, expected 176, received 0

1 16365(ipPhone ) (ip_phone_han 527 ) 11/11 10:54:51: Ch 49: [x.6250]

detected a closed socket

1 16314(ipPhone ) (ip_phone_han 409 ) 11/11 10:54:51: Ch 47 extension

164487560: Error receiving data, expected 176, received 0

1 16314(ipPhone ) (ip_phone_han 527 ) 11/11 10:54:51: Ch 47: [x.6248]

detected a closed socket

1 16301(ipPhone ) (ip_phone_han 409 ) 11/11 10:54:51: Ch 46 extension

161661320: Error receiving data, expected 176, received 0

1 16301(ipPhone ) (ip_phone_han 527 ) 11/11 10:54:51: Ch 46: [x.6247]

detected a closed socket

1 16258(ipPhone ) (ip_phone_han 409 ) 11/11 10:54:51: Ch 43 extension

138531208: Error receiving data, expected 176, received 0

1 16258(ipPhone ) (ip_phone_han 527 ) 11/11 10:54:51: Ch 43: [x.6244]

detected a closed socket

1 05766(recorder) (recorder.c 497 MINOR ) 11/11 10:54:51: Logfile size rea

ched 800000. Previous log file has been moved to /usr/vm/log/logfile_8.

1 16298(mitaiMon) (mtaimonitor. 363 ) 11/11 10:54:51: Ch 45, Resilient

/usr/vm/log/logfile
```

You are advised to view or print and clear this report on a weekly basis.

Reading the Logfile Report

The logfile maintains the following format:

<sitecode><m> <tid>(task_name>) <date> <time>: <error message> <code>

<sitecode>	Site code assigned to module (serial output only)
<m>	Module where failure occurred
<tid>	Task ID of program reporting problem
<task_name>	Name of system resource
<date>	Date of occurrence
<time>	Time of occurrence
<error message>	Type of error that occurred (may also indicate resets and other system activity)
<code>	Failure code

If you are unsure of the meaning or importance of any logfile message, **do not clear the logfile** until you consult with the system technician or your distributor.

Run the Logfile Report

The Logfile Report can be extensive and, therefore, time-consuming to scroll through. You are advised to review and clear all logfiles on a weekly basis. The Logfile Report can become extensive and, therefore, time-consuming to scroll through.

View the Logfile

1. From the Main Menu, select **(R) Reports** and then **(L) Log File**.
2. Select **(V) View Log File Content**.
3. The log file is displayed. Press **Page Down** to scroll through the report.
4. Press Q to exit the report. The system returns to the Log File Menu.

CAUTION: If you are unsure of the meaning or importance of any logfile message, do not clear (delete) the logfile until you consult with the system technician or your distributor.

Configure the Log File

1. From the Main Menu, select **(R) Reports** and then **(L) Log File**.
2. Select **(C) Configure Primary Log Output**.
3. To enable console output for this module, select **(E) Enable Console Output**. To disable logging to this module's console, select **(D) Disable Console Output**.
4. To change the name of the log file (default is "logfile"), select **(N) Specify Disk Log File Name** and then enter a new name for the log file.
5. Exit from the Log File menu to save your changes.

To Delete the Log File Report

1. From the Main Menu, select **(R) Reports** and then **(L) Log File**.
2. Select **(D) Delete Log File**.
3. The system prompts you to confirm the deletion. If you are unsure of the meaning or importance of any log file message, **do not clear the log file** until you consult with the system technician or your administrator.
4. Enter **Y** to continue and delete the log file OR enter **N** to keep the log file.

Access Log File help

1. From the Main Menu, select **(R) Reports** and then **(L) Log File**.
2. Select **(H) Help**.

26.72.8 Mailbox Data Report

Overview

The Mailbox Data Report is available through the Reports Menu; it is keyed to the mailboxes themselves, and it provides statistics for **every mailbox** on the system. The example below shows an excerpt from a sample Mailbox Data Report.

INTERNAL INDEX: NONE BILLED INDEX: NONE NON-BILLED INDEX: NONE

FAX RETRIEVAL ACCESS TYPE: NONE

FAX DEFAULT TELEPHONE NUMBER: NONE

CALL PLACEMENT ACCESS TYPE: NONE TIME ZONE OFFSET: 0

DISTRIBUTION LISTS WITH CHANGE RIGHTS: all

DISTRIBUTION LISTS WITH REVIEW RIGHTS: all

MAILBOX: 4095 Created: 12/05/08 12:03 pm

MSGS: 0 UNPLAYED: 0 URGENT: 0 RECEIPT: 0

LCOS: Standard : 1 FCOS: CentrexCD 15.00 : 2

GCOS: Default GCOS 1 : 1 NCOS: Default : 1

TCOS: Admin : 1 RCOS: : 1

BAD LOGS: 0 LAST LOG: 11/04/09 4:17 pm MINS: 0.0

PASSWD: Y TUTOR: N DAY: M NIGHT: M

NAME: Dave Beach CODE:

EXTEN: 4095 INDEX: 0

ATTEN DN: INDEX: 0

ALT-EX#1: ALT-EX#2:

ALT-EX#3: ALT-EX#4:

ACCESS: NONE NOTIFICATION DISABLED: N

INTERNAL INDEX: NONE BILLED INDEX: NONE NON-BILLED INDEX: NONE

MWI #01: Mitai Messaging

FAX RETRIEVAL ACCESS TYPE: NONE

FAX DEFAULT TELEPHONE NUMBER: NONE

CALL PLACEMENT ACCESS TYPE: NONE TIME ZONE OFFSET: 0

DISTRIBUTION LISTS WITH CHANGE RIGHTS: all

DISTRIBUTION LISTS WITH REVIEW RIGHTS: all

MAILBOX: 5005 Created: 05/29/09 6:04 pm

There are other mailbox reports available through the Mailbox Maintenance menu that are keyed to search criteria that you specify. They allow you to obtain statistics on **specific** mailboxes. Refer to Find Mailbox Information for procedures to run these reports: the Mailbox Data Inquiry Report, the Mailbox Block Inquiry Report, and the Mailbox Dump Report.

Run the Mailbox Data Report

1. From the Main Menu, select **(R) Reports** and then **(M) Mailbox Data**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

The system runs the report and returns to the Reports Menu.

26.72.9 Network Class of Service (NCOS) Report

Overview

The Network Class of Service (NCOS) controls users' access to the network. NCOS settings control whether a mailbox owner can send, give, or answer messages over the network. It is part of the NP Net Digital Network optional feature. An excerpt from a sample NCOS report is shown here:

```
                        >>>
Mitel Corporation <<<

NETWORK CLASS OF SERVICE

Tue Nov 10 15:35:50 2009

NCOS: Default : 1

002 003 004 005 006 007 010 011 012

NCOS: <No name> : 2

001 002 003 004 005 006 007 010 011 012

NCOS: <No name> : 3

NCOS: <No name> : 4

NCOS: <No name> : 5
```

Run the NCOS Report

1. From the Main Menu, select **(R) Reports** and then **(H) NCOS**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

The system runs the report and returns to the Reports Menu.

26.72.10 NP Receptionist Treatments Report

Overview

NP Receptionist treatment types are discussed in the Mailbox section of this guide. NP Receptionist offers two reports to show NP Receptionist configuration:

- **Receptionist Day/Night Treatment Types Report:** Each mailbox configuration contains day and night treatment types that tell the system how mailbox owners want calls handled under different conditions. The Receptionist Day/Night Treatment Types Report displays the treatment types that you can choose when you create mailboxes. **Note:** Some treatment types will not be available when NP Receptionist is configured to perform a blind call transfer (put the called party on hold, dial the number, and hang up). See Hidden ('Blind') Mailbox Extension Number Programming.
- **Pre-extension Dial Strings Report:** See Pre-extension Dial Strings Report for more information.

A sample Receptionist Day/Night Treatment Types Report is shown here:

```
>>> Mitel Corporation <<<

NP RECEPTIONIST DAY/NIGHT TREATMENT TYPES

Wed Nov 11 14:49:30 20xx

EXTENSION TYPES Auth Redial

Index Name Time Auth Code Dflt RNA BUSY REJ SCREEN

1 treatment 1 A D R R R Y

2 treatment 2 A D R R R N

3 treatment 3 A A R R R Y

4 treatment 4 A M R R R Y

5 treatment 5 A M M M R N

6 treatment 6 A M M M M Y

7 treatment 7 A R M R M Y

8 treatment 8 A R R R M Y

9 treatment 9 A R R R R N

10 MSU A M R R R N

12 Financial Aid A M M M R N

TRUNK TYPES Auth Redial

Index Name Time Auth Code Dflt Connect Fail
```

Reading the Receptionist Day/Night Treatment Types Report

The sample report shows 10 Extension treatment types. Refer to the table below for a description of the fields.

Extension Types	Treatment types
Index	Index number that represents each treatment type
Name	Descriptive name that identifies each treatment type

Extension Types	Treatment types
Auth Time	Authorized time period(s) when this number may be accessed (A = all, D = day, N = night)
Auth Code	Authorization code (usually a number) that the caller must enter before NP Receptionist rings the extension. Special codes: M = enter any valid mailbox number P = enter a valid passcode blank field = an authorization code is not necessary
Redial Dflt	Redial menu that plays when Redial is selected for any e xtension failure condition
RNA	Action taken when the extension rings but there is no answer: R = play the default Redial menu (see "Redial Dflt" field above) A = transfer to an assistance number M = prompt the caller to leave a message in the mailbox
Busy	Action taken when the extension is busy: R = play the default Redial menu A = transfer to an assistance number M = prompt the caller to leave a message in the mailbox

Extension Types	Treatment types
Rej	Action taken when call screening is in effect and the recipient rejects the call: R = play the default Redial menu A = transfer to an assistance number M = prompt the caller to leave a message in the mailbox
Screen	Shows whether the user wants NP Receptionist to scre en all outside calls: Y = yes, N = no
Trunk Types	Trunk treatment types
Connect	Connect criteria; the conditions under which the server should consider the trunk call to be successful: C = Cut through, R = Ring, T = Tone (dial or modem)
Failure	Action taken when the connect criteria for the trunk call a re not met: R = play the default Redial menu A = transfe r to an assistance number M = prompt the caller to leave a message in the mailbox

Run the Receptionist Day/Night Treatment Types Report

1. From the Main Menu, select **(R) Reports** and then **(T) NP Receptionist Treatments**.
2. Select an output routing for the report:

- **C** to send the report to the console without pausing
- **P** to send the report to the console, pausing as the screen fills
- **F** to send the report to a file on the server
- **A** to append the report to an existing file on the server

The system runs the report. Press **Q** to return to the Reports Menu.

26.72.11 Pager Access Codes Report

Overview

The Pager (Systems) Access Codes Report displays the index number, name, access code, and hold time of each supported pager system. To see all parameters configured for supported pager systems, run a system Configuration Report.

An excerpt from a sample report is shown here:

```
>>> Mitel Corporation <<<

PAGER SYSTEMS ACCESS CODES

Wed Nov 11 14:33:49 20xx

INDEX PAGER NAME ACCESS CODE HOLD TIME

0 Inhouse T145++ 3

1 Local T8+ 3

2 On Campus T 3

3 Faxbill T8+10102880 3
```

Run the Pager Access Codes Report

1. From the Main Menu, select **(R) Reports** and then **(R) Pager Access Codes**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

The system runs the report and returns to the Reports Menu.

26.72.12 Phonebook Report

Overview

The Phonebook Report is an alphabetical listing of mailbox names. It shows the corresponding mailbox number and GCOS assigned to the mailbox. You can print the report or display it on the maintenance console.

When you choose the Phonebook Report option, the system uses the Dial-by-Name database to create a phonebook. The mailbox owner's name is included in the Dial-by-Name database only when:

- Dial-by-Name function is enabled
- Feature bit 092 (User will be in Dial-by-Name database) is assigned to the mailbox FCOS.

A sample phonebook report is shown here:

```
>>>Acme Management Systems<<<

PHONEBOOK

Tue Apr 31, 20xx 12:57 pm

NAME MAILBOX GCOS

------------------------- -------- -----

ATTEND. MB 3850 2

Allen, Debbi 3852 9

Allen, Richard 511 14

Bau, Lee 255 14

Barry, Randall 601 14

Borregas, Rita 3809 9
```

Run the Phonebook Report

1. From the Main Menu, select **(R) Reports** and then **(J) Phonebook Report**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

The system displays, saves, or prints an alphabetical list of every mailbox owner's name, mailbox number, and the GCOS assigned to the mailbox.

26.72.13 Pre-extension Dial Strings Report

Description

NP Receptionist is a program that automatically answers calls and requests the extension number of the called party. When a caller enters an extension number, NP Receptionist converts it to a mailbox number. The system then checks the **mailbox extension number** field (of this mailbox) for the actual extension number to outdial.

A pre-extension dial string is a series of instructions and/or characters that the system must outdial before dialing that mailbox extension number.

Example:The dial string may consist of the dialing sequence and account code for a non-"Dial 1" long-distance carrier. If the string does not match one of the pre-extension dial strings configured by the system technician, you must enter this string in the extension number field of every mailbox that outdials to this carrier.

When an appropriate pre-extension dial string has been configured, users can select the string by simply entering an index number in the **pre-extension index** field.

The report displays the pre-extension dial strings associated with each index configured for mailboxes served by NP Receptionist.

The Pre-extension Dial Strings Report and the Receptionist Day/Night Treatment Types Report are the two reports that show NP Receptionist configuration.

Run the Pre-extension Dial Strings Report

1. From the Main Menu, select **(R) Reports** and then **(D) Pre-extension dial strings**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server
3. The system provides a list of predial strings, or it indicates that no Pre-extension dial strings configured; then it returns to the Reports Menu.

26.72.14 Show or Edit the History File

The History File is a record of modifications made to the server. Entries are made to this record by the system administrator, or by technical personnel. You should review this record before updating software on the server to verify that no custom changes have been made that might be overwritten by the new software.

You can view the current History File, and add entries to it (update it), using the Text console only.

To view the History File:

1. From the Main Menu, select **(S) System Maintenance**, **(O) Additional Options**, **(U) Utility Menu**, and then **(H) History**.
2. Select **(S) Show File** and enter a **record number** to view OR press **A** for all records. The server displays the file to the console. Press **Ctrl-S** to stop scrolling. Press **Ctrl-Q** to restart scrolling.

To enter information in the history file (update it):

1. From the Main Menu, select **(S) System Maintenance**, **(O) Additional Options**, **(U) Utility Menu**, and then **(H) History**.
2. Select **(U) Update File**.

3. At the **Contact person name:** prompt, enter the name of the person who made changes to the server, up to 15 characters.
4. At the **Reported problem:** prompt, enter the description of the problem you encountered, up to 79 characters.
5. At the **Fixed Problem:** prompt, enter the description of changes you made to the server to correct the reported problem, up to 159 characters.
6. At the **Other comments:** prompt, enter any other necessary information, up to 79 characters, or press **Enter** to leave blank.

26.72.15 System Information Report

The System Information Report provides the following details:

- Release and revision numbers of software currently installed
- Disk serial number
- Storage capacity of hard disk (in hours)
- Ports and links
- Optional features installed

An excerpt from a sample report is shown here:

```
>>>
Mitel Corporation<<<
```

SYSTEM INFORMATION

Tue Nov 10 15:39:11 2009

Install Time: Fri Oct 16 10:43:39 EDT 2009

NuPoint Messenger Base Software Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

Install Time: Fri Oct 16 10:43:40 EDT 2009

NuPoint Messenger LanBackup Optional Feature Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

Install Time: Fri Oct 16 10:43:43 EDT 2009

NuPoint Messenger Caller Line Id user interface Optional Feature Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

Install Time: Fri Oct 16 10:43:45 EDT 2009

NuPoint Messenger FPSA Optional Feature Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

/usr/vm/log/tmp_ShL.0A1

Install Time: Fri Oct 16 10:43:48 EDT 2009

NuPoint Messenger NP Admin Server Optional Feature Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

Install Time: Fri Oct 16 10:43:51 EDT 2009

NuPoint Messenger NP Call Director Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

Install Time: Fri Oct 16 10:44:04 EDT 2009

NuPoint Messenger NP Receptionist Optional Feature Release 12.5.5.16 Rev 01

Release Time: Thu Oct 1 15:38:30 EDT 2009

Run the System Information Report

1. From the Main Menu, select **(R) Reports** and then **(I) System Information**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

The system runs the report and returns to the Reports Menu.

26.73 Overview - Statistics Reporting

Statistics reports display how system resources are used.

Statistics Reporting in the Web Console:

The Web Console enables you to run three types of Statistics reports:

- **Line Usage Report:** This report shows the number of seconds during which individual lines were busy and how many calls each line received over a specific reporting time. The data can be displayed for a selection of lines.
- **Line Group Usage Report:** This report shows the number of seconds during which line groups were busy and how many calls each group received over a specific reporting time. The data can be displayed for a selection of groups.
- **Speech Block Usage Report:** The speech storage units, called “storage blocks”, depend on the storage hour capacity of the hard disk. In addition to messages, mailbox names, greetings, prompts, and distribution list names all consume speech storage blocks. The Speech Usage form is similar to Line Usage form except it does not have any Line Selections.

Reports are displayed in dita format. You can print them and export them to a CSV file.

Statistics Reporting in the Text Console:

A summary of the available Text Console reports is provided here:

- **Line Group Usage–**All Trunks Busy (ATB) **Statistics: Shows the number of times, in a specified period, that every port in a line group is busy and the total number of seconds that this condition occurs within that time period.**
- **Line Group Usage–** Line–Statistics: Shows the number of seconds that an individual port in a line group is busy and the number of calls received by that port, within a specified time period. (This report is similar to Line Usage Statistics except that it is at the line group level.)
- Line Usage Statistics: Shows the number of seconds that an individual port is busy, and the number of calls each line receives over a specified reporting period.
- **Mailbox Statistics**: Shows mailbox usage. Several reports are available through the Mailbox Maintenance Menu (Mailbox Data Inquiry Report, Mailbox Block Inquiry Report, Mailbox Dump Report)

and the Mailbox Statistics Menu option of the Statistics Menu (Total Speech and Account Breakdown, Idle Mailboxes, Mailbox Totals Report).

- Message Counts Usage Statistics: Shows the number of messages received, the number available, and the percentage of message storage available for a specified time period.
- Speech Blocks Usage Statistics: Shows the amount of speech storage units in use and the amount available over a specified time period.
- Complete Summary: Shows a summary of all report statistics. Also called "Total Statistics Summary Report".
- Total System Statistics: Shows the amount of storage capacity consumed on the hard disk and the amount available.
- **Virtual Drive Statistics:** Shows the amount of storage capacity consumed on each of the drive partitions and the amount available.
- Network Usage Statistics: **Shows network messaging activity for a specified reporting period.**

26.73.1 Run a Line Usage Report

A Line Usage report shows the number of seconds during which individual lines were busy and how many calls each line received over a specific reporting time. The data can be displayed for a selection of lines.

To run a Line Usage Report:

1. In the navigation tree, click Report Generation, then click Statistics, and then click Line Usage. The Line Usage Report Options form is displayed.
2. Configure the following Line Usage Report options as required, and then click OK:

Fields	Values
Available	Only Programmed Groups will be displayed.
Selected	
Report resolution	Select one of three: • Summary Only • 1 hour intervals • 15 min intervals
Time Range from Date	Select from the drop-down lists or click the Calendar pop-up and select a date.
Time Range from Time	Enter in 12 Hr and 60 min format (00:00-12:59), and then select AM or PM from the drop-down list. Time r ange can be from and to the same time.
Time Range To Date	Select from the drop-down lists or click the Calendar pop-up and select a date.
Time Range To Time	Enter in 12 Hr and 60 min format (00:00-12:59), and then select AM or PM from the drop-down list. Time r ange can be from and to the same time.

3. The Line Usage Report is displayed in dita format.

   - To print the report, click on **Printer Friendly Version...**.
   - To save the report as a CSV tile, click on**Export to CSV File...**.

Reading the Line Usage Report

The report heading shows the NuPoint Unified Messaging system name in the title. This name is acquired from the Network Element and is configured through the Network Element Configuration.

The report displays the following statistics:

Columns	Displayed Information
Time	mm/dd/yyyy hh:mm:ss AM/PM
Module	1-4
Slot	1-15
Line	Starting from 0
Busy Seconds	Numeric value
Calls Answered	Numeric value

26.73.2 Run a Line Group Usage Report

A Line Group Usage report shows the number of seconds during which line groups were busy and how many calls each line group received over a specific reporting time. The data can be displayed for a selection of line groups.

To run a Line Usage Report:

1. In the navigation tree, click Report Generation, then click Statistics, and then click Line Group Usage. The Line Group Usage Report Options form is displayed.
2. Configure the following Line Group Usage Report Options, and then click OK.

Fields	Values
Available	Maximum 24. Only Programmed Groups will be displ ayed.
Selected	Maximum 24.
Report resolution	Select one of three: • Summary only • 1 hour intervals • 15 minute intervals
Time Range from Date	Select from the drop-down lists or click the Calendar pop-up and select a start date.

Fields	Values
Time Range To Date	Select from the drop-down lists or click the Calendar pop-up and select an end date.
Time Range from Time	Enter in 12 Hr and 60 min format (00:00-12:59). Time range can be from and to the same time.
Time Range To Time	Enter in 12 Hr and 60 min format (00:00-12:59). Time range can be from and to the same time.

3. The Line Usage Report is displayed in dita format.

- To print the report, click on **Printer Friendly Version...**.
- To save the report as a CSV tile, click on **Export to CSV File...**.

Reading the Line Group Usage Report

The report heading shows the NuPoint Unified Messaging system name in the title. This name is acquired from the Network Element and is configured through the Network Element Configuration.

The report displays the following statistics:

Columns	Displayed Information
Time	mm/dd/yyyy hh:mm:ss AM/PM
Line Group	1-24
All Trunks Busy Seconds	Numeric value
All Trunks Busy Count	Numeric value

26.73.3 Run a Speech Block Usage Report

A Speech Block Usage report shows statistics on message numbers and speech blocks. The speech storage units, called “storage blocks”, depend on the storage hour capacity of the hard disk. Messages, mailbox names, greetings, prompts, and distribution list names all consume speech storage blocks.

The Speech Usage form is similar to Line Usage form except it does not have any Line Selections.

To run a Speech Block Usage Report:

1. In the navigation tree, click Report Generation, then click Statistics, and then click Speech Block Usage. The Speech Block Usage Report Options form is displayed.

2. Configure the following Speech Block Usage Report Options as required, and then click OK.

Fields	Values
Report resolution	Select one of three: • Summary only • 1 hour intervals • 15 minute intervals
Time Range from Date	Select from the drop-down lists or click the Calendar pop-up and select a date.
Time Range To Date	Select from the drop-down lists or click the Calendar pop-up and select a date.
Time Range from Time	Enter in 12 Hr and 60 min format (00:00-12:59). Time range can be from and to the same time.
Time Range To Time	Enter in 12 Hr and 60 min format (00:00-12:59). Time range can be from and to the same time.

3. The Speech Block Usage Report is displayed in dita format.

- To print the report, click on **Printer Friendly Version...**.
- To save the report as a CSV tile, click on **Export to CSV File...**.

Reading the Speech Block Usage Report

The report heading shows the NuPoint Unified Messaging system name in the title. This name is acquired from the Network Elements and is configured through the Network Element Configuration.

The report displays the following statistics:

Columns	Displayed Information
Time	mm/dd/yyyy hh:mm:ss AM/PM
Total Message Numbers	Numeric value
Free Message Numbers	Numeric value
Total Speech Blocks	Numeric value
Free Speech Blocks	Numeric value

26.73.4 Line Group Usage Report – All Trunks Busy Statistics

The Line Group Usage Report, also called the Line Groups–All Trunks Busy Report, shows how many times and for how many seconds every port in a line group is busy simultaneously. This condition is called All Trunks Busy, or ATB.

- Two counters are used for this resource: seconds and number.

The system checks each line group every second for an ATB condition and adds one second to the group's seconds counter every time the condition occurs. The number counter is also incremented. Neither counter is incremented if at least one trunk within a group is not busy.

Note:
You must specify the line group(s), the start and stop times, and the start and stop days for the report.

The report can be presented as the Line Group Usage Report or the Line Usage Report. An excerpt from a sample standard report is shown below. Reports may be requested for any or all parts of the most recent seven days' activities. You can display data for a single line group or a range of line groups.

To Run the Line Group Usage (ATB) Report

1. Enter **A** for Line Group Usage (ATB) from the Statistics Menu (enter **S** from the Reports Menu).

   The system displays the Line Group ATB Report Menu.

   LINE GROUP ATB REPORT MENU

   (**A**) Beginning Group (1 - 24) = [1]

   (**B**) Ending Group (1 - 24) = [24]

   (**C**) Beginning Hour (0 - 23) = [8]

   (**D**) Ending Hour (0 - 23) = [17]

   (**E**) Beginning Day (0 - 6) = [1]

   (**F**) Ending Day (0 - 6) = [5]

   (**G**) Summary = [N]

   (**R**) Run Report

   (**X**) Exit

2. Choose the group or range of groups to report:

   - Enter **A**and the number of the first group in the range to report.
   - Enter **B**and the number of the last group in the range to report.
   - Enter the same group number for both A and B to report only one group.

3. Enter **C** to select the time interval for the data to display:

   - Enter the first hour of the time period to report (0 = midnight; 12 = noon.)
   - Enter **D**and the last hour of the time period.
   - Notice that the default values are 8 (8 a.m.) to 17 (5 p.m.)

   The system retains statistical data for one week (7 days); 0 = Sun., 1 = Mon., 2 = Tue. ... 6 = Sat. The default is Mon - Fri.
4. Enter **R** to run the report.

   The system prompts you to choose a report destination.
5. Select the report destination.

The Line Group Usage Report displays All Trunks Busy data for each line group, in 15-minute increments, for each hour of the chosen interval.

The Line Usage Report shows a single value for each line group.

Note:
Reports always run in the order of ascending date. If you designate a beginning hour that is greater than the ending hour, the report automatically switches them. However, if the beginning day number is greater than the ending day number, the report will wrap-around. For example, if the beginning day is 03 and the ending day is 01, the report order will be: 03, 04, 05, 06, 01.

Sample Line Group Usage (ATB) Report

```
                          LINE GROUP ATB 15min REPORT
                           Thu Aug  1, 1996 10:46 am

07/29/96  8hr-16hr        --- minutes interval ---
Port Group 1 [Message Center]

DAY=01 HOUR=08          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=09          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=10          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=11          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=12          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=13          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=14          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=15          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0

DAY=01 HOUR=16          00-14     15-29     30-44     45-59    TOTA
ATB_SEC                    0         0         0         0
ATB_CNT                    0         0         0         0
HIGHEST ATB_SEC: 0 sec at 8,9,10,11,12,13,14,15,16 hr
LOWEST  ATB_SEC: 0 sec at 8,9,10,11,12,13,14,15,16 hr
```

Reading the Line Group Usage (ATB) Report

In the sample report, the heading shows the date and time that the report was run.

The first line shows the date of the first statistic in the report and the time interval when the data was gathered.

PORT GROUP

The data displayed immediately below this entry refer to Line Group 1.

DAY = 01 HOUR = 15

The data displayed refers to the hour between 3 p.m. and 4 p.m. on Monday. Entry 00-14 indicates that the data in the column was gathered during the first 15-minutes of the hour; 15-29 refers to the second 15-minutes of the hour; 30-44 refers to the third 15-minutes of the hour; 45-59 refers to the final 15-minutes of the hour.

TOTAL

The data for the four 15-minute intervals. If a hyphen appears in place of a numerical value, it means that data have not been gathered.

EXAMPLE: If the report is run at 3:30 p.m., and the report interval is for hours 12 - 15 (noon to 3 p.m.), the entries for hour 15 (3 to 4 p.m.) show hyphens.

BUSY

The percentage of the hour when all trunks were busy.

EXAMPLE: Between 3 p.m. and 4 p.m., Group 1 had an ATB condition that occurred for 150 out of 3600 seconds; this would be 4% of the time.

ATB_SEC

The total number of seconds in the time period that an ATB condition occurred.

ATB_CNT

The number of times that an ATB condition occurred. The counter is incremented when an ATB condition first occurs. The ATB condition must clear and reoccur before the counter is incremented again.

EXAMPLE: If you had an ATB condition that lasted for 3 seconds, the ATB-SEC counter increases by 3, but the ATB_CNT counter is increased by 1.

HIGHEST ATB_SEC

The greatest total amount of time that ATB conditions occurred in a fifteen-minute interval for the period reported. (It does not mean the longest single interval during which an ATB occurred.) In other words, this period is the busiest during the interval reported.

LOWEST ATB_SEC

The least total amount of time that ATB conditions occurred in a fifteen-minute interval for the period reported. (It does not mean the shortest single interval during which an ATB occurred.) This period has the slowest traffic during the interval reported.

Reading the Line Usage Report

The Line Usage Report (summary) displays the line groups by numbers and provides the total number of seconds, the total number of times, and the total percentage of time that an ATB condition occurred in that line group for the entire period reported.

This report is less specific than the Line Group Usage Report, but it allows you to see at a glance which line group received the most traffic for a specified time interval. In addition, by comparing the ATB count with the ATB seconds count, you can determine the average duration of the ATB condition during a specific period for each line group.

26.73.5 Line Group Usage–Line–Statistics Report

The Line Group Usage–Line–Report shows the number of seconds that individual ports in a line group are busy and how many calls each port receives over a specified reporting period. You can choose to display the data for a single line group or for a range of line groups. The reporting period can be any hour, or range of hours, from the current day or portions of the most recent seven days.

You can choose to run either a full report, which gives the statistics in 15-minute increments for each hour of the reporting period, or a summary report, which shows the average line group usage for each hour. The figure at the end of this topic provides an excerpt from a sample Line Group Usage–Line–Report.

To Run the Line Group Usage–Line–Report

1. Enter **G** for Group Usage–Line from the Statistics Menu.

   The system displays the Line Group Usage Report Menu.

```
LINE GROUP USAGE REPORT MENU
```

(**A**) Beginning Hour (0 - 23) = [8]

(**B**) Ending Hour (0 - 23) = [17]

(**C**) Beginning Group Number (1 - 24) = [1]

(**D**) Ending Group Number (1 - 24) = [24]

(**E**) Beginning Day (0 - 6) = [1]

(**F**) Ending Day (0 - 6) = [5]

(**R**) Run Report

(**X**) Exit

2. Enter **A** to select the time interval for the data to display.

   - Enter the first hour of the time period to report

     (0 = midnight; 12 = noon).
   - Enter **B**, then enter the last hour of the time period.

   Notice that the default values are 8 (8 a.m.) to 17 (5 p.m.)
3. Choose the group, or range of groups, to report:

   - Enter **C**and the number of the first group in the range to report**.**
   - Enter **D**and the number of the last group in the range to report.
   - Leave **C** and **D** at the default settings to report all groups.
   - Enter the same group number for both C and D to report only one group.

     The system retains statistical data from 12:00 midnight of the previous day.
   - Option **E**allows you to choose today's information or yesterday's data (the default setting is Monday).
   - Enter **F**to choose the ending day.
4. Enter **R** to run the report.

   The system prompts you to choose a report destination.

5. Enter the report destination to begin the report.

Sample Standard Line Group Usage-Line-Report

```
                                LINE GROUP USAGE 15min REPORT
                                  Thu Aug  1, 1996 10:58 am

08/01/96  8hr-16hr   --- minutes interval ---  Group #5 [DTMF To P

LINE      1:3:0 HOUR=08 00-14     15-29     30-44     45-59    TOT
SECONDS                  0        11         0         0
CALLS                    0         0         0         0

LINE      1:3:1 HOUR=08 00-14     15-29     30-44     45-59    TOT
SECONDS                  0         0        10         0
CALLS                    0         0         0         0


LINE      1:3:0 HOUR=09 00-14     15-29     30-44     45-59    TOT
SECONDS                  0         0         0         0
CALLS                    0         0         0         0

LINE      1:3:1 HOUR=09 00-14     15-29     30-44     45-59    TOT
SECONDS                  0         0         0         0
CALLS                    0         0         0         0
```

Reading the Line Group Usage–Line–Report

In the sample report, the heading shows the date and time that the report was run.

The first line of the report shows the date and time interval when the data were gathered.

GROUP

The lines belong to Line Group 1.

LINE 1:0:3 HOUR = 14

The data displayed immediately below refers to the triplet 1:0:3 (module 1, slot 0, port 3) for the time period between 2 p.m. and 3 p.m. Entry 00-14 indicates that data in the column were gathered during the first fifteen minutes of the hour; 15-29 refers to the second 15-minutes of the hour; 30-44 refers to the third 15 minutes of the hour; 45-59 refers to the final 15-minutes of the hour.

TOTAL

The data for the four 15-minute intervals. When a hyphen appears in place of a numerical value, it means that data have not been gathered.

EXAMPLE: If the report is run at 3:30 p.m., and the report interval is for hours 12 - 15 (noon to 3 p.m.), the entries for hour 15 (3 p.m. to 4 p.m.) show hyphens.

USAGE

The percentage of the hour the line was busy.

EXAMPLE: Line 1:0:0 was busy for 300 seconds out of 3600 or for 8% of the time between

2 p.m. and 3 p.m.

SECONDS

The total number of seconds that the line was busy during the time period.

CALLS

The number of calls that were received by the line during the time period.

Reading the Line Group Usage–Line–Summary Report

The summary report displays the line groups by number and gives the total number of seconds and the total number of times that a line in that line group was used during the entire period reported. This report is less specific than the standard report, but it allows you to see at a glance which line group receives the most traffic during the specified time interval.

26.73.6 Line Usage Statistics Report

Overview

The Line Usage Report shows the number of seconds that individual ports were busy and how many calls each line received over a specified reporting period. You can choose to display the data for a single line or for a range of line numbers. The reporting period can be any hour, or range of hours, from the current day or from portions of the most recent seven days.

An excerpt from a sample Standard Line Usage Report is shown here:

```
LINE
USAGE 15min REPORT

Thu May 14, 20XX 2:01 pm

05/11/XX 8hr-12hr --- minutes interval ---

DAY=01 LINE=1:0:183

HOUR=08 00-14 15-29 30-44 45-59 TOTAL USAGE

SECONDS 0 0 0 0 0 0 %

CALLS 0 0 0 0 0

HOUR=09 00-14 15-29 30-44 45-59 TOTAL USAGE

SECONDS 0 0 0 0 0 0 %

CALLS 0 0 0 0 0

HOUR=10 00-14 15-29 30-44 45-59 TOTAL USAGE

SECONDS 0 0 0 0 0 0 %

CALLS 0 0 0 0 0

HOUR=11 00-14 15-29 30-44 45-59 TOTAL USAGE

SECONDS 0 0 0 0 0 0 %

CALLS 0 0 0 0 0

HOUR=12 00-14 15-29 30-44 45-59 TOTAL USAGE

SECONDS 0 0 0 0 0 0 %

CALLS 0 0 0 0 0

HIGHEST USAGE: 0 sec at 8,9,10,11,12 hr

LOWEST USAGE: 0 sec at 8,9,10,11,12 hr
```

Reading the Standard Line Usage Report

In the sample report, the heading shows the date and time that the report was run.

The first line of the report shows the date and time interval during which the data were gathered.

DAY = 01 LINE = 1:0:183 The data displayed immediately below refer to the triplet 1:0:183 (module 1, slot 0, port 183), on Monday. Entry 00-14 indicates that data in the column were gathered during the first 15-minutes of the hour; 15-29 refers to the second 15-minutes of the hour; 30-44 refers to the third 15-minutes of the hour; 45-59 refers to the final 15-minutes of the hour.

TOTAL The data for the four 15-minute intervals. If a hyphen appears in place of a numerical value, it means that the data have not been gathered.

EXAMPLE: If the report is run at 3:30 p.m., and the report interval is for hours 12-15 (noon to 3 p.m.), the entries for hour 15 (3 to 4 p.m.) show hyphens.

USAGE The percentage of the hour the line was busy.

SECONDS The total number of seconds that the line was busy during the time period.

CALLS The number of calls received by the line during the time period.

HIGHEST USAGE The greatest total amount of time that the line was busy in a single 15-minute interval of the reporting period.

LOWEST USAGE The least total amount of time that the line was busy in a single 15-minute interval of the reporting period. This period has the slowest traffic for the line during the interval reported.

Reading the Line Usage Summary Report

The Line Usage Summary Report displays the ports by triplet, gives the total number of seconds that each line is busy, and the total number of calls that each line receives during the entire report period. The summary report is less specific than the standard report, but it allows you to see at a glance which line receives the most traffic for the specified time interval. In addition, by comparing the number of seconds that a port is busy with the number of calls that the line receives, you can determine the average duration of a call during this period for each port.

Run the Line Usage Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(L) Line Usage**.
2. Select **(A) Add Lines to Report** and enter the number of the first line in the range to report. To report all lines, leave (A) an (B) at the default settings. To report only one line, enter the same number at both. Enter the triplet as: <module>:<slot>: <port> in one of the following formats:

   - Line number range: <module>:<slot>:<port>-<module>:<slot>:<port>.
   - Wild card entry * (all lines all modules), or <module>:* (all lines on <module>), or <module>:<slot>:* (all ports on <module>:<slot>).
   - Enter multiple values, as described, separated by commas.

Note:
Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

3. In the Line Usage Report menu:

   - Select **(B) Drop Lines to Report** and enter the number of the last line in the range to report using the format described in step 2.
   - Select **(D) Beginning Hour** and enter the last hour of the time period to report. (0 = midnight; 12 = noon. Default is 8)
   - Select **(E) Ending Hour** and enter the last hour of the time period to report. (Default is 17.)
   - Select **(F) Beginning Day** and enter the first day of the week to report (Sun-Sat = 0-6. Default is Mon - Fri.)
   - Select **(G) Ending Day** and enter the last day of the week to report.
   - (Optional) Select **(H) Summary =** and choose **N** for detailed report or **Y** for a summary report. (Default is N.)
   - Select **(R) Run report.**
4. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The Standard Line Usage Report displays data for each line, in 15-minute increments, for each hour of the chosen interval. The Line Usage Summary Report shows a single value for each line.

26.73.7 Mailbox Statistics Reports

Overview

Mailbox usage statistics reports are available through both the Mailbox Maintenance Menu and the Reports > Statistics > Mailbox Statistics Menu.

The Mailbox Maintenance Menu offers the following reports discussed in the Mailbox Configuration section:

- Mailbox Data Inquiry Report
- Mailbox Block Inquiry Report
- Mailbox Dump Report

The Reports > Statistics Menu offers three reports that provide summary "snapshots" of current mailbox usage and speech storage.

- Total Speech and Account Breakdown Report
- Idle Mailboxes Report
- Mailbox Totals Report

Total Speech and Account Breakdown Report

The Total Speech and Account Breakdown Report summarizes account (mailbox) statistics and speech statistics for all mailboxes in the system. Speech storage is used for messages, names, and greetings. A sample Total Speech and Account Breakdown Report is shown here:

ACCOUNT STATISTICS

Mailboxes: 8814 0 %

Dist Lists: 0 0 %

Copy Lists: 0 0 %

Config Records: 0 0 %

Statistics Records: 0 0 %

---------- ----- -----

Total: 42445043204294967290 %

Total Free Used

Message Numbers 268403456 268403422 0 %

Speech Blocks 36478574 28807719 21 %

SPEECH STATISTICS

Amount Frames Blocks Blocks

------ ------ ------ ------

greet1: 13 4957 0 0 %

greet2: 1 224 0 0 %

greet3: 1 192 0 0 %

greet4: 1 224 0 0 %

names: 9 134635984 0 0 %

dlnames: 0 0 0 0 %

fax greet: 4 2784 0 0 %

fax msg: 0 0 0 0 %

messages: 9 245467360 7670855 21 %

blocks used by greets and names: 0

blocks used by fax messages/greets: 0

average time in seconds for messages: 44399

(END)

Run the Total Speech and Account Breakdown Report

1. From the Main menu, select **(R) Reports**, **(S) Statistics**, and then **(R) Mailbox Statistics**.
2. Select **(B) Total Speech Account Breakdown**.
3. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The system displays, saves, or prints account statistics, speech statistics, and a summary of message statistics.

Idle Mailboxes Report

The Idle Mailboxes Report

- Shows mailbox numbers that are not logged into by their owners
- Summarizes mailbox usage statistics
- Lists FCOS, LCOS, and department codes assigned to idle mailboxes
- Shows the number of mailboxes that are logged into or that receive messages as "Mailboxes with Activity"

A sample Idle Mailbox Report is shown here:

```
>>>
Mitel Corporation <<<
```

MAILBOX STATISTICS

Fri Nov 13 14:54:22 20XX

The following mailboxes have NEVER logged in:

1234 1235 1236 1250 1251 1252 1253

1254 1260 1261 1262 1263 1264 5000

5002 5008 5108 5399 5400 8521 9998

9999 10000 10001 10002 10003 10004 10005

MAILBOX STATISTICS since Tue Nov 1, 20XX 8:00 am

8814 Mailboxes included in this report

2 Mailboxes with activity

8812 Mailboxes have never logged in

2 Mailboxes have logged in

7 Mailboxes with pagers

0 Total calls to pagers

0.0 Average calls to pagers per subscriber

0 Wakeup messages received

10 Total messages deposited

25 Total greets played

52 Total logins

14.1 User connect time (minutes)

4.5 Caller connect time (minutes)

0.0 Disk usage (minute_size*hours_kept)

0.2 Average user connect time

0.1 Average caller connect time

Run the Idle Mailboxes Report

1. From the Main menu, select **(R) Reports**, **(S) Statistics**, and then **(R) Mailbox Statistics**.
2. Select **(I) Idle Mailboxes**.
3. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The system displays numbers, FCOS, LCOS, and department codes of all idle mailboxes. The report summarizes idle mailbox activity.

Mailbox Totals Report

The Mailbox Totals Report gives the same type of information as the Idle Mailboxes Report; however, it reports *all* mailboxes on the system. The "Mailboxes with Activity" entry shows the number of mailboxes that are logged into or that receive messages.

To Run the Mailbox Totals Report

1. From the Main menu, select **(R) Reports**, **(S) Statistics**, and then **(R) Mailbox Statistics**.
2. Select **(M)** for Mailbox Totals Report
3. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The system displays, saves, or prints numbers of all mailboxes, FCOS, LCOS and department codes assigned to mailboxes. It summarizes mailbox activity.

26.73.8 Message Counts Usage Statistics Report

Overview

The Message Counts Usage Report shows the number of messages received, the number of messages still available, and the percentage of message storage available in a specified reporting period.

The reporting period can be any hour or range of hours in the current day or portions of the most recent seven days. You can chose to run either a full report, which gives the statistics in 15-minute increments for

each hour of the reporting period, or a summary report, which shows the average message usage for each hour. An excerpt from a sample Standard Message Counts Usage Report is shown here:

```
>>>
Mitel Corporation <<<
```

MESSAGE USAGE 15min REPORT

Fri Nov 13, 2009 3:10 pm

11/09/09 8hr-17hr --- minutes interval --- Max Messages=268403456

MESSAGE HOUR=08 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

MESSAGE HOUR=09 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

MESSAGE HOUR=10 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

MESSAGE HOUR=11 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

MESSAGE HOUR=12 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

MESSAGE HOUR=13 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

MESSAGE HOUR=14 00-14 15-29 30-44 45-59 AVERAGE

MESSAGE FREE 268403424 268403424 268403424 268403424 268403424

PERCENT USED 0 % 0 % 0 % 0 % 0 %

Reading the Standard Message Counts Usage Report

In the sample report, the heading shows the date and time that the report was run.

The first line of the report shows the date and time interval that the data were gathered and the total number of messages received during that time period. This line is repeated for each day of the report.

MESSAGE HOUR = 08 The data displayed immediately below were gathered during the hour between 8 a.m and 5 p.m. Entry 00-14 indicates that data in the column were gathered during the first 15-minutes of the hour; 15-29 refers to the second 15-minutes of the hour; 30-44 refers to the third 15-minutes of the hour; 45-59 refers to the final 15-minutes of the hour. The report covers data hourly.

AVERAGE The average value for the four 15-minute samples. If a hyphen appears in place of a numerical value, it means that data have not been gathered.

MESSAGE FREE The number of messages *not in use at the time of sampling.*

PERCENT USED The number of messages in use, as a percentage of the maximum number of messages allowed on the system.

Reading the Message Counts Usage Summary Report

The summary report displays, by day and by hour

- Total number of messages used
- Total number of messages available
- Percentage of message storage used

The summary report is less specific than the standard report, but it allows you to easily determine the hours when message storage is at its peak and the hours with low message storage.

You can use the report to detail the hours immediately before and after midnight in order to judge the effectiveness of the automatic purge.

EXAMPLE: If message storage is near or above 80% on a regular basis, the LCOS of most mailboxes on the system should be adjusted to give these mailboxes a shorter message retention time. This makes the purge more effective, and frees message storage more quickly.

As an alternative, the maximum number of messages and maximum message length parameters can be decreased for as many system LCOS as is feasible.

Run the Message Counts Usage Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(M) Message count usage**.

2. In the Line Group Usage menu:

   - select **(A) Beginning Hour** and enter the first hour of the time period to report (0 = midnight; 12 = noon. Default is 8)
   - select **(B) Ending Hour** and enter the last hour of the time period to report. (Default is 17.)
   - select **(C) Beginning Day** and enter the first day of the week to report (Sun-Sat = 0-6. Default is Mon - Fri.)
   - select **(D) Ending Day** and enter the last day of the week to report
   - (optional) select **(E) Summary =** and choose **N** for detailed report or **Y** for a summary report. (Default is N.)
   - select **(R) Run report**

3. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The standard Message Usage Report displays data for each hour of the chosen interval in 15-minute increments. The Message Usage Summary Report shows a single value for each hour.

26.73.9 Speech Blocks Usage Statistics Report

Overview

Each system has a maximum number of storage units available on the hard disk. The number of speech storage units, called "speech blocks", depends on the storage hour capacity of the hard disk. Messages, mailbox names and greetings, prompts, and distribution list names consume speech storage blocks.

The Speech Blocks Usage Report shows the following information for a specified reporting period:

- Maximum number of speech blocks for your system
- Number of blocks in use
- Percentage of message storage available

The reporting period can be any hour or range of hours from the current day or from portions of the most recent seven days. You can choose to run either a full report, which gives the statistics in 15-minute

increments for each hour of the reporting period, or a summary report, which shows the average speech blocks usage for each hour. A sample Speech Blocks Usage report is shown here:

```
 >>>
Mitel Corporation<<<
```

SPEECH USAGE 15min REPORT

Fri Nov 13, 20XX 3:18 pm

11/09/XX 8hr-17hr --- minutes interval --- Max Speech Blks=36478574

SPEECH HOUR=08 00-14 15-29 30-44 45-59 AVERAGE

BLOCKS FREE 29252256 29252256 29252256 29241265 29249508

PERCENT USED 20 % 20 % 20 % 20 % 20 %

SPEECH HOUR=09 00-14 15-29 30-44 45-59 AVERAGE

BLOCKS FREE 29241265 29241265 29241265 29241265 29241265

PERCENT USED 20 % 20 % 20 % 20 % 20 %

SPEECH HOUR=10 00-14 15-29 30-44 45-59 AVERAGE

BLOCKS FREE 29227570 29227570 29227570 29227570 29227570

PERCENT USED 20 % 20 % 20 % 20 % 20 %

SPEECH HOUR=11 00-14 15-29 30-44 45-59 AVERAGE

BLOCKS FREE 29238007 29238007 29238007 29238007 29238007

PERCENT USED 20 % 20 % 20 % 20 % 20 %

SPEECH HOUR=12 00-14 15-29 30-44 45-59 AVERAGE

BLOCKS FREE 29227015 29227015 29227015 29227015 29227015

PERCENT USED 20 % 20 % 20 % 20 % 20 %

SPEECH HOUR=13 00-14 15-29 30-44 45-59 AVERAGE

BLOCKS FREE 29227015 29213322 29213322 29213322 29216745

PERCENT USED 20 % 20 % 20 % 20 % 20 %

Reading the Standard Speech Blocks Usage Report

In the sample report, the heading shows the date and time that the report was run.

The first line of the report shows the date and time interval when data were gathered and the maximum number of available speech storage blocks on the system (**Max Speech Blks**). This line is repeated for each day of the report.

SPEECH HOUR = 08 The data displayed immediately below was gathered during the hour between 8 a.m. and 5 p.m. A column entry of 00-14 indicates data were gathered during the first 15-minutes of the hour; an entry of 15-29 refers to the second 15-minutes of the hour; 30-44 refers to the third 15-minutes of the hour; 45-59 refers to the final 15-minutes of the hour.

AVERAGE The average value of the four 15-minute samples. If a hyphen appears in place of a numerical value, it means that the data have not yet been gathered.

BLOCKS FREE The number of speech blocks *not in use at the time of sampling.*

PERCENT USED The number of speech blocks in use, as a percentage of the maximum number of speech blocks allowed on the system.

Reading the Speech Blocks Usage Summary Report

The summary report displays the number of speech blocks used, the number that are free, and the percentage of speech storage used for each hour. The summary report is less specific than the standard report, but it allows you to determine the hours when speech storage is at its peak. The report also indicates the hours that have low speech storage.

To obtain an accurate picture of message and non-message related speech storage, the results of this report can be compared with the results of the Message Usage Report.

If names and greetings consume a large percentage of speech storage and leave too little storage for transient messages, you have the following options:

- (a) Decrease the maximum greeting length allowed in the LCOS for that system
- (b) Limit the recording of names for certain FCOS
- (c) Perform both (a) and (b)

Run the Speech Blocks Usage Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(S) Speech Blocks Usage**.

2. In the Speech Blocks Usage menu:

   - select **(A) Beginning Hour** and enter the first hour of the time period to report (0 = midnight; 12 = noon. Default is 8)
   - select **(B) Ending Hour** and enter the last hour of the time period to report. (Default is 17.)
   - select **(C) Beginning Day** and enter the first day of the week to report (Sun-Sat = 0-6. Default is Mon - Fri.)
   - select **(D) Ending Day** and enter the last day of the week to report
   - (optional) select **(E) Summary =** and choose **N** for detailed report or **Y** for a summary report. (Default is N.)
   - select **(R) Run report**

3. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The standard Speech Blocks Usage Report displays data for each hour of the chosen interval, in 15-minute increments. The Speech Blocks Usage Summary Report shows a single value for each hour.

26.73.10 Complete Summary Report

Overview

The Complete Summary Report is also known as the Total Statistics Summary Report. The report provides information for the previous week, in Sunday-to-Saturday order, and shows total statistics for items such as:

- Message counts
- Speech blocks
- Network usage
- Amount of storage capacity consumed on the hard disk
- Amount of storage capacity available on the hard disk.

A sample Total Statistics Summary report is shown here:

```
                                    >>>
          Mitel Corporation <<<
```

TOTAL STATISTICS SUMMARY REPORT

Fri Nov 13, 2009 3:26 pm

----------< SUNDAY >----------

Date: Sun Nov 8 23:00:02 2009

Last Reset: Fri Nov 6 13:41:37 2009

Total Messages: 0 Lowest Messages Free: 99999999

Total Speech: 36478574 Lowest Speech Free: 29347353

Total Calls: 0 Total Seconds: 0:00:00

Line ATB Count: 0 Line ATB Seconds: 0:00:00

VR Sessions: 0 VR Total Secs: 0:00:00

VR ATB Count: 0 VR ATB Seconds: 0:00:00

VR No Res Cnt: 0

NETWORKING <========== PEAKS ==========><========== TOTALS =========>

MESSAGES: IN QUEUE MINUTES LATENCY DELIVERED UNDELIV RECEIVED

BATCH: 0 0 0:00:00 0 0 0

URGENT: 0 0 0:00:00 0 - 0

----------< MONDAY >----------

Date: Mon Nov 9 23:00:02 2009

Last Reset: Fri Nov 6 13:41:37 2009

Total Messages: 0 Lowest Messages Free: 99999999

Total Speech: 36478574 Lowest Speech Free: 29024995

Total Calls: 2 Total Seconds: 0:00:04

Line ATB Count: 0 Line ATB Seconds: 0:00:00

VR Sessions: 0 VR Total Secs: 0:00:00

Reading the Complete Summary Report

The Complete Summary Report entries have the following meanings:

Each day of the week has a banner with the day name, the date, and the date of the last system reset.

TOTAL MESSAGES The number of messages available on the system.

LOWEST MESSAGES FREE The lowest number of messages that are not in use that day (system checks every fifteen minutes).

TOTAL SPEECH The number of speech blocks available on the system.

LOWEST SPEECH FREE The lowest number of speech blocks that are not in use that day (system checks every fifteen minutes).

TOTAL CALLS The number of calls processed by the system.

TOTAL SECONDS The number of seconds that the ports are busy.

LINE ATB COUNT The number of times that an ATB condition occurs in a line group.

LINE ATB SECONDS The total number of seconds the entire line group is busy.

NETWORKING MESSAGES The peak and total amounts for network delivery of messages (NP Net) in both regular and urgent queues. Numbers indicate peak times and daily totals.

Run the Complete Summary Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(C) Complete Summary Report**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

26.73.11 Total System Statistics Report

Overview

The Total System Statistics Report shows the amount of storage capacity consumed on the hard disk and the amount available. A sample Total System Statistics Report is shown here:

```
>>>
Mitel Corporation <<<
```

SYSTEM STATISTICS

Mon Nov 16 08:39:15 20XX

Total Free Used

Message Numbers 268403456 268403424 0 %

Disk Usage (4KB) 36478574 28594986 22 %

Account Sectors 11197 188803 6 %

Prompt Blocks

british 6282

dutch 7229

english 6872

```
Calls
answered since Mon Nov 16, 20XX  8:06 am: 2
```

Reading the Total System Statistics Report

System Statistics entries have the following meanings:

MESSAGE NUMBERS The links between the messages, greetings, and names associated with mailboxes and the mailboxes themselves. Each message, name, or greeting uses one message number.

DISK USAGE Number of disk records used and free.

ACCOUNT SECTORS All mailbox and system information, including users' mailbox numbers, distribution lists, passcodes, and any line with phone line exceptions.

SPEECH BLOCKS All speech recorded through the telephone in the form of messages, comments, greetings, list names, and names. Approximately 2.2 seconds of speech consume one speech block.

PROMPTS Lists each set of prompts loaded on your system and the number of speech blocks used. Use this data to determine whether you have space for additional prompts.

Run the Total System Statistics Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(T) Total System Statistics**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server
3. The system displays the output. Press **Q** to return to the menu.

26.73.12 Virtual Drive Statistics Report

Overview

The Virtual Drive Statistics Report shows the amount of storage capacity consumed on each of the drive partitions and the amount available. Hard disks in the system are partitioned into multiple logical, or virtual drives.

The report fields are the same as the Total System Statistics Report. A sample Virtual Drive Statistics Report is shown here:

```
>>>
Mitel Corporation <<<

SYSTEM STATISTICS

Mon Nov 16 09:43:54 20XX

Total Free Used

Virtual Drive #129

Message Numbers 3750 3749 0 %

Speech Blocks 16000 15996 0 %

Virtual Drive #130

Message Numbers 3750 3749 0 %

Speech Blocks 16000 15996 0 %

Virtual Drive #131

Message Numbers 3750 3749 0 %

Speech Blocks 16000 15996 0 %

Virtual Drive #132

Message Numbers 3750 3749 0 %

Speech Blocks 16000 15996 0 %

Virtual Drive #133

Message Numbers 3750 3749 0 %

Speech Blocks 16000 15937 0 %
```

Reading the Total System Statistics Report

System Statistics entries have the following meanings:

MESSAGE NUMBERS The links between the messages, greetings, and names associated with mailboxes and the mailboxes themselves. Each message, name, or greeting uses one message number.

DISK USAGE Number of disk records used and free.

SPEECH BLOCKS All speech recorded through the telephone in the form of messages, comments, greetings, list names, and names. Approximately 2.2 seconds of speech consume one speech block.

Run the Virtual Drive Statistics Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(V) Virtual Drive Statistics**.
2. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server
3. The system displays the output. Press **Q** to return to the menu.

26.73.13 Network Usage Statistics Report

Overview

The Network Usage Report gives 15-minute "snapshots" of network message activity for a specified reporting period. This period can be any hour or range of hours from the current day or the previous six days. A sample of a Network Usage report is shown here:

```
               >>>
Mitel Corporation<<<
```

NETWORK USAGE 15min REPORT

Mon Nov 16, 20XX 10:53 am

11/16/XX 8hr-9hr --- minutes interval ---

MESSAGE DAY=01 HOUR=08 00-14 15-29 30-44 45-59 AVERAGE

BATCH IN QUEUE 0 0 0 0 0

URG IN QUEUE 0 0 0 0 0

BATCH MAX LENGTH 0 0 0 0 -

URG MAX LENGTH 0 0 0 0 -

BATCH LATENCY H:M:S 0:00:00 0:00:00 0:00:00 0:00:00 -

URG LATENCY 0:00:00 0:00:00 0:00:00 0:00:00 -

BATCH DELIVERED 0 0 0 0 0

URG DELIVERED 0 0 0 0 0

TOTAL UNDELIVERED 0 0 0 0 0

BATCH RECEIVED 0 0 0 0 0

URG RECEIVED 0 0 0 0 0

UNDLV RMT MBOX 0 0 0 0 0

UNDLV NETQ FULL 0 0 0 0 0

TOTAL FRAME TX 0 0 0 0 0

TOTAL FRAME RX 0 0 0 0 0

UNDLV NWK 0 0 0 0 0

NETWORK UNDELIVERED 0 0 0 0 0

Reading the Standard Network Usage Report

In the sample report, the heading shows the node name, the report name, the date, and the time that the report was run.

The first line shows the date and time interval when the data were gathered.

HYPHEN (-) (In any column) indicates that the system was not processing messages during the report period (for example, during a power failure or when the system was taken offline for maintenance). A 0 (zero) in any column means the system was operable, but there was no activity.

MESSAGE DAY = 01, HOUR = 08 Indicates that the data displayed immediately below were gathered on Monday, during the hour between 8 a.m. and 9 a.m. Entry 00-14 indicates that data in the column were gathered during the first 15-minutes of the hour; 15-29 refers to the second 15-minutes of the hour; 30-44 refers to the third 15-minutes of the hour; 45-59 refers to the last 15-minutes of the hour.

AVERAGE The average value of the four 15-minute samples. If a hyphen appears in place of a numerical value, it means that the data have not been gathered.

*EXAMPLE:*If the report is run at 3:30 p.m., and the report interval is for hours 12-15 (noon

to 3 p.m.) of the same day, the entries for hour 15 (3 p.m. to 4 p.m.) will be hyphens.

BATCH IN QUEUE The total number of batch (non-urgent) messages and receipt updates present in the network queue during the time period.

URG IN QUEUE The total number of urgent messages in the network queue during the time period.

BATCH MAX LENGTH The total number of minutes of recorded speech in the network batch queue during the time period.

URG MAX LENGTH The total number of minutes of recorded speech in the urgent network queue during the time period.

BATCH LATENCY The maximum number of seconds that a message remained in the batch network queue during the time period.

URG LATENCY The maximum number of seconds that a message remained in the urgent network queue during the time period.

BATCH DELIVERED The total number of batch messages delivered to their destination nodes during the time period. (Receipt updates do not count.)

URG DELIVERED The total number of urgent messages delivered to their destination nodes during the time period.

TOTAL UNDELIVERED The total number of messages (batch and urgent) rejected by their destination nodes during the time period. (Receipt updates do not count.)

The Network Usage Summary Report

The Network Usage Summary Report gives peak (maximum) and total statistics for network message activity during a specified reporting period.

PEAKS Statistics for maximum activity during the reporting period. Although separate statistics are kept for batch and urgent message queues, these statistics are not broken down by destination node. In other words, urgent queue statistics refer to urgent messages accumulated for every node on the network.

Run the Network Usage Report

1. From the Main Menu, select **(R) Reports**, **(S) Statistics**, and then **(N) Network Statistics**.
2. In the Speech Blocks Usage menu:

   - select **(A) Beginning Hour** and enter the first hour of the time period to report (0 = midnight; 12 = noon. Default is 8)
   - select **(B) Ending Hour** and enter the last hour of the time period to report. (Default is 17.)
   - select **(C) Beginning Day** and enter the first day of the week to report (Sun-Sat = 0-6. Default is Mon - Fri.)
   - select **(D) Ending Day** and enter the last day of the week to report
   - (optional) select **(E) Summary =** and choose **N** for detailed report or **Y** for a summary report. (Default is N.)
   - select **(R) Run report**
3. Select an output routing for the report:

   - **C** to send the report to the console without pausing
   - **F** to send the report to a file on the server

The standard Network Statistics Report displays data for each hour of the chosen interval, in 15-minute increments. The summary report shows a single value for each hour.

26.74 Overview - Billing Reports

The system generates four billing reports. Each report provides the charges for individual mailboxes by statistic, then calculates the total amount due. Each report serves a different purpose.

- **Billing Reports** are the standard reports, usually run monthly.
- **Mailbox Blocked Reports** (Blocked Billing Reports) retain a special format and are usually sent out to other databases via the serial port.
- **Previous Billing Reports** are run when a copy of the Billing Report from the last billing cycle is desired, or when a problem occurs during the "Gather" step of the billing procedure.
- **Termination Reports** are run when a mailbox is checked out and deleted, or when paging service is discontinued during a billing cycle.

This section outlines the steps involved to generate a Billing Report and provides instructions for running reports.

26.74.1 About Billing Reports

After the server performs a gather, the statistics and charges that are calculated go into the Billing Report. The report gives a breakdown of the charges for individual mailboxes by statistics, then calculates the total amount that is due.

The Billing Report appears on three tabs:

Current Data

The Current Data tab reports the charge for the FCOS assigned to the mailbox, then lists the charges for each statistic that applies to the mailbox. Statistics for which the dollar amount is zero are not reported.

Charges are based on the rates that are in effect at the time the report is generated. No mailbox data is changed by adjusting rates or generating the report, as long as a new gather is not performed. If you find any errors in rates after the report is run, adjust the rates then run the report again (omitting the gather).

Previous Data

The information in the Previous Data tab is identical to the Current Data tab, except that it uses the data from the previous billing data file.

Termination Data

A typical use of the Termination Data information is in the hotel or motel environment. The report can be run either before or after the mailbox is checked out, but the results can be different:

- If you run the Billing Report **before** the mailbox is checked out, and there are unplayed messages, the Termination Data tab will not show charges for disk usage for these messages, since this resource is calculated when messages are deleted.
- If you run the Billing Report **after** the mailbox is checked out, the Termination Data tab shows charges for all messages, since all messages must be deleted in order to check out the mailbox. To zero the billing counters, you must delete, then recreate, the mailbox.

To charge only for messages that the mailbox holder has played, run the Billing Report before the unplayed messages are deleted.

To charge for **all** messages received, whether they were played or not, check the mailbox out first, then run the Billing Report.

To generate a billing report, you must:

1. Set the billing rates.
2. Perform an automatic gather or a manual gather.
3. Run the Billing Report.

26.74.2 Run a Billing Report

A Billing Report is generated for a mailbox and is run from the Billing Report view. Mailbox data is displayed on the form.

Note:
Running a Billing Report generates pop-ups in your browser window.

To run a Billing Report:

1. In the navigation tree, click Report Generation, then click Billing, and then click Billing Report. The Billing Report Statistics (below) are displayed.
2. In the Mailbox: field, enter the number of the mailbox you want to run a billing report for, and then click Search. The data for the Current tab is displayed.
3. To generate a report for printing, click Printer Friendly Version...
4. To export the report to a comma-separated value (CSV) file, click Export to CSV file...

   Note: By default, Microsoft Excel does not display UTF-8 characters properly. To export a file with UTF-8 characters successfully, open the file in Notepad, click Save As and save the file without any changes.
5. In the Options pop-up screen, select Billing Info from **Current Mailbox**, **All Mailboxes**, or **Mailbox Range** and then select Gathering Period from**Current Data**,**Previous Data**or**Termination Data**.

Billing Report Statistics

Each billing report displays the following information and statistics:

Mailbox Information

Field	Information
Mailbox:	The number of the mailbox that the report was run on
Owner:	Name of the mailbox user
Department:	Department code of the mailbox user
Data Gathered On:	Date and Time (mm/dd/yyyy, hh:mm:ss AM/PM).
Total Charge: (for the tab)	This data is calculated by the system.
	Below the Total Charge: field is a breakdown of statistics making up the total according to the billing categories o n the Billing Rates Form. The statistics are organized a ccording to Item, Count, and Charge, respectively. If th e numeric value for any statistic is 0, then the statistic is not displayed.

26.74.3 Run the Billing Report

The Billing Report is usually run monthly, but can be run as many times as you wish during a single billing cycle. As long as a new Gather is not performed, adjusting rates or generating the report does not change mailbox data. If you find errors in rates after the report is run, adjust the rates, then run the report again (but omit the Gather). Charges are based on the rates that are in effect at the time that the report is generated.

Run the Billing Report

1. Request a Gather to ensure that the Billing Report reflects current charges (unless you want a report of previous charges).
2. From the Main menu, select **(R) Report Generation**, **(B) Billing**, and then **(B) Billing Report**.
3. Select an output routing for the report:

   - C to send the report to the console without pausing
   - P to send the report to the console, pausing as the screen fills
   - F to send the report to a file on the server
   - A to append the report to an existing file on the server
4. At the **Range of extensions to bill?** prompt, enter a mailbox or range in one of the following formats:

   - Single mailbox number (from 1 to 99999999999)
   - Range of mailbox numbers (for example: 2000-2999) OR
   - Press **Enter** to bill all mailbox numbers

   If you want to bill two different ranges of mailbox numbers, you must run the report twice.
5. At the **FCOS service to bill?** prompt, enter FCOS (1-640) in one of the following formats:

   - a = All
   - e = Even-numbered
   - o = Odd-numbered
   - l = Lower half
   - u = Upper half
   - Range of first-last (for example: 1-5)
   - Series of numbers separated by commas (for example: 1,3,5)
   - Single number. OR
   - Press **Enter** to choose mailboxes regardless of FCOS assigned.

Note:
FCOS 65 to 640 are billed at the rate for FCOS 64.

If you want to bill more than one FCOS, but not all, you must run a separate report for each FCOS.

1. At the **LCOS service to bill?** prompt, enter LCOS (1-640) in one of the formats outlined in step 5, OR press **Enter** to choose mailboxes regardless of LCOS assigned. To bill selected LCOS, run a separate report for each one.
2. At the **GCOS service to bill?** prompt, enter a GCOS number or range from 1 through 64 OR press **Enter** to choose mailboxes regardless of GCOS assigned (including affinity GCOS 65-32,000).
3. At the **NCOS service to bill?** prompt, enter an NCOS number or range from 1 through 64 OR press **Enter** to choose mailboxes regardless of NCOS assigned.

4. • At the **Department code to bill?** prompt, enter a single department code (1 to 10 characters), OR press **Enter** to bill all mailboxes regardless of department code.
5. • At the **Pager system number to bill?** prompt, enter a pager system number (0 through 15), OR press **Enter** to choose mailboxes regardless of pager system assigned. To bill a single group of pagers (with the same pager system number), enter the number of the pager system. Separate reports for each pager system can be run if you wish.

The system runs the report according to the choices entered and sends it to the selected destination.

Reading the Billing Report

The Billing Report prints out the charges for each mailbox individually by statistic, then it gives a total.

Statistics with a zero (0) dollar amount are not reported. When charges are reported for all mailboxes, the system concludes the report with a Billing Report Summary and returns to the Billing Menu.

26.74.4 Mailbox Blocked Report (Blocked Billing Report)

Overview

The Mailbox Blocked Report (sometimes called Blocked Billing Report) retains a special format and is usually sent out through the serial port to other databases. It presents the same information as the Billing Report but in blocked form—without titles or summaries.

Use this report when you want to organize the billing data into your own format, such as for an invoice or monthly statement.

To Run the Mailbox Blocked Report

1. From the Main menu, select **(R) Report Generation**, **(B) Billing**, and then **(M) Mailbox Blocked Report**.
2. Complete steps 3 through 10 under Run the Billing Report.

Reading the Mailbox Blocked Report (Field Descriptions)

To help you identify the field names and field lengths of statistics provided in the Mailbox Blocked Report, use the following table. All fields are right justified; all fields other than the mailbox number are blank-filled.

Field Name	Field Length (Number of Characters)
Mailbox number	16
Department code	10
User messages	5
Caller messages	5
Wakeup messages	5

Field Name	Field Length (Number of Characters)
Logins	5
Greets	5
User connect time	5
Caller connect time	5
Disk usage	10
Calls to pagers	5
Calls for message delivery	5
FCOS number (Repeated 16 times for line group billing.)	3
LCOS number (Repeated 16 times for line group billing.)	3
GCOS number (Repeated 16 times for line group billi ng.)	5
Number of network messages	5
Number of urgent network messages	5
Number of network nodes sent to	5
Number of network nodes sent urgent to	5
Number of remote network recipients sent to	5
Number of remote network recipients sent urgent to	5
0.1-minute increments of network messages sent	5
0.1-minute increments of network messages sent urgent	5
0.1-minute increments of network nodes sent to	5
0.1-minute increments of network nodes sent urgent to	5
0.1-minute increments of remote network recipients sent to	10
0.1-minute increments of remote network recipients sent urgent to	10
Number of network receipt responses	5
Number of network messages received	5
Number of network urgent messages received	5
0.1-minute increments of message length received over network	5
0.1-minute increments of urgent message length rece ived over network	5

26.74.5 Previous Billing Report

The Previous Billing Report is identical to the Billing Report except that it uses data from the **previous** billing data file. Run a Previous Billing Report when a copy of the Billing Report from the previous billing period is required.

To Run the Previous Billing Report

1. From the Main menu, select **(R) Report Generation**, **(B) Billing**, and then **(P) Previous Billing Report**.
2. At the **Where should billing data come from? (F/H/X)** prompt, select **H**.
3. Complete steps 4 through 10 under To Run the Billing Report.

26.75 Overview

A special feature of this system allows you to perform various administrative functions from a telephone. The Administration by Phone feature is convenient when the system's maintenance console is located at a distance from the workstation.

Although this feature cannot completely replace console administration, telephone administration software supports numerous features available from the console, and is appropriate for specific functions discussed in this section.

Note: If your system has more than one line group and more than one administrator's mailbox, you must ensure that you call the line group associated with the administrator's mailbox that you are using in order to conduct Administration by Phone.

Administration by Phone is not available to mailboxes with the NP TDD line group configuration.

Telephone Administration Timing

Certain timing parameters are programmed into Administration by Phone to detect inactivity and to safeguard the system against unauthorized use. These time-out factors make it essential for you to be well-prepared before you begin a telephone administration session.

- Three to five seconds of response time are permitted for each prompt before it announces "no change" and returns to the Administration Menu.
- Any activity causes a one-minute timer to start, after the system accesses administration. If one minute lapses without input, the system automatically disconnects, and the entire access procedure must be repeated.
- If you are running out of time, enter the digit 1 (one) in response to any prompt, to restart the timer. The system issues an error message and repeats the prompt.

26.75.1 Access the Telephone Administration Menu

Administration by Phone can only be performed from the administrator's mailbox. Follow these steps to access the telephone Administration Menu:

1. Enter the system's main extension number to reach NP Receptionist.

2. Log in to the administrator's mailbox:

   - Press the star key (*) to enter the message center.
   - Enter the administrator's mailbox number to enter the Voice Mail system
   - Press the star key (*) to indicate that you are the owner of this mailbox

You hear the Administrator���s system greeting: "Hello <administrator's name>. Please enter your passcode."

1. Enter the administrator's mailbox telephone passcode. You are now logged in; you hear the standard prompt:

1. • Enter **M** to make a new message
   • Enter **U** to change User options
   • Enter **X** to exit

1. Press **U** (the **8** key) for the User Options Menu. You hear the standard User Options Menu, offering options to change name, greeting, passcode, etc.
2. Press the star key (*) to access the Administration Menu. The system plays the telephone Administration Menu:

Press	Menu
A	Add a New Mailbox
D	Delete a Mailbox
M	Modify a Mailbox
P	Change a Mailbox Passcode
K	Change System Clock
I	Initiate Mailbox Backup to Floppy Diskette (no longer supported)
U	Usage Statistics

Press	Menu
X	Exit Administration

To Record a Name for the Administrator's Mailbox

The system plays a greeting to the administrator when you log in. A name can be recorded with the Name command.

1. Log in to the administrator's mailbox by following Steps 1 to 3 in "Access the Telephone Administration Menu".
2. When you hear the Main Menu, press **U** (the **8** key) for the User Options Menu.
3. Press **N** (the **6** key) to change the mailbox Name.
4. Press **R** (the **7** key) to Record the name.

For security reasons, **do not** name the mailbox "Administrator's Mailbox". Unauthorized users should not know that they have accessed a special-purpose mailbox.

26.75.2 Add a New Mailbox by Phone

To Add a Mailbox by Phone

The following sequence shows the prompts and responses necessary to add a mailbox by phone. This procedure can only be performed from the administrator's mailbox.

1. Access the Telephone Administration Menu.
2. Press **A** (the **2** key) to Add a mailbox.
3. When prompted, enter:
   - the mailbox number to add
   - a Features class of service (FCOS)
   - a Limits class of service (LCOS)
   - a two-digit message waiting type
4. The system responds: "Mailbox <number> added." and then returns to the Administration Menu.

Note:
To confirm that the values entered are correct, press **M** (the **6** key) to modify the mailbox you just added. Press the **#** key (pound) in response to each prompt to leave all values unchanged.

Console versus Phone

There are important differences between creating a mailbox on the Text/Web console and adding a new mailbox by phone.

- Programming for NP Receptionist cannot be added by using the phone. The system does not prompt for treatment types, mailbox extension numbers, or attendant extension numbers.
- When Administration by Phone prompts for a Features class of service, enter the FCOS. The system accepts any FCOS number from 1 through 640, regardless of whether any feature bits are programmed for that FCOS. Error messages are **not** issued; be certain to enter the correct FCOS.
- Enter the LCOS when Administration by Phone prompts. The system accepts any LCOS number from 1 through 640; be certain to enter the correct LCOS.
- Any valid message waiting indicator can be assigned to the mailbox, but information such as paging cannot be added by phone.
- This message waiting indicator does not work without extra programming. Mailboxes requiring extra programming may be created on the maintenance console. See MWI Types.

26.75.3 Delete a Mailbox by Phone

You can delete a single mailbox by phone, but a you cannot delete a range of mailboxes by phone. You can only delete a mailbox from the administrator's mailbox.

To delete a mailbox by phone:

1. Access the Telephone Administration Menu.
2. Press **D** (the 3 button) to delete a mailbox.
3. When prompted, enter the mailbox number to delete. You hear the message "Mailbox [number] has [number] messages total. If you really intend to delete mailbox [number], enter the mailbox number again."
4. Enter the mailbox number again. The server responds with "Mailbox deleted," and returns you to the Administration Menu.
5. Press **X** (the 9 button) to exit from the Administration Menu.

26.75.4 Modify A Mailbox by Phone

When Modify is selected from the Administration Menu, the system gives the current mailbox number, class of service, mailbox type, and an AC message waiting lamp address; then, it prompts for any changes. You can only perform this procedure from the administrator's mailbox.

To modify a mailbox by phone:

1. Access the Telephone Administration Menu.
2. Press the **M** (the 6 button) to modify a mailbox.

3. When prompted, enter the mailbox number to modify. The server responds with the current mailbox number, class of service, mailbox type, mailbox message waiting type, if applicable; then prompts you for changes. To leave any value unchanged, press the **star (*)** button in response to the prompt:

   - enter a new mailbox number, if required
   - enter a new Features class of service (FCOS).
   - enter a new Limits class of service (LCOS).
   - enter a 2-digit message waiting type

   The server responds with "Mailbox modified," and returns you to the Administration Menu.
4. Press **X** (the 9 button) to exit the Administration Menu.

26.75.5 Change/Reset Mailbox Passcode or Enable/Disable Tutorial by Phone

You can set or clear the passcode and enable the tutorial for a mailbox by phone. This feature is useful to start new mailbox owners on the system or to clear the passcode of a mailbox owner who forgets his or her passcode. You can only perform this procedure from the administrator's mailbox.

1. Access the Telephone Administration Menu.
2. Press **P** (the **7** key) to change a mailbox Passcode.
3. Enter the number of the selected mailbox.
4. Enter the new passcode (four to 10 digits), OR *enter four 0s (zeros) to clear the passcode. The system confirms the passcode change.*
5. When prompted, press **Y** (the **9** key) if you want a tutorial on this mailbox, OR *p*ress **N** (the **6** key) if you do not want a tutorial on this mailbox.
6. Press **X** (the **9** key) to exit the Administration Menu.

CAUTION:
CAUTION: Do not give the administrator a trivial passcode. When you hear the message: "I'm sorry, you cannot access your mailbox at this time. Good-bye," it is often due to a passcode problem.

26.75.6 Set the System Date and Time

You can review or alter the system date and time by phone. This feature is useful to make the one-hour correction for daylight savings time. You can only perform this procedure from the administrator's mailbox.

Press * (star) at any time to cancel the procedure and exit the menu.

To set date and time:

1. Access the Telephone Administration Menu.
2. Press **K** (the **5** key) to change the system clock. The system responds with the current date and time.

3. When prompted, enter the following values, or press # to leave a value unchanged:

   - the one- or two-digit month (1 for January, 12 for December)
   - one- or two-digit day
   - two-digit year (last two digits of the year)
   - three-digit time (for example, enter 145 for 1:45) and press **A** for a.m or press **P** for p.m.

   The system responds: "The date changed to <day>, <date>, <year>, <time>."
4. Press **X** (the **9** key) to exit the Administration Menu.

26.75.7 Enable an Alternate Company Greeting

To enable an alternate greeting:

1. Dial the server extension number.
2. Log into the administrator's mailbox**.**

   - Press the **star (*)** button then enter the administrator's mailbox number.
   - Enter the administrator's passcode.
   - Press the **8 button** for User Options.
3. Press the **4 button** for Greetings.
4. Specify an alternate for the company day greeting or night greeting, or both, as follows:

   - For an alternate to the day greeting, press the **3 button f**ollowed by the **3 button**.
   - For an alternate to the night greeting, press the **6 button** followed by the **3 button**.
   - For an alternate to both greetings, press the **2 button**.
5. Press the **9 button** to exit to the Main Menu and make the alternate greeting take effect. The alternate greeting will play instead of the company greeting specified in the preceding step.

26.75.8 Report System Usage Statistics by Phone

You can use the phone to obtain system and mailbox summary usage statistics for 30 mailboxes at a time. Instead of running a Total Statistics Report during weekly maintenance, this procedure can be used to determine whether a manual message purge is necessary. Statistics Reports discusses mailbox statistics reports and message purging.

To Control the Report

- Respond to the prompt that asks you for the first mailbox number. NuPoint Unified Messaging reports the system statistics and starts the mailbox report at the selected mailbox. To cancel the report at this point, do not respond to the prompt.
- Extend the report by pressing **C** (the **2** key) after the statistics for the first 30 mailboxes are listed (when prompted). The system responds by reporting statistics for the next 30 mailboxes.
- To stop the summary report, press any key at any time.

To Generate Usage Statistics by Phone

1. Access the Telephone Administration Menu.
2. Press **U** (the 8 button) to get Usage statistics.
3. When prompted, enter a mailbox number at which you want to begin summary. The system responds "NuPoint Voice storage is [number] percent full, [number] minutes out of [number] total." Next, the system lists the statistics for the first mailbox: "Mailbox [number], [name], has [number] messages total, [number] urgent, [number] unplayed, using [number] seconds." Then, the system lists the statistics for the next 29 mailboxes.
4. When prompted, press **the 2 button** to continue listing. The system lists statistics for the next 30 mailboxes. You can press any key at any time during the summary to stop. When the listing is finished, the system plays the message, "End of summary."
5. Press **X** (the 9 button) to exit from the Administration Menu.

26.75.9 Inquire About Mailboxes by Phone

Neither the Inquire nor the Search function is available by phone. However, the following information can be obtained:

Usage Statistics:

1. Access the Telephone Administration Menu.
2. Press **U** (the 8 button) to get Usage statistics and enter a mailbox number to start the inquiry. Press the * (star) key to stop the report after the required statistics have been supplied.

Feature Class of Service, Limits Class of Service, Message Waiting Type, and AC Message Waiting Lamp Address:

1. Access the Telephone Administration Menu.
2. Press **M** (the **6** key) to Modify from the Administration Menu.
3. Press the # (pound) key in response to each prompt to leave the current values unchanged. Press the * (star) key to stop.

26.76 Overview

The NuPoint UM system contains an application designed specifically for Telephone Answering Service (TAS) Bureau use. This section highlights features useful to a TAS bureau.

Individual privileges and restrictions can be added to build customized Feature and Limits Classes of Service (FCOS and LCOS).

26.76.1 DID Mailboxes

DID mailboxes allow callers to dial a telephone number that is answered with the mailbox greeting. While some systems can use the PBX forwarding capability to allow the voice mail system to answer calls with the user's mailbox greeting, DID mailboxes answer the calls directly.

Logging in to DID Information-Only Mailboxes (Including Greeting-Only Mailboxes)

Mailboxes with Greeting-only, Chain, and Time classes of service (and any other FCOS that issue greetings and do not receive outside caller messages) are collectively referred to as "Information-only" mailboxes. The login procedure for DID Information-only mailboxes differs from the procedure for mailboxes with other FCOS.

To Log in to a DID Information-Only Mailbox

To eliminate confusion, subscribers who choose DID Information-only mailboxes should be informed of this login procedure.

1. Press the ***** key (star), or **0** key (zero), while the greeting is playing. This process does not interrupt the greeting; the greeting continues to play. The system prompts you to enter a passcode (if the mailbox is passcode protected).

> **Note**:
> You do not have to wait for the prompt, but you must wait until the entire greeting plays before entering your passcode.

2. Enter your passcode. You are now logged in.

Recording the First Greeting for DID Information-Only Mailboxes

New DID Information-only mailboxes do not have greetings. When a new user tries to access the mailbox to record a greeting, the system responds: "That is not a valid mailbox number." The user must press the * key (star) or 0 key (zero) (while "That is not a valid mailbox number" plays) and enter the passcode.

This procedure can be confusing for a new user. To alleviate the confusion, perform the following steps:

1. Initially assign Unlimited FCOS (FCOS 1) to the mailbox.
2. Log in to the mailbox, and record a greeting to welcome the new subscriber.
3. After the greeting is recorded, use the **Modify** command to give the mailbox the correct FCOS (Modify a Mailbox by Phone).

Login Tip for DID Mailbox Users

When a subscriber has a DID mailbox that can receive messages (non-Information-only class of service), toll charges can be saved by using this tip:

When a user calls in to check for messages and the phone rings, the user should hang up immediately. Ringing indicates that no unplayed messages exist in the mailbox; if users hang up before the system answers, the call is not charged. If the system answers the call with the mailbox greeting before callers hear ringing, there are unplayed messages in the mailbox.

26.76.2 The Message Attendant Application

Designed specifically for Telephone Answering Service (TAS) bureau use, the Message Attendant application provides an open line for TAS operators to dictate messages into client mailboxes. The open line allows the operator to access client mailboxes quickly. Because clients retrieve their messages by calling the system and logging into their mailboxes in the standard manner, operator time is not required for this function.

Message Attendant Prompts and Commands

The Message Attendant application uses three different tones to prompt the operator. As with other applications, the system issues a "beep" tone when prompting to record a name, greeting, or message. A "beep-beep" home base tone, tells the operator that the system is waiting for input of a mailbox number. As soon as the system knows the mailbox number, it issues a "bloop-bloop" pause mode indicator and waits for further commands from the operator. The commands to record a message are as follows:

Key Pressed	Operation
2 or #	Begin record mode. This command is used both to begin a message and to append to a message just recorded.
3	Discard message, and return to Pause mode.
7	Review message, and return to Pause mode.
1, 9, or *	Send message, and exit to home base.
*	Return to home base from either Record or Pause mode. This command also saves any recording made.

26.76.3 TAS Operator Procedures

The TAS operator must deliver messages to the client's mailbox. In addition, the operator may be required to change the name, greeting, and/or passcode for a mailbox.

To Leave a Message in a Mailbox

1. Seat the headphone jack, dial into the system, and hear the characteristic "beep-beep" home base tone.
2. Answer the call, dial the called party's mailbox number, and hear the "bloop-bloop" pause mode indicator.
3. Press the **2** key or **#** key (pound) to begin recording, hear the "beep" record prompt tone, and dictate the message.

4. Press the **1** key, **9** key, or * key (star) to send the message, and hear the "beep-beep" home base tone. You are now ready to answer the next call.

   OR

   Press **R** (the **7** key) to Review, press **D** (the **3** key) to Discard, and press the **1** key, **9** key, or ***** key (star), to send the message.

To Record Names and Greetings and Enter Passcodes:

If the client's mailbox is capable of being checked in and out, the TAS operator can change the client's name, greeting, or passcode.

Note:
To give a mailbox the capability of being checked in and out, the Administrator must answer **Y** to the question: "Can mailbox be checked in or out?" when the mailbox is created.

1. Seat the headphone jack, dial into the system, and hear the characteristic "beep-beep" home base tone.
2. Dial the mailbox number, and hear the "bloop-bloop" pause mode indicator.
3. Enter one of the following commands:

To Record a Name:

1. Press **N** (the **6** key). The system responds: "Record a new name for <mailbox number>. (Beep)"
2. Record the mailbox user's name.
3. Press the **1** key, **9** key, or ***** key (star), to save the recorded name and return to the home base tone.

To Record a Greeting:

1. Press **G** (the **4** key). The system responds: "Record a new greeting for <user's name>. (Beep)"
2. Record a greeting for the mailbox user's callers.
3. Press the **1** key, **9** key, or ***** key (star) to save the greeting and return to the home base tone.

To Enter or Change a Mailbox Passcode:

1. Press the **5** key. The system responds: "Enter a four-digit passcode for <user's name>, four zeros to clear the passcode. (Beep)".
2. Enter the new passcode and hear the "beep-beep" home base tone.

26.77 Installing an Optional Feature

You must have purchased a license for the new feature prior to installing it. This license must also first be propagated to the NuPoint Unified Messaging system, through either an online or offline synchronization with the AMC. For more information about synchronization, see the *NuPoint Unified Messaging Technician's Handbook.*

Note: MiCollab versions of NuPoint UM use a different procedure (below).

For NuPoint UM Standalone

You can use either the MSL server manager or MSL server console to install software blades.

You can download and install software blades in a single step, or you can download them for installation at a later time. The first option ties up your computer for a short period of time. The second option, which is known as "caching," enables you to initiate the download and then use your computer for other purposes.

Server Manager

To install an optional feature from the **MSL server manager** web interface:

1. Open a web browser and enter the address of the MSL server manager (http:\\<IP address or FQDN of NuPoint UM server>\server-manager)
2. Log in as "admin".
3. In the ServiceLink menu, click **Blades**.
4. To ensure that you are seeing the most recent list, click **Update List**.
5. Scroll through the list and locate the blade for the feature that you are adding to the system.
6. Do one of the following:

   - To install a new blade immediately, click the Install link beside it.
   - To download a blade for installation at a later time, click the Cache link beside it. Complete the installation process by clicking the Install link.
7. A license agreement screen appears. Accept the license agreement to continue with the installation.
8. The system installs the software blade for the new feature.
9. Reboot the server when the blade installation is complete.

Server Console

To install an optional feature from the **MSL server console**:

1. Access the server console at the server, or remotely using PuTTY.
2. Navigate to the **Access server manager** option and then select **Yes** to proceed.
3. When prompted, log in as "admin".

4. Insert NuPoint UM Software DVD 1 or 2 into the DVD-ROM drive.

DVD Name	DVD File Name	DVD Contents
NPM Blades-DVD 1	NP-UM_x.x.x.x.DVD1.iso	• NuPoint Unified Messaging installer • OCP • Software (language prompts) • Documentation
NPM Blades-DVD 2	NP-UM_x.x.x.x.DVD2.iso	• Speech Auto Attendant • Text to Speech • Speech Recognition engine

5. Navigate to the **Blades** option and locate the blade for the feature that you are adding to the system.
6. Do one of the following:

   - To install a new blade immediately, click the Install link beside it.
   - To download a blade for installation at a later time, click the Cache link beside it. Complete the installation process by clicking the Install link.
7. A license agreement screen appears. Accept the license agreement to continue with the installation.
8. The system installs the software blade for the new feature.
9. Reboot the server when the blade installation is complete.

For MiCollab Versions of NuPoint UM:

1. Access the server console at the server, or remotely using PuTTY.
2. Select the option to **Install Mitel Applications from CD/DVD**. The available options are displayed.
3. Highlight the option, or options, you want to install and press the space bar to select. Select **OK**.
4. Select **Continue** to confirm the selection.
5. When prompted, insert the NuPoint UM DVD with the specified volume label (for example, NPUM 14.1.1.17) and select **Continue**. The server caches the selected software.
6. Select **Next** to install the cached software.
7. When installation is complete, select **Next** to return to the console menu.

26.78 Direct Drop Overview

The base for the Direct Drop feature in NuPoint is the Activity message in CMG Speech with following diversion to a Virtual Machine (VM) system or the Direct Drop feature in InAttend where the attendant transfers a waiting call to a VM system.

The Direct Drop feature suppresses the user greeting when a call is diverted from BluStar Collaboration Management (CMG) Speech or InAttend to NuPoint. Direct Drop works only with MX-One integrations with NPM. To enable Direct Drop on CMG deployments of InAttend, a user Activity must be set in CMG

(Message Diversion) or a Direct Drop made by attendant in InAttend. Refer to *CMG Help* for instructions on how to set the user Activity.

Note:
Standalone InAttend does not use CMG and setting the user Activity is not supported. If InAttend integrates with a third-party server using **Transfer to Voice Mail** option, then Direct Drop of the call is supported. See *InAttend User Guide* for more information.

When Direct Drop is enabled, CMG plays the Activity message of the user before the call is diverted to NuPoint to record the message while suppressing the user defined Welcome message. Therefore, callers hear only the message “Please leave your message at the tone” and then the beep. In CMG deployments of InAttend, with no user Activity set, for calls reaching NuPoint directly from MX-One and for calls forwarded to NuPoint, the user greeting plays as usual if the line group is set to NuPoint Voice.

Configuring Direct Drop

In CMG

1. NuPoint needs to exist as an External VM system in CMG Speech.
2. This external VM system needs to be defined in a CMG User Group with the Pilot number of Direct Drop line group configured on NuPoint.
3. Specific users need to have this User Group defined in the CMG Speech tab.

In NuPoint

To configure Direct Drop in NuPoint:

1. In the server manager, under **Applications**, click **NuPoint Web Console**.
2. In the navigation tree, under **Offline Configuration**, click **Edit Offline Configuration.**
3. Click **Line Groups**.
4. Click **Add** to add a new line group. Select the application parameter as **Direct Drop**, select the user interface as **NuPoint Voice** or **Call Director**, and enter a Pilot Number.
5. Click **Save**.

In InAttend

To configure Direct Drop in Standalone InAttend, refer to the *InAttend Configuration Guide*.

Enabling Direct Drop

To enable Direct Drop in Standalone InAttend, refer to the *InAttend Configuration Guide*.

To enable Direct Drop in CMG deployments of InAttend, a user Activity must be specified and set on the CMG for the destination mailbox. Activities can be set for a specific duration on the CMG. The following Activity options are predefined on the CMG:

- Lunch break
- Left for the day
- Away from desk
- Meeting
- Business trip
- Visiting a customer
- Vacation
- Not available
- Back soon
- Sick leave

With Direct Drop enabled, the system greetings play as usual, but all user greetings are suppressed. Some of the user greetings are listed below:

- General Greetings
- Conditional Personnel Greetings (Forward, Busy, and No answer)
- Primary Personnel Greetings
- Daily Greetings (Default, Today)
- Extended Absence Greetings

26.79 About Call Detail Recorder

Note:
This option must be enabled/configured using the **Text Console**.

Call Detail Recorder (CDR) is an optional feature that implements a call accounting system that is referred to in the telecommunications industry as call detail recording. This section describes the features and capabilities of the Call Detail Recorder optional feature. It works with the NuPoint Voice application on the NuPoint UM server and must be enabled/configured using the Text console. You can generate reports about call detail information using either the Web console or the Text console.

CDR creates a record of each call transaction (such as a voice message) on the NuPoint Unified Messaging server. Records are stored in a single-line, fixed-length format. They are uniquely identified by consecutive Call Sequence Numbers, which range from 1 to 999999. After record 999999 is written, the next record is number 1. Records are not overwritten when the Sequence number goes back to 1. Overwriting only occurs when the defined maximum number of records have been stored.

The CDR application is designed to be run by one user at a time to avoid two people overwriting each other's selections. If the CDR Main Menu is running on one terminal, and a second user tries to start the CDR Main Menu, it terminates after giving the second user an error message.

CDR runs continuously once you start it. Even if you shut down or reboot the server, CDR restarts when the NuPoint Voice application loads. Similarly, if you stop CDR, it remains off until you restart it from the CDR menu.

Most configuration options can be changed while CDR is running EXCEPT the following:

- Deleting CDR records
- Reducing the maximum number of CDR records. However, you can *increase* the maximum number while CDR is running.

CDR Features

Call Detail Recorder is designed for easy data transport to another computer system. The remote site can then process the call information using any appropriate application. Call Detail Recorder provides the following features:

- Multiple call types, including network
- Call details using abbreviated codes
- Flexible output file format (40 160 columns per line)
- File wraparound capability
- Warning messages before CDR records are overwritten
- Active status maintained across server resets
- Administrator-defined CDR file limit
- Online report generator
- Output file download capability, including:
  - Limited download search criteria
  - Administrator-defined field delimiter, pad string, and length
  - ASCII/Text transfer support
  - Test download capability
  - Auto-disconnect after download

CDR Records

CDR creates a record of each call transaction on the NuPoint UM server (for example, a voice message). Records are stored in a single-line, fixed-length format. They are uniquely identified by consecutive Call Sequence Numbers, which range from 1 to 999999. After record 999999 is written, the next record is number 1. (Call Sequence Numbers "turn over," just like the odometer in a car.) Records are not overwritten when the Sequence number goes back to 1. Overwriting occurs when the defined maximum number of records have been stored.

Note: CDR records are sometimes referred to as "messages" in the menus or prompts.

CDR Fields

The CDR Record Fields table below lists the 26 fields that can appear in a CDR record. For information about field length and/or formatting, see CDR Reports.

CDR records contain certain fields that need further explanation. These fields contain two-digit numerical codes that identify certain details of every call monitored. The tables that follow this one describe the meanings of these fields:

- Field 13: CDR Call Types
- Field 14: CDR Access Types

- Field 15: CDR Termination Types
- Field 23: CDR Error Codes

Finally, you can see the interrelationship of the above fields by referring to Interpreting Your Results.

CDR Record Fields		
Field	**Abbreviation**	**Meaning**
1	**CSN**	**Call sequence number**
2	**DATE**	**Call start date**
3	**TIME**	**Call start time**
4	**STIM**	**Call stop time**
5	**PORT**	**Port number (Module, Port, and Line)**
6	**SYID**	**Server System ID (site code)**
7	**CDUR**	**Call duration**
8	**FMBX**	**From mailbox (when using tree or chain mailbox) or originating mailbox**
9	**TMBX**	**To mailbox (destination mailbox or mailbox called; also mailbox logged into by user)**
10	**FNUM**	**Originating telephone number or network node number**

CDR Record Fields		
Field	**Abbreviation**	**Meaning**
11	TNUM	Destination telephone number or network node number, or mailbox transferred to from a tree or chain mailbox
12	MSG	Server speech message number
13	CT	Call type (see CDR Call Types table)
14	AT	Access type (see CDR Access Types table)
15	TT	Termination type (see CDR Termination Types table)
16	ME	Invalid mailbox entries
17	PE	Invalid Passcode entries
18	MS	Number of messages sent
19	MP	Number of messages played or received
20	MD	Number of messages discarded
21	MK	Number of messages kept
22	TA	Number of failed transfer attempts

CDR Record Fields		
Field	**Abbreviation**	**Meaning**
23	**EC**	**Error code (see CDR Error Codes Table)**

Call Types (Field 13)

CDR allows you to determine different types of calls, which lets you bill them at different rates, for example, or ignore certain types you include in your basic service package. The table below shows the available call types you can track.

Call Type (CT) is the 13th field in each CDR record.

You should use Call Type 1 only when you need as much detail as possible, such as when troubleshooting. It lists every message sent to and from each mailbox. For example, if a user sends one message to a distribution list with four users, and you are logging Call Type 1 messages, CDR generates four records, one for each recipient. If you do not log Call Type 1, CDR still creates one record indicating that a user sent four messages (4 appears in the MS field).

CDR Call Types			
Call Type	**Meaning**	**Call Type**	**Meaning**
01	**Local message delivery (to local mailboxes, by outside caller or user) *Use only when maximum detail needed*.**	**15**	**Incoming Busy-forwarded call**
02	**Outgoing NP WakeUp call**	**16**	**Incoming No-answer-forwarded call**
03	**Telephone call placement**	**17**	**Incoming Indirect**
04	**This call type no longer used**	**18**	**Outgoing NP Net call setup**

CDR Call Types			
Call Type	**Meaning**	**Call Type**	**Meaning**
05	**Paging call or outside message delivery**	**19**	**Incoming NP Net call setup**
06	**This call type no longer used**	**20**	**This call type no longer used**
07	**Outgoing NP Net call**	**21**	**This call type no longer used**
08	**Cut-through paging call**	**22**	**Outgoing NP Net disconnect**
09	**This call type no longer used**	**23**	**Incoming NP Net disconnect**
10	**Incoming NP Net call**	**24**	**This call type no longer used**
11	**Mailbox Purge**	**25**	**This call type no longer used**
12	**Incoming direct call**	**26**	**This call type no longer used**
13	**Incoming direct call - No passcode**	**27**	**NuPoint Voice resource access**
14	**Incoming Call-forwarded call**	**28**	**NP View network access**

Each of these Call Types and their related fields is described in the "Analyzing CDR Data" section.

Networking Application Call Types

NP Net has its own call types (see the table above) that display Call Setup information. These call types only log the time used by the handshaking process to connect a pair of NP Net servers. In addition to the Call Setup message types, NP Net has its own incoming and outgoing call types that log the time used in

transmitting or receiving each individual message between two NP Net servers. Finally, there are two NP Net disconnect call types.

Access Types (Field 14)

Access Type (AT) is the 14th field in each CDR record and shows how the caller or user accessed the server. You can use Access Types for differential billing or to determine your clients' usage of the server. The following table shows the possible access types.

CDR Access Types			
Access Type	**Meaning**	**Access Type**	**Meaning**
01	**Outside caller**	**10**	**This access type no longer used**
02	**Mailbox user**	**11**	**NP Net receipt update**
03	**Mobile DID user**	**12**	**Name broadcast**
04	**Outside caller to template mailbox**	**13**	**Greeting broadcast**
05	**This access type no longer used**	**14**	**Passcode broadcast**
06	**NP View session over TCP/IP network**	**15**	**Message Delivery, billed (all-types)**
07	**Outside caller called into NP Receptionist**	**16-22**	**This access type no longer used**
08	**Message Delivery, non-billed (all types)**	**23-25**	**Reserved for future use**
09	**User accessed Administration-by-Phone functions**	**40**	**NP OnDemand feature**

Termination Types (Field 15)

Termination Type (TT) is the 15th field of each CDR record. It indicates how the call was ended. Again, you can use this for differential billing or to determine your clients' usage of the server. The following table lists the Termination Types available.

Termination Types 1 through 8 are generated at the completion of a call. Types 9 and 10 are for calls that continue after a record is logged. For example, if an outside caller leaves a message and stays on the line to hear the prompt, the caller can then leave a message for another user. CDR creates a second record for the next action the caller performs. This subsequent record indicates the mailbox being used in the From Mailbox field (FMBX, field number 8).

CDR Termination Types	
Termination Type	**Meaning**
00	**Unknown**
01	**Call completed successfully**
02	**Caller/user hung up**
03	**Call failed**
04	**Caller/user disconnected by the server, or three invalid mailboxes entered sequentially, or invalid passcode entries, or no response from caller/user**
05	**Caller/user transferred to an extension**
06	**Caller/user transferred to attendant**
07	**Caller/user transferred to E-mail**
08	**Message delayed by recipient (used with Call Placement)**
09	**Caller/user transferred to mailbox (from tree or chain mailbox)**

CDR Termination Types	
Termination Type	**Meaning**
10	**Caller/user recycled (completed call, performed another function)**

Error Codes (Field 23)

The Error Code (EC) is the 23rd field in the CDR record. It indicates if there was any error or problem with the call. You can use error codes for differential billing (for example, only bill calls with certain codes) or to determine if there is a problem with the server when troubleshooting.

The following table lists the available Error Codes and their meanings.

CDR Error Codes			
Error Code	**Meaning**	**Error Code**	**Meaning**
00	**Unknown error. Contact your support representative.**	**12**	**Message rejected by destination**
01	**Call successfully completed**	**13**	**Mailbox was in use when user called**
02	**Call terminated due to excess invalid mailbox number entry attempts**	**14**	**Could not transfer caller/user to an extension**
03	**Call terminated due to excess invalid passcode entry attempts**	**15**	**Could not transfer caller/user to an attendant**
04	**Timeout on waiting for input**	**16**	**Could not transfer caller/user to E-mail**

CDR Error Codes			
Error Code	**Meaning**	**Error Code**	**Meaning**
05	**Too many bad access code entries**	**17**	**Access to mailbox denied**
06	**Destination was busy**	**18**	**This error code no longer used**
07	**Destination did not answer**	**19**	**This error code no longer used**
08	**Network node does not exist**	**20**	**Time limit reached**
09	**Mailbox does not exist**	**21**	**Message is bad or does not exist**
10	**Invalid telephone number**	**22**	**Destination mailbox is full**
11	**Invalid extension number**	**23**	**This error code no longer used**

26.79.1 CDR Disk Storage

CDR storage space consists of one or more CDR record blocks that are stored in the server account drive. Each block stores up to 64 CDR records. The maximum number of blocks that you can allocate is 15,625, which could store up to 999,999 CDR records. Since each block occupies one account record (also called OAA record), allocating too many blocks for CDR can interfere with the ability of the server to accept or deliver messages.

When you start to change the number of CDR records, the server tells you how many account records are available. Then you can determine how many of those to allocate for CDR records. You can also check Total System Statistics for more details on account record use. Remember, other server applications cannot use any of the space you allocate to CDR.

Maximum Number of Records

The CDR Configuration Menu allows you to set the maximum number of CDR records to be logged on the server before a wraparound takes place. A wraparound occurs when the server has stored the maximum number of records. The next CDR record stored overwrites the oldest block (64 CDR records).

Do not confuse this "wraparound" feature with the "turning over" of the Call Sequence Number. Once the Sequence Number reaches 999999, it resets the next number to 1, like an odometer. However, only the Sequence Number is reset; records or blocks are not overwritten.

Before configuring the CDR application, you should estimate how many records you want to store. Determine how often you want to download your data (for external processing); a typical sequence would be once per week. hen you should note the number of ports (phone lines) your server has, how many calls per time period each port handles, and how many records are stored per call (for example, using a tree or chain mailbox creates two records per call).

Calls x Ports x Days = 100 x 120 x 7 = 84000 records needed

To compute the number of accounting records you need, divide the number of CDR records needed by 64 and round up to the next whole number (integer):

CDR records / 64 records/block = blocks needed

84000 / 64 = 1312.5 Þ 1313 blocks (accounting records)

Monitor your actual server performance to see if your estimate was accurate. It is better to err on the higher side to avoid overwriting the oldest records. The more CDR records you plan to log, the more accounting records you need. Call Type 1, in particular, creates a large number of CDR records. Remember that the accounting records are also used for mailboxes and distribution lists, so you must determine how many of these to allocate to CDR. Once allocated to CDR, you cannot use them for other operations. To make them available again for normal mailbox processing, you would have to lower the maximum number of CDR records and then delete the existing CDR data.

Use this worksheet to compute your server’s storage needs. The sample worksheet below has been filled out with the example used above. Blank worksheets are available in the Appendix.

Sample CDR Disk Storage Space Worksheet		
Instruction	**Your Answer**	**Comments**
1. Ports in NuPoint Unified Messaging server	***120***	
2. Average calls per day	***100***	
3. Number of days between CDR downloads	***7***	
4. Call adjustment	***1***	**CDR records per call, usually = 1**

Sample CDR Disk Storage Space Worksheet		
Instruction	**Your Answer**	**Comments**
5. Multiply ports xcalls x days adjustment (step1 xstep**2 x step 3 x step 4)**	***84000***	**Total CDR records**
6. Divide step5 by 64	***1312.5***	**64 records per block**
7. Round up to next whole number	***1313***	**Record blocks needed**

Changing the Maximum Number

Once you compute how many records you need, enter that number in the **Maximum Number of CDR msgs** parameter. If you type **?** for help, the server indicates how many account records are available. If you change the number of records stored, new storage is not allocated until you exit the CDR Configuration menu.

To use CDR, you must change the default from 0 to a positive number, or you cannot store any records.

If you reduce this number, you must delete the CDR records to free up account records. You do not need to delete after increasing the number of records stored. You can reduce the number of records only if CDR is stopped. Be sure to restart CDR after stopping it to change number of records saved.

The server warns you if you request too many CDR records to allow enough records for normal mailbox and distribution list operation. If you get this warning, it is recommended that you enter a smaller number of CDR records, or it could impact server performance. You are required to leave a minimum of 300 account records in order to run the NuPoint Voice application.

Total System Statistics

This is a **Text Console** menu choice that displays server statistics. Use it to find the total number of available speech blocks, when determining CDR record (message) space. See below for an example of the output.

Check total system statistics before entering CDR, since both are under the Report Generation menu. This way you do not have to exit and reenter CDR. If you only need to know the number of account records, then you can choose the *Max Number of CDR msgs* parameter in the Configuration Menu. The server displays the number of available account records before asking you to enter a new number.

TOTAL STATISTICS SUMMARY REPORT

Fri Apr 21, 1995 12:26 pm

----------< SUNDAY >----------

Date: Sun Apr 16 23:15:07 1995

Last Reset: Sat Apr 15 08:52:55 1995

Total Messages: 90000 Lowest Messages Free: 86377

Total Speech: 384000 Lowest Speech Free: 325480

Total Calls: 0 Total Seconds: 0:00:00

Line ATB Count: 0 Line ATB Seconds: 0:00:00

NETWORKING <========== PEAKS ==========><========== TOTALS =========>

MESSAGES: IN QUEUE MINUTES LATENCY DELIVERED UNDELIV RECEIVED

BATCH: 9 0 0:00:00 0 0 27

URGENT: 0 0 0:00:00 0 - 1

----------< MONDAY >----------

Date: Mon Apr 17 23:15:06 1995

Last Reset: Mon Apr 17 15:14:50 1995

Total Messages: 90000 Lowest Messages Free: 86234

Total Speech: 384000 Lowest Speech Free: 324377

Total Calls: 0 Total Seconds: 0:00:00

Line ATB Count: 0 Line ATB Seconds: 0:00:00

NETWORKING <========== PEAKS ==========><========== TOTALS =========>

MESSAGES: IN QUEUE MINUTES LATENCY DELIVERED UNDELIV RECEIVED

BATCH: 55 0 0:00:00 0 0 354

URGENT: 0 0 0:00:00 0 - 34

Logfile Messages

CDR logs the following message into the server error logfile when the CDR file nears the maximum number of records allowed (see Maximum Number of Records earlier in this section):

<module> <task-ID> <date> <time>: CDR file is X% full at <CSN>

Note:
Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

The parameters are explained in the table below. Error messages are logged when CDR storage is 85, 90, and 95 percent full. Here is a sample message:

1 0341 03/22 3:28:15: CDR file is 85% full at 605123

CDR Log File Parameters	
Parameter	**Meaning**
<module>	**The module (host) number**
<task-ID>	**The task identification number**
<date>	**The current date**
<time>	**The current time**
X	**Percentage of capacity reached (85, 90, or 95)**
<CSN>	**Call Sequence Number being processed at the time**

When CDR storage reaches 100% of the number allowed, the following message is logged to the server error logfile:

<module> <task-ID> <date><time>: CDR space is re-used at <CSN>

At this point, new CDR records are overwritten onto the oldest ones, sequentially. This is called a wraparound. See "Maximum Number of Records" earlier in this section.

Example:

```
1 0341
03/22   3:28:15: CDR file is re-used at
605123
```

Handling New Records

A new CDR record is not written to disk immediately, but is delayed for a certain period of time to reduce disk access. CDR normally writes to disk all records received once every 180 seconds, or when the CDR record block is full (64 records). You can change this delay from anywhere between 10 and 600 seconds with the Maximum Delay parameter.

Decreasing this parameter is not recommended, as it could impact server performance. Increasing this parameter, while improving performance, leaves you at risk of losing more data in the event of a power outage or server failure.

Any changes you make to the report configuration take effect immediately. However, you have to exit the Report Menu in order for the CDR Configuration changes to be saved. New CDR records coming into the server while the report menu is accessed are not always available if you run a report. In order to get the latest records, you might have to exit the Report Menu and then reenter it to include the newest records.

Deleting CDR Records

CDR allows you to erase the contents of the entire CDR storage space. Deleting records does not reset the server's Call Sequence Number, however. For example, if CDR records numbered 100000 through 200000 were stored before you deleted them, the next CDR record received is assigned Call Sequence Number 200001.

Since CDR automatically overwrites old records when storage space is full, it is not necessary to delete records routinely after each download.

You must delete existing CDR records if you are lowering the maximum number of records stored; otherwise, the lower number does not take effect, and the space is not released for use as accounting records.

CDR Disk Storage Worksheet

Worksheet for computing CDR Disk Storage:

Instruction	Your Answer	Comments
1. Ports in NuPoint Unified Messaging server		
2. Average calls per day		

Instruction	Your Answer	Comments
3. Number of days between CDR downloads		
4. Call adjustment		CDR records per call, usually = 1
5. Multiply ports **x** calls x days x adjustment (1 x 2 x 3 x 4)		Total CDR records
6. Divide (5) by 64		64 records per block
7. Round up to next whole number		Record blocks needed

Sample:

Instruction	Your Answer	Comments
1. Ports in NuPoint Unified Messaging server	120	
2. Average calls per day	100	
3. Number of days between CDR downloads	7	
4. Call adjustment	1	CDR records per call, usually = 1
5. Multiply ports **x** calls x days x adjustment (1 x 2 x 3 x 4)	84000	Total CDR Records
6. Divide (5) by 64	1312.5	64 records per block

Instruction	Your Answer	Comments
7. Round up to next whole number	1313	Record blocks needed

26.79.2 Line Numbers

One configuration choice for you to determine is which lines to enable. Lines enabled in the CDR Configuration Menu have their call traffic saved as CDR records.

Each line number is expressed as a *triplet*, where module, slot, and port number are separated by colons (:). If you have a one-module server, you can refer to just the slot and port number. If you have a multi-module server, you must specify the module number as well, or the server assumes you are configuring Module 1 only.

Note:
Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

Module (Host)	Slot	Port (virtual)
NuPoint UM 60 ports = always 1 NuPoint UM 120 ports = always 1 NuPoint UM **640** = specify 1 or 2 (default is 1)	Always 0 for mail ports. Always 5 for fax ports.	0 - licensed port limit, no duplicates allowed OR * for all ports

An example of a triplet is 1:0:2. This means Module 1, Slot 0, and Port 2. This is distinct from 2:0:2, which would be on Module 2, and from 1:0:1 which is Port 1 on the same Module and Slot as the first case. Triplets do not use colons when stored in CDR records; module, slot, and port are two-character numerics in a six-character field. The above triplet is stored by CDR as 010002.

When configuring Line Numbers for CDR, you have several menu options that help you set up the lines you want to monitor. The Enable all Lines option chooses every line in your server automatically. You do not have to worry about how many modules, ports, or lines you have. If you want to use CDR on a subset of your lines, the Enable Individual Lines and Disable Individual Lines options are available. You can specify which lines to add to or subtract from the list of monitored lines. The Show Individual Lines option displays the list of lines that are monitored by CDR.

You can use the wildcard character (*) when specifying which lines to enable or disable. For example, the triplet 2:0:* represents all lines on Module 2, Slot 0. The expression 1:* represents all ports and lines on Module 1 (the second wildcard is redundant). Use the Enable and Disable options to add or remove lines,

and the Show option to verify your selection. If you wish to enable all but a very few lines, your easiest course is to Enable All Lines, then Disable the lines you do not want. You must exit the CDR Configuration Menu in order to save any changes made within these options.

Download your data frequently if you enable all lines; this is the maximum data possible and overwriting can occur if CDR space is used up.

Note: If you enter a triplet and leave out one set of numbers, the server assumes you are specifying Module 1. For example, if you enter 0:4, it assumes Module 1, Slot 0, Port 4.

26.79.3 Configure CDR

This procedure describes how to set the configuration options in CDR Configuration Menu. If you perform this procedure when you set up CDR for the first time, you do not have to do it again unless you need to change a setting.

Note:
If you want to reduce the number of CDR records stored, you must first stop CDR if it is running.

To configure CDR:

1. From the Main menu, select **(R) Reports** and then **(A) Call Detail Recorder** and then **(A) Configure Menu**.
2. Select **(A) Configure Menu**.
3. Do one of the following:

   - To enable all lines, select **(A) Enable all lines** and then enter **Y**.
   - To enable individual lines, select **(B) Enable individual lines** and enter the line triplet that represents the line to add.
4. Select **(E) Call Types** and enter one of the following:

   - **A** for all call types
   - A single call type **number** (1-28), for example, 4.
   - A **range** of call types, for example 1-20.
   - A comma-separated **list** of call types, such as 1,3,5,7.
   - A **combination** of ranges and list, for example 1-4,6,7-9,12.
   - **?** for a list of call types and their definitions.

5. Select **(F) Max number of CDR msgs** and enter a number of CDR records (messages) to store (1-999999).

   - CDR records are stored in blocks of 64 records. It is recommended that you choose a number that is divisible by 64, to maximize disk storage efficiency.
   - If you reduce the number of CDR records stored, the area committed to disk storage is not reduced until you delete the records. If you increase the number of records, disk storage changes when you exit the CDR Configuration Menu.
   - You must leave a minimum of 300 accounting records in order to run the NuPoint Voice application. You are not permitted to leave fewer records than this.

6. Select **(H) Max delay to write CDR records to disk**and enter the delay in seconds (10-600). CDR records are buffered as they come in, and written to disk as the buffer fills. The larger the delay, the fewer disk write operations are performed. This increases the possibility that you could lose some data in the event of a server failure. It is recommended that you not reduce this parameter below the default of 180 seconds.
7. Exit the CDR configuration menu to save your choices. If you reduced the number of CDR messages stored, you must Delete CDR messages first.

26.79.4 Starting and Stopping CDR

Once started, CDR continues to run until you select Stop CDR. If you reset your system, CDR automatically starts up again. If you stop CDR, it remains stopped until you select "Start CDR" again.

To **start** CDR:

1. From the Main menu, select **(R) Reports** and then **(A) Call Detail Recorder**. Ensure that your configuration and report settings are set as required.
2. Select **(B) Start**. The system confirms that CDR is started.
3. Select **(X)** to Exit.

To **stop** CDR:

1. From the Main menu, select **(R) Reports** and then **(A) Call Detail Recorder**. Ensure that your configuration and report settings are set as required. Ensure you are at a good point to stop CDR, such as a low-usage time. When CDR is stopped, it does not log any activity.
2. Select **(C) Stop**. The system prompts you to confirm. Type **stop cdr** (all upper-case or all lower-case) to confirm.
3. The system confirms that CDR is stopped.
4. Select (X) to exit.

26.79.5 Delete Existing CDR Records

This procedure describes how to delete the current CDR messages stored on disk.

Note:
Once messages are deleted, they cannot be restored.

To delete existing CDR messages:

1. From the Main menu, select **(R) Reports Menu**, and then**(A) Call Detail Recorder**.
2. Stop CDR if it is running.
3. Select **(D) Delete**.
4. Select **(A) Delete Messages** and then press **Y** to confirm deletion, or press N to stop the procedure.
5. Exit the CDR menu.

26.79.6 CDR Reports

You can generate on-screen reports of your CDR message data. There are a number of ways to customize these reports, including which messages to include, which fields to include, and how to format your report. Report creation and modification options are available in the CDR Report menu.

Although you cannot use the Web Console to enable or configure CDR, you can use it to produce custom CDR reports.

Report Options

These are the options available in the CDR Report menu. You must exit the Report Menu to save any changes you make here.

Report Details

There are 26 fields, or report details, that can be stored in a CDR record. You can include a subset of the available information in your report, which is the set of information you will later download. If you only need some of the data, you can specify which fields you want to include in the report.

The CDR Record Fields table lists all fields and their descriptions. The following table lists their field lengths and formats, so you can compute your report width and set up your remote application properly.

Call Types

You can select any or all 28 Call Types in your report. In particular, Call Type 1 creates a large number of messages, and you might not want to include it. See CDR Records for a list of Call Types.

Do not confuse specifying which Call Types are stored by the server with which Call Types are included in your report. The former is chosen in the Configuration Menu, the latter in the Report Menu.

CDR Record Field Lengths and Formats			
Field	**Code**	**Length**	**Format**
1	CSN	6	nnnnnn
2	DATE	6	mmddyy (month, day, year)
3	TIME	6	hhmmss (hour, minute, second)
4	STIM	6	hhmmss (hour, minute, second)
5	PORT	6	mmppll (module, port, line)
6	SYID	4	xxxx (first 4 chars of site code)
7	CDUR	4	ssss (seconds)
8	FMBX	14*	nnnnnnnnnnnnn
9	TMBX	14*	nnnnnnnnnnnnn
10	FNUM	16*	nnnnnnnnnnnnnnn
11	TNUM	16*	nnnnnnnnnnnnnnn
12	MSG	7	nnnnnnn
13	CT	2	nn
14	AT	2	nn

CDR Record Field Lengths and Formats			
Field	**Code**	**Length**	**Format**
15	TT	2	nn
16	ME	2	nn
17	PE	2	nn
18	MS	2	nn
19	MP	2	nn
20	MD	2	nn
21	MK	2	nn
22	TA	2	nn
23	EC	2	nn
24	FS	2	nn
25	FP	2	nn
26	PS	2	nn
n = numeric character, x = alphanumeric character, other characters are defined. * = maximum length possible for this variable field. The default length is 11.			

Field Lengths

You can adjust the field lengths of four CDR fields: 8, 9, 10 and 11 (FMBX, TMBX, FNUM and TNUM). These fields contain mailbox or telephone numbers. For example, if all your mailboxes are four characters, you can set fields 8 and 9 (the From and To Mailbox fields) to a length of 4 instead of 11 (the default). This saves space in your output. You can also increase the length of these fields, if necessary.

If your field data is shorter than the field length, the data is right-justified and filled with the string pad character you specify. This pad character is described below.

Field Delimiter

You can specify a field delimiter to make data processing easier on the remote computer system. For example, some processing applications require comma separated fields. The default delimiter is a space between details.

Enter 0 for a space, 1 for a tab, or any other character for another delimiter. Be sure you know what field delimiter is required by the remote application using the data.

Report Width

Once you know how many details to include, and you have determined field lengths for the adjustable details, you can set a width for the report by using the Number of Columns option. This allows you to better view the on-screen report or to allow one entire record on one line for a remote download.

The default is 40 columns, and you can specify a number between 40 and 160. If your CDR records need more columns than your screen can display, it wraps extra characters to a second or third line. Select a width based on whether you want to display the report on your server console or download the data. Use the larger widths for downloading. Most VT-100 terminal displays are 80 columns wide--72 or 80 is a good choice for these terminals.

When setting this parameter, be aware of how many details you specified for your report, and the field lengths you set. This ensures that your report is readable without unexpected wraparound.

Call Sequence Number Range

You can adjust your report to include all CDR records, or a range of records, by choosing a starting and ending Call Sequence Number. By determining when certain calls were placed, this feature allows you to report messages for a specific time period.

CDR assigns consecutive sequence numbers to each call until number 999999; the next call is assigned number 1. If CDR exceeds its maximum number of records, it overwrites the oldest record. However, the newest record does not reuse the oldest record’s sequence number. Either of these occurrences can cause the ending number to be lower than the starting number for a particular time period. A lower ending sequence number is no problem for CDR, but you should be aware of the possibility.

Search Capability

You can specify a search string for your report using the Search For option. This is useful if you want to see data for a particular mailbox or telephone number. Your search string can be up to 160 characters. Enter a period (.) to reset the search to blank.

Since you cannot specify the position of your search string, searches for a particular call type, such as "01," are meaningless. Your results list all occurrences of "01" anywhere in all CDR records. The feature is best used for finding longer strings, such as telephone or mailbox numbers.

To ensure you are finding a particular string, use the delimiter character as a boundary. This prevents finding your string within a larger field. For example, if you are searching for mailbox 5760, and enter the search string 5760, you also find records with the DN 4085555760 and 2125760555. To prevent this, use the search string " 5760 " (this example assumes a space is your delimiter and that your mailbox field lengths are set to four characters).

String Pad Character

You can specify which character to use to pad data fields. The default is 0 (zero). Padding is used when the result takes up fewer characters than the space allotted for the field. For example, if your mailbox fields are 11 characters, and a record contains four-digit mailbox information, a pad character of zero results in 00000001234. If you change the pad character to a space, your result is 1234.

Note:
You cannot enter a period (.) as your string pad character.

Sample Output

The figure below shows a sample of CDR report output. The delimiter is a blank, and all report details (fields) are shown. The report width is set to 80, so each CDR record is on two lines (this avoids splitting any of the data fields). The field lengths are set to 11 (the default), and are zero-filled (that is, padded with leading zeroes).

This report was created by the Generate On-Screen Report option.

275282 071892 025245 025250 0412 0000 0005 00000000000 00000003563 00000000000 55223183563
0000000 05 08 01 00 00 00 00 00 00 00 01 00 00 00

275284 071892 025236 025422 0401 0000 0106 00000000000 00000003565 00000000000 00000000000
0622073 17 02 02 00 00 01 00 00 00 00 01 00 00 00

275290 071892 034454 034517 0213 0000 0023 00000000000 00000003728 00000000000 00000000000
0000000 16 02 01 00 00 00 00 00 00 00 01 00 00 00

275294 071892 044933 045039 0413 0000 0066 00000000000 00000003561 00000000000 19134510876
0623891 04 08 01 00 00 00 00 00 00 00 01 01 00 02

275371 071892 081446 081903 0000 0000 0257 00000005223 00000076582 00000000001 00000000140
0622103 07 08 01 00 00 00 00 00 00 00 01 00 00 00

275459 071892 101125 101135 0307 0000 0010 00000000000 00000003001 00000000000 00000000000
0000000 12 01 01 00 00 00 00 00 00 00 01 00 00 00

275908 071992 100211 100237 0314 0000 0026 00000000000 00000000000 17035504009 00000000000 0000000 21 08 01 00 00 00 00 00 00 00 01 00 00 00

275912 071992 100237 100345 0314 0000 0068 00000004000 00000003512 17035504009 00000000000 1015499 09 08 01 00 00 01 00 00 00 00 01 00 00 00

Sample CDR Report Output

There are also report options that create immediate results. Display CDR Statistics produces the following output:

REPORT STATISTICS:

Call Sequence Number of oldest message: 1633

Call Sequence Number of next message: 1642

Display Download Statistics produces the following output:

DOWNLOAD STATISTICS:

Most recent Call Sequence Number: 230

Most recent Record: 2

Download Start Time: 1-Sep-92 5:05:21 pm

Download Stop Time: 1-Sep-92 5:05:57 pm

Download Result: OK

The download statistics are only updated when you download new CDR records. If you select a range of Sequence Numbers to download, the statistics are not affected.

26.79.7 Set CDR Report Options

This procedure describes how to set or change the options in CDR Report Menu. None of the following commands are required to create a report. If this procedure is properly done once, you do not have to do it again unless you need to change a setting.

To set CDR Report Options

1. From the Main menu, select **(R) Reports** and then **(A) Call Detail Recorder** and then **(D) Report Menu**.

2. Select **(A) Details** and enter any of the following:

   - **A** for all call details
   - A single call detail **number** (1-26), for example, 9
   - A **range** of call details, for example 10-23
   - A comma-separated **list** of call details, such as 11,13,15,17
   - A **combination** of ranges and list, for example 1-4,6,7-9,12
   - **?** for a list of call details and their definitions

3. To change field lengths, select **(B) Field Lengths** and select the field length to change:

   - **A** for Source Mailbox
   - **B** for Destination Mailbox
   - **C** for Source Node or Number
   - **D** for Destination Node or Number

4. When prompted for field length, enter a**number**for the length of the field you selected: Source and Destination Mailbox field length (1-14) or Source and Destination Number field length (1-16). Repeat this step until you have changed all field lengths you wish to. Then exit the Field Length Menu to save the new field lengths.
5. Select (C) Call Types and enter one of the following:

   - **A**for all call details
   - A single call detail **number** (1-26), for example, 9
   - A **range** of call details, for example 10-23
   - A comma-separated **list** of call details, such as 11,13,15,17
   - A **combination** of ranges and list, for example 1-4,6,7-9,12
   - **?** for a list of call details and their definitions

Note:
You must select the call types you want in the CDR Configuration Menu to store them in CDR Records. If you select them in the CDR Report Menu and not in the CDR Configuration Menu, you will not have the information.

1. Select **(D) Field delimiter character** and enter the field delimiter to separate data fields in your report. Enter **0** for a space, **1** for a tab, or enter any other printable ASCII character.
2. Select **(E) Starting Call Sequence Number** and enter the call sequence number (1-999999) at which to start.
3. Select **(F) Ending Call Sequence Number** and enter the ending sequence number.
4. Select **(G) Number of columns** and enter a report width in number of columns (40-160).
5. Select **(J) Search for** and enter a search string (1-160 characters). To ensure your search checks the correct field, use the field delimiter character as a boundary in your search string. For example, to find occurrences of mailbox number 5678, enter " 5678 "(assuming mailbox field length is set to 4 and the field delimiter character is a space).
6. Select **(K) String pad character** and select a character to fill any right-justified fields in the report (the default character is '0').
7. Exit the CDR menu to save your choices.

26.79.8 Create CDR Report

To create a CDR report:

1. Ensure that you have set up CDR report options.
2. From the Main menu, select **(R) Reports** and then **(A) Call Detail Recorder** and then **(D) Report Menu**.
3. Select **(H) Generate onscreen report**. The report displays on your console screen. If your console is connected to a printer, you can send the report there.
4. When the report is complete, exit the CDR Report menu.

26.79.9 Run a Call Detail Record Report

1. In the navigation tree, click Report Generation >Call Detail Record.
2. On the **Record Description** tab, enter Time Range, Mailbox Range, and Call Types data as described in the table below.
3. On the **Field Selections** tab, select the CDR fields that you want included in the report.
4. Click OK. To print the report, click **Printer Friendly Version**. To save the report as a CSV tile, click**Export to CSV File**.

Call Detail Record Fields Description

Record Description Tab Fields	Description
Time Range:	
Unlimited	Includes all time ranges.
From Date	Select a start date from the drop-down lists. Or click the Calendar pop-up and select a date.
To Date	Select an end date from the drop-down lists. Or click the Calendar pop-up and select a date.
From Time	Enter start time in 12 Hr and 60 min format (00:00-12:59).
To Time	Enter end time in 12 Hr and 60 min format (00:00-12: 59).
Mailbox Range	
All Mailboxes	Default
Mailbox Range	Maximum 25 digits. Mailbox numbers separated by a hy phen (for example, 2002-2050).
Call Types	
All Call Types	Default

Record Description Tab Fields	Description
Range	Range is 01-28. Only one continuous range is allowed (for example, 2002-2050). Call Types are: • 01 - Local message delivery (to local mailboxes, by outside caller or user) Use only when maximum detail needed. • 02 - Outgoing NP-UM WakeUp call • 03 - Telephone call placement • 04 - (This call type no longer used) • 05 - Paging call or outside message delivery • 06 - (This call type no longer used) • 07 - Outgoing NP-UM Net call • 08 - Cut-through paging call • 09 - (This call type no longer used) • 10 - Incoming NP-UM Net call • 11 - Mailbox Purge • 12 - Incoming direct call • 13 - Incoming direct call - No passcode • 14 - Incoming Call-forwarded call • 15 - Incoming Busy-forwarded call • 16 - Incoming No-answer-forwarded call • 17 - Incoming Indirect • 18 - Outgoing NP-UM Net call setup • 19 - Incoming NP-UM Net call setup • 20 - (This call type no longer used) • 21 - (This call type no longer used) • 22 - Outgoing NP-UM Net disconnect • 23 - Incoming NP-UM Net disconnect • 24 - This call type no longer used • 25 - (This call type no longer used) • 26 - (This call type no longer used) • 27 - NuPoint Voice resource access • 28 - NP-UM View network access
Field Selection Tab Fields	Description

Record Description Tab Fields	Description
Field Selections	• Call sequence number (disabled, selected by default) • Call start date (disabled, selected by default) • Call start time (disabled, selected by default) • Call stop time • Port number • System ID (disabled, selected by default) • Call duration (disabled, selected by default) • From mailbox • To mailbox • Speech message number • Call type • Access type • Termination type • Invalid mailbox entries • Invalid passcode entries • Number of messages sent • Number of messages played/received • Number of messages discarded • Number of messages kept • Number of failed transfer attempts • Error code • Number of fax messages sent • Number of fax messages played • Number of fax pages

26.79.10 Interpreting Your Results

Your billing software can evaluate certain CDR fields in order to determine which of several possible mailbox transactions occurred. See the CDR Record Field Relationships table below for the values these fields can take. Explanations are abbreviated somewhat, but each field has a cross-reference back to its full table if you need more explanation. Refer to this field relationship table as you follow the examples listed below.

For example, there is a clear relationship between the TIME (call start time) and STIM (call stop time) fields, along with the CDUR (call duration) field. If STIM minus TIME is not equal to CDUR, this suggests either a problem or other user actions on the server. FMBX and TNUM are related when using a tree or chain mailbox; FMBX is the one dialed into, and TNUM is the mailbox transferred to.

The examples in this section show how you can use CDR for your billing application. Refer to each call type and the possible field values for successful and failed calls. Your application should examine these fields when creating bills for your customers.

Useful fields for processing call types are shown in the table below. Other recommended fields are listed within each call type's section.

CDR Record Field Relationships

CDR Field	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
CDR Field Abbreviation (Table 2-1)	CSN	DATE	TIME	STIM	PORT	SYID	CDUR	FMBX	TMBX	FNUM	TNUM	MSG	CT	AT	TT	ME	PE	MS	MP	MD	MK	TA	EC	FS	FP	PS

Value	Call Type(Field 13)	Access Type(Field 14)	Termination Type (Field 15)	Error Code(Field 23)
01	Local message delivery	Outside caller	Call completed	Call successfully completed
02	Outgoing NP Wake Up call	Mailbox user	Caller/user hung up	Excess entry attempts
03	Telephone call placement	Mobile DID user	Call failed	Excess passcode attempts
04	This call type no longer used	Outside caller to template mbox	Disconnected by the server	Timeout on waiting for input
05	Paging call	This access type no longer used	Transferred to an extension	Excess bad access code entries
06	This call type no longer used	NP View session over TCP/IP	Transferred to attendant	Destination was busy
07	Outgoing NP Net call	Outside caller to AutoAttendant	Caller/user transferred to E-mail	Destination did not answer
08	Cut-through paging call	Message delivery, non-billed	Message delayed by recipient	Network node does not exist
09	This call type no longer used	Accessed Admin-by-Phone	Tree/chain mbox xfer to mailbox	Mailbox does not exist
10	Incoming NP Net call	This access type no longer used	Caller/user recycled	Invalid telephone number
11	Mailbox Purge	NP Net receipt update		Invalid extension number
12	Incoming direct call	Name broadcast		Message rejected by destination
13	Incoming direct call-no passcode	Greeting broadcast		Mailbox in use when user called
14	Incoming call-forwarded	Passcode broadcast		Could not transfer to extension
15	Incoming busy-forwarded	Message delivery, billed		Could not transfer to attendant
16	Incoming no answer-forwarded	This access type no longer used		Could not transfer to E-mail
17	Incoming indirect	This access type no longer used		Access (to mailbox) denied

Value	Call Type(Field 13)	Access Type(Field 14)	Termination Type (Field 15)	Error Code(Field 23)
18	Outgoing NP Net call setup	This access type no longer used		This error code no longer used
19	Incoming NP Net call setup	This access type no longer used		This error code no longer used
20	This call type no longer used	This access type no longer used		Time limit reached
21	This call type no longer used	This access type no longer used		Message is bad or does not exist
22	Outgoing NP Net disconnect	This access type no longer used		Destination mailbox is full
23	Incoming NP Net disconnect			This error code no longer used
24	This call type no longer used			
25	This call type no longer used			
26	This call type no longer used			
27	NuPoint Voice resource access			
28	NP View network access			
40		NP OnDemand		

Abbreviations: xfer=transfer mbox = mailbox VM=NuPoint Voice

Useful Fields for Processing All Call Types		
CDR Field	Field #	CDR Field Description
CSN	1	Call sequence number
DATE	2	Call start date
TIME	3	Call start time
STIM	4	Call stop time
PORT	5	Port number (module and line)
CDUR	7	Call duration
CT	13	Call type
AT	14	Access type
TT	15	Termination type
EC	23	Error code

Each call type has a table of values for successful completion or failure to complete the call. In most cases, the access type, termination type, and error code always contain the same values, regardless of the call type. These values are listed here:

Standard Field Values for Most Call Types		
CDR Field, #	**Success**	**Failure**
AT (14	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	varies

If a call type generates different values than listed in this table, these values are shown in **bold type**. Error code values for call failure vary with the call type, so check each call type's table for a list of expected error code values.

Example of CDR Results

Here is a sample call.

An outside caller reached chain/tree mailbox 2000, then logged into mailbox 2001, made a message, logged out of mailbox 2001, then pressed a key to recycle to another NuPoint Voice session. The resulting CDR output is shown here:

275284 071892 025236 025422 0401 0000 0106 00000000000 00000002000 00000000000 00000002001 0000000 **17 02 09** 00 00 00 00 00 00 00 01 00 00 00

275285 071892 025423 025830 0401 0000 0247 00000002000 00000002001 00000000000 00000000000 0622073 **17 02 10** 00 00 01 00 00 00 00 01 00 00 00

The bold type shows Call Type 17 (Incoming), with Access Type 02 (Mailbox User), Termination Types 09 (Tree/chain mailbox transfer) and 10 (Recycle).

In addition, the first record shows no FMBX (outside caller), a TMBX of 2000 and a TNUM of 2001. The second record shows a FMBX of 2000 and a TMBX of 2001, indicating that the caller accessed 2001 through a chain or tree (2000).

26.80 Processing Each Call Type

Following are the relevant fields and expected values for you to use in processing each call type.

Call Type 1 (Local Message Delivery)

Call Type 1 is used for transmitting messages to mailbox users from other users. See Call Types 12-17 for handling messages received from an outside caller.

CAUTION:

Call Type 1 creates numerous CDR records, which are the details of Call Types 8 though 17. In particular, enabling Call Type 1 creates a CDR record for every mailbox in a distribution list or broadcast mailbox. Unless you need the specifics of Call Type 1, do not enable it in the Configuration Menu.

Field Values for Call Type 1		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	**08 (delivery)** **14 (passcode broadcast)**	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	**09(mailbox bad or does not exist)** **12(destination mailbox can't receive msg)** **17(message denied: wrong FCOS)** **21(cannot allocate msg for destination mbox)** **22(mailbox is full)**

Other useful fields:

FMBX (8) Mailbox originating the message **TMBX (9)** Destination mailbox to which the message is delivered to **MSG (12)** The server's speech message number **MS (18)** Number of messages sent (usually 1)

Call Type 2 (Outgoing Auto-Wakeup)

This is an outgoing call made by the server. You can determine whether the outgoing number involves long-distance charges in processing this call type.

Field Values for Call Type 2		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)

Field Values for Call Type 2		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
EC (23)	01 (no error)	**06(destination telephone was busy)** **07(call was not answered)** **10(bad destination telephone number)**

Other useful fields:

TMBX (9) Mailbox number of the message originator **TNUM (11)** Destination telephone number dialed by server **MS (18)** Number of messages sent (usually 1)

Call Type 3 (Telephone Call Placement)

Call Type 3 indicates a message sent to an outside telephone number. While this is similar to a Call Type 2, additional Termination Types are possible on call failure. There are also more possible resulting Error Codes.

Field Values for Call Type 3		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	**03 (failure)** **04(disconnected)** **08(delayed)**

Field Values for Call Type 3		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
EC (23)	01 (no error)	**03(excess invalid passcode attempts)** **06(destination telephone was busy)** **07(call was not answered)** **09(originating mailbox is bad)** **10(bad destination telephone number)** **12(rejected by recipient)** **21(message is bad or no longer exists)**

Other useful fields:

TMBX (9) Mailbox number of the message originator **TNUM (11)** Destination telephone number dialed by the server **MSG (12)** The server's speech message number

Call Type 5 (Paging or Message Delivery)

Call Type 5 can be either a paging or a message delivery call. Both types involve the server calling a telephone number specified by the user. Any field not specified below as specifically paging or message delivery applies to any Call Type 5 record. In the Error Code field, the first three errors apply to paging and message delivery, and the last three errors only to message delivery.

The paging portion of Call Type 5 is similar to Call Type 2. Fields vary for the Message Delivery portion. Message delivery is also similar to Call Type 2, but since the called party has to log into a mailbox and enter a passcode, the resulting field values are different.

Field Values for Call Type 5		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	**08 (delivery)** ***Paging***	**08 (delivery)** ***Paging***
	02(user logged in, got msg) ***Message Delivery***	**01(call received by non-subscriber)** ***Message Delivery***
	15(user logged in, got msg, bill flag set) ***Message Delivery***	

Field Values for Call Type 5		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
TT (15)	01 (success)	**03 (failure) *Paging*** **04(disconnected) *Message Delivery***
EC (23)	01 (no error)	**06(destination telephone was busy)** **07(call was not answered)** **09(mailbox is bad or doesn't exist)** **10(bad destination telephone number)** **03(excess invalid passcodes) *Message Delivery*** **04(timeout or no response) *Message Delivery***

Other useful fields for both Paging and Message Delivery:

TMBX (9) Mailbox number of the message originator **TNUM (11)** Destination telephone number dialed by the server **MSG (12)** The server's speech message number

These fields are only used in Message Delivery calls:

MP (19) Number of messages played or received

If a paging message is unsuccessful, any retry of the message creates an additional Type 5 record.

You can tell the difference between a Paging and a Message Delivery record by checking if any of the above four fields are greater than zero. Look for the Messages Played (MP) field, as the purpose of Message Delivery is to notify a user that there are unplayed messages in the mailbox.

Call Type 7 (Outgoing NP Net)

Call Type 7 is similar to Call Type 2, except it involves networking. This call should be preceded by a header record of Call Type 18 or another Call Type 7. It should be followed by another Call Type 7 or a disconnect of Call Type 22. Verify that these calls occurred on the same line number by checking the PORT field.

Field Values for Call Type 7		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	**04(timeout occurred)** **08(invalid destination node)** **23(bad link)**

Other useful fields:

FMBX (8) Mailbox number of the message originator **TMBX (9)** Destination mailbox number **TNUM (11)** Network node number of destination mailbox **MSG (12)** Message number of the message sent

Call Type 8 (Cut-Through Paging)

Call Type 8 is similar to Call Type 5 (paging). You should examine the telephone number called to determine long-distance charges, if any.

Field Values for Call Type 8		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	**04(timeout or no response)** **06(destination telephone was busy)** **07(call was not answered)** **10(bad destination telephone number)**

Other useful fields:

TMBX (9) Mailbox number of the message originator. **TNUM (11)** Destination telephone number dialed by the server.

Call Type 10 (Incoming NP Net)

Call Type 10 is similar to Call Type 1, except it involves networking. This call should be preceded by a header record of Call Type 19 or another Call Type 10. It should be followed by another Call Type 10 or a disconnect of Call Type 23. Verify that these calls occurred on the same line number by checking the PORT field.

Field Values for Call Type 10		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	**08 (delivery)** **11(receipt update)** **12(name broadcast)** **13(greet broadcast)** **14(passcode broadcast)**	**08 (delivery)** **11(receipt update)** **12(name broadcast)** **13(greet broadcast)** **14(passcode broadcast)**
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	**04(timeout occurred)** **09(mailbox bad or no longer exists)** **17(delivery of msg to destination mbox denied)** **22(destination mbox was full)**

Other useful fields:

FMBX (8) Mailbox number of the message originator **TMBX (9)** Destination mailbox number **FNUM (10)** Message originator's network node number **TNUM (11)** Network node number of destination mailbox **MSG (12)** Received message's number, created by the server

Call Type 11 (Mailbox Delete on Purge)

Call Type 11 is not really a call type, but a status update. A CDR record with a Call Type 11 indicates that the mailbox associated with it (FMBX) was purged either because its messages were played or because its unplayed messages retention limit (in its LCOS) had expired. This is associated with the NP OnDemand optional feature, where mailboxes are only created as callers request them.

See "Call Types 12 Through 17" for additional information on how CDR handles the NP OnDemand feature. For more information on NP OnDemand, refer to its documentation.

Field Values for Call Type 11		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	

Other useful fields:

FMBX (8) Mailbox number deleted

Call Types 12 Through 17 (Incoming)

Call Types 12 through 17 produce the same field results, so they are presented as one type in this section. Table 6-12 shows the distinction between these six Call Types.

Call Types 12 Through 17	
Call Type	**Definition**
12	Incoming directly to mailbox
13	Incoming directly to mailbox with no passcode required
14	Incoming hard-forwarded to mailbox
15	Incoming busy-forwarded to mailbox
16	Incoming forwarded to mailbox on Ring No Answer
17	Incoming indirect (tree/chain, recycle to another mailbox)

Note: In most other call types, the standard result for the access type field (AT, 14) is 08 (delivery. This result should *not* occur with the Incoming call types.

These call types have a number of possible results for access type and termination type. Use the error code to determine call success or failure.

The field values for Call Types 12-17 are listed in Table 6-16. Other useful fields for Call Types 12 through 17 are:

FMBX (8) Mailbox number (if available) of mailbox accessed/entered **TMBX (9)** Mailbox number of mailbox accessed or destination mailbox **TNUM (11)** Mailbox/extension number transferred to after TMBX **MSG (12)** Message number of the last message recorded or accessed **ME (16)** Invalid mailbox entries **PE (17)** Invalid passcode entries **MS (18)** Number of messages sent **MP (19)** Number of messages played/ received **MD (20)** Number of messages deleted **MK (21)** Number of messages kept **TA (22)** Number of failed transfer attempts **P S (26)** Number of cut-through pages initiated by the caller

Field Values for Call Types 12-17		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
AT (14)	**01(outside caller)** **02(mailbox user/subscriber)** **03(mobile DID user)** **04(template mailbox caller)** **05This value no longer used** **07(outside caller to Receptionist)** **09(user accessed Admin-by-phone)** **10This value no longer used** 40(mailbox on demand)	**01(outside caller)** **02(mailbox user/subscriber)** **03(mobile DID user)** **04(template mailbox caller)** **05This value no longer used** **07(outside caller to Receptionist)** **09(user accessed Admin-by-phone)** **10This value no longer used** 40(mailbox on demand)
TT (15)	**01 (success)** **02(caller/user hang up)** **04(NuPoint Voice disconnected call)** **05(caller/user transfer to extension)** **06(caller/user transfer to attendant)** **07(caller/user transfer to E-mail)** **08(transfer to another mailbox)**	**02(caller/user hang up)** **03 (failure)** **04(Server disconnected call)** **05(caller/user transfer to extension)** **06(caller/user transfer to attendant)** **07(caller/user transfer to E-mail)** **08(transfer to another mailbox)**

Field Values for Call Types 12-17		
CDR Field, #	**Successful Delivery**	**Failed Delivery**
EC (23)	01 (no error)	**02(too many bad mailbox entries)** **03(too many bad passcode entries)** **04(time out occurred)** **05(too many bad access code entries)** **13(mailbox in use when user called)** **14(could not transfer to extension)** **15(could not transfer to attendant)** **16(could not transfer to E-mail)** **17(access to mailbox was denied)** **20(time limit reached)** **22(destination mailbox was full)**

NP OnDemand is an Optional Feature. When a mailbox is created, the access type is 40, with an error code of 0 showing successful creation. The first record for an NP OnDemand mailbox contains the first message sent. Subsequent messages to this mailbox have access types used for existing messages. When the mailbox is purged, the server creates a CDR record showing Access Type 40 and Call Type 11.

For more information on the feature, refer to the NP OnDemand documentation.

Call Type 18 (Outgoing NP Net Setup)

Call Type 18 is similar to Call Type 2, except for the network node number. However, it is used as a header record, and should be followed by one or more Call Type 7 (Outgoing NP Net call) records, and finally a Call Type 22 (Outgoing NP Net disconnect). Your billing application should log all such records on the same line number, so check the PORT field.

Field Values for Call Type 18		
CDR Field, #	**Successful Call Setup**	**Failed Call Setup**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	**04(timeout occurred)** **06(destination server was busy)** **07(destination server did not answer)** **08(invalid destination node)** **23(could not establish network link with destination server)**

Other useful fields:

TNUM (11) Network node number of destination mailbox

Call Type 19 (Incoming NP Net setup)

Call Type 19 is similar to Call Type 1, except for the network node number. However, it is used as a header record, and should be followed by one or more Call Type 10 (Incoming NP Net call) records, and finally a Call Type 23 (Incoming NP Net disconnect).

Field Values for Call Type 19		
CDR Field, #	**Successful Call Setup**	**Failed Call Setup**
AT (14)	08 (delivery)	08 (delivery)
TT (15)	01 (success)	03 (failure)
EC (23)	01 (no error)	**04(timeout occurred)** **23(could not establish network link with remote server)**

Other useful fields:

FNUM (10) Network node number of message originator (if available)

Call Types 22, 23 (Outgoing/Incoming NP Net disconnect)

Call Types 22 and 23 always report a successful disconnect. The fields should yield the standard results. Call Type 22 should be preceded by a Call Type 18 (Outgoing NP Net call setup) record and one or more Call Type 7 (Outgoing NP Net call) records. Call Type 23 should be preceded by a Call Type 19 (Incoming

NP Net call setup) record and one or more Call Type 10 (Incoming NP Net call) records. In tracking these call chains, verify that they all occurred on the same line number (PORT field).

Field Values for Call Types 22-23	
CDR Field, #	**Successful Disconnect**
AT (14)	08 (delivery)
TT (15)	01 (success)
EC (23)	01 (no error)

Other useful fields:

TNUM (11) Network node number of dest. mailbox (for outgoing calls) **FNUM (10)** Network node number of originator (for incoming calls)

Call Types 24 Through 27 (E-Mail)

Call Types 24 through 27 are used with e-mail applications. CDR records for e-mail applications are generated by specific applications, with format specific to the application. Refer to the documentation for e-mail applications for more information. Additional call types are reserved to allow for future and custom e-mail applications. Contact your support representative for more information on using CDR with e-mail.

Field Values for Call Type 24-27		
CDR Field, #	**Success**	**Failure**
AT (14)	**05This value no longer used** **10This value no longer used** **16-22These values no longer used**	00 (unknown error)
TT (15)	07(Caller transferred to e-mail)	03 (failure)
EC (23)	01 (no error)	**16(E-mail access failed)** **19This value no longer used**

Other useful fields:

TNUM (11) Network node number of dest. mailbox (for outgoing calls) **FNUM (10)** Network node number of originator (for incoming calls)

Call Type 28 (NP View)

Call Type 28 shows a call made through the NP View application. Here are the possible values.

Field Values for Call Type 28		
CDR Field, #	**Success**	**Failure**
AT (14)	06 (session over TCP/IP)	
TT (15)	01 (success)	04 (disconnect)
EC (23)	00 (unknown error)	

Other useful fields:

TMBX (9) Destination mailbox **FNUM (10)** Network node number of originator (for incoming calls)

Note:
The PORT field should contain the low-word of the IP address instead of a triplet.

26.81 Hacker Detection

You can monitor attempted server break-ins with CDR. If the termination type (Field 15 or TT) equals 4 (Caller/user disconnected by the server), then the mailbox fields (FMBX and TMBX) will have invalid numbers you can examine. The invalid mailbox and passcode fields (Fields 16 and 17, ME and PE) would have entries. FMBX, TMBX and TNUM then contain the three invalid numbers. Fields names are specified in the CDR Fields table, and termination types in the CDR Termination Types table. An example of how the CDR output might look is shown here:

275284 071892 025236 025422 0401 0000 0106 00000000000 **00000019999 00000012345** 00000000000 **00000054321** 12 01 **04 02 01** 00 00 00 00 00 01 00 00 00

26.82 Description

Call Director is an optional feature that you can use to create automated attendant and call processing applications, known as *call flows*, for your organization, departments, and for individual mailboxes and extensions. A call flow is a collection of call-processing actions that control how an incoming call is handled. Without Call Director, NuPoint Unified Messaging simply sends an incoming call to the called person's voice mailbox.

Call flow actions direct NuPoint Unified Messaging to:

- Play a message
- Perform a call transfer
- Forward a call to a specified voice mailbox, extension, external phone, or the Dial-by-Name application
- Send a page or a text message, or
- Hang up

Call flow owners can be either the mailbox owner or the System Administrator. End users can program personal call flows that are associated with their own voice mailboxes. The Administrator can manage personal call flows as well as corporate call flows that are applied to line groups. The Administrator is also responsible for the global configuration settings that determine how individual call flows work. These settings include call transfer sequences, valid extension lengths, attendant's extension number, and time-outs.

You can configure Call Director using either the Text console or the Web console but all interactions with Call Director are made using the **Web Console** and the Telephone User Interface (TUI). The TUI is used for audio recording and to enable and disable the "Override" call flow action.

Call Director functionality includes the ability to edit line group configuration, edit a call flow, create call flow templates and generate Call Director reports.

Note:
Call redirection features such as call forwarding can be overridden only from Call Director, not from the NP Receptionist.

Conditions

Call Director is a licensed option activated by FCOS bit **292** (Enable NP Call Director). Each desktop with the required FCOS bit consumes one license. If you have 400 Call Director licenses and you configure 500 users with FCOS 292, only 400 of those users have access to Call Director.

Note:
Call Director replaces NP Agent. NP Agent and Call Director are NOT compatible; any NuPoint Agent call box applications you want to use in Release 9.0 or later, must be recreated in Call Director.

26.82.1 Call Director - Configuration

To configure the Call Director optional feature:

1. Make Call Director available to users by assigning an FCOS that includes feature bit **292** (Enable NP Call Director). This bit causes the Call Director tab to be displayed in the Web View interface.

Note:
Ensure that you have adequate Call Director licenses before adding the bit to an FCOS. Call Director is licensed on a per-mailbox basis. If you assign the Call Director FCOS to more mailboxes than you have Call Director licenses for, then the feature may work only intermittently. To avoid this situation, verify the number of Call Director licenses you have assigned before assigning the FCOS to mailboxes.

To verify how many licenses you have:

1. Use the **Text console** to run the Call Director Database Report. This will give you listings of how many Call Director Mailboxes are in use and which mailboxes are using them.

Note:
When you assign an FCOS containing the Call Director bit **292** (Enable NP Call Director) to a mailbox, the mailbox is not immediately enabled with the Call Director feature. A Call Director Database update (below) is required to enable Call Director for new users.

To update the Call Director database:

2. You can wait for the automatic update that is done at midnight every night, or you can perform a manual update. To perform a manual update from the **Text console** Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(H) Update Call Director Database**.
3. Create a Line Group for Call Director.

26.82.2 Call Director - Operation

To access Call Director in the Web Console:

1. Access the Web Console.
2. In the Address bar of your browser, type the following URL, substituting the actual hostname or IP address of your NuPoint UM server:

   http://*<hostname or IP address of server>*/**npm-admin**
3. On the Web Console login page, enter your Administrator user name and password.
4. In the navigation tree, click **Call Director**. From here you can configure properties and manage call flows.

Note:
For detailed instructions, see the **Call Director** section of this guide, located directly after this (Optional Features) section.

To access Call Director TUI functions:

1. Log into your NuPoint UM Administrator voice mailbox.
2. Press *.

- Do one of the following:
- To administer templates, press **2**.
- To administer user call flows, press **8**.
- To administer line group call flows, press **5**
- Do one of the following:
- Enter the voice mailbox number of the user whose personal call flow you want to modify.
- Enter the line group number of the corporate call flow that you want to modify.
- Press **#**, and then follow the voice mail prompts to do one or more of the following.
- Enable or disable Override.
- Listen to a current message, or record a new message.

For more information, see the *Mitel TUI Quick Reference Guide* available at Mitel Online.

26.83 Competitive TUI Emulation - Description

The Competitive TUI Emulation feature provides a telephone user interface (TUI) that emulates the TUI of other commonly used voice mail systems. You can assign this feature to users who are familiar with a competitive TUI so that they do not need to learn the NuPoint Unified Messaging TUI. Users can use the Competitive TUI for common functions including playing, saving, making, forwarding, answering, and deleting messages, as well as reaching user options. Outside callers and administrators, however, must use the standard NuPoint Unified Messaging TUI.

This feature is controlled for individual mailboxes through FCOS feature bit **288**, Enable TUI Emulation and by the LCOS Prompt language selection, "TUI Emulation".

Conditions

Competitive TUI Emulation is not supported for use with

- The Administrator's mailbox
- Billing information enabled by feature bit 276
- The Enhanced Auto Wakeup feature of the NP WakeUp optional feature, enabled by feature bit 287
- The Speech Navigation feature, enabled by feature bit 99
- Feature bits 158 (Continue Sending Message), 276 (Press 0 for More Billing Info), 287 (Enable Enhanced Auto Wakeup), and 300 (Enable Secure Tutorial).

Installation

You install the Competitive TUI Emulation option and the required prompts from the NuPoint UM software installation CD/DVD. Follow the instructions for Optional Feature installation.

26.83.1 Competitive TUI Emulation - Configuration

To configure Competitive TUI Emulation, use the Text console:

1. Customize an FCOS to include feature bit **288** (Enable TUI Emulation).
2. Create an LCOS with the language set to **TUI Emulation**. Set any other LCOS settings required for the user.
3. For the required mailboxes, assign the customized FCOS and LCOS.

26.83.2 Competitive TUI Emulation - Operation

You can use the TUI Emulation feature to play, save, make, give, answer, and delete messages, or to reach the User Options menu.

To use the TUI:

1. Log in to your mailbox.
2. At the Main menu
   - Press **1** to play messages.
   - Press **2** to make a message.
   - Press **4** to reach the User Options menu.
   - Press **9** to log out and exit.
3. While playing a message, you can
   - Press **1** to rewind the current message.
   - Press **2** to toggle between pausing and restarting the current message.
   - Press **3** to skip forward in the current message.
   - Press **5** to hear the date and time for the current message.
   - Press **9** to return to the Main menu.
   - Press **0**, then **0** to reach the attendant.
   - Press **1**, then **1** to go back to the start of the current message.
   - Press **3**, then **3** to skip to the end of the current message.
   - Press 0 for help.

4. After playing a message, you can

- Press **1** to play the next message.
- Press **4** to replay the current message.
- Press **5** to hear the date and time for the current message.
- Press **6** to forward the current message to another user.
- Press **7** to delete the current message.
- Press **7**, then **9** to delete the current message and exit to the Main menu.
- Press **8** to reply to the current message.
- Press **9** to save the current message.
- Press **9**, then **9** to save the current message and exit to the Main menu.
- Press **0**, then **0** to reach the attendant.
- Press **0** for help.

26.84 Cut-Through Paging - Description

Cut-through Paging (CTP) is an enhancement to the paging feature. CTP allows the caller/user to input a telephone number for the page recipient to call. The telephone number can be between 1 and 25 digits and is sent to the recipient's pager as part of the paging notification.

In addition, the CTP feature allows the page recipient the option of requesting a page notification receipt. If requested, a notification receipt is deposited in the recipient's mailbox after each cut-through page. A page notification receipt allows the recipient to keep a record, through NuPoint Voice messages, of all messages received.

Cut-through Paging is supported for the English language, only.

The CTP feature is configurable by Feature Class of Service (FCOS) bits. A page recipient's mailbox can be configured four different ways:

- **Method 1**: The mailbox can receive a telephone number OR a recorded message, but not both. Mailbox will not receive page notification receipts.
- **Method 2:** The mailbox can receive a telephone number, a recorded message, or both a telephone number and a recorded message. The mailbox will not receive page notification receipts.
- **Method 3:** The mailbox can receive a telephone number or a recorded message but not both. The mailbox will receive page notification receipts.
- **Method 4:** The mailbox can receive a telephone number, a recorded message or both. The mailbox will receive page notification receipts.

Method	Telephone Number	Recorded Message	Both	Page Notification Receipts
1	Y	Y	N	N

Method	Telephone Number	Recorded Message	Both	Page Notification Receipts
2	Y	Y	Y	N
3	Y	Y	N	Y
4	Y	Y	Y	Y

CTP is supported for single-addressee messages only. Users creating multiple-addressee messages will not be able to access CTP.

Like all pages, the cut-through page is only sent when the current time is within the mailbox's configured page "start" time and "stop" time window. In addition, the CTP recipient is paged once only.

Page notification receipts are not supported for broadcast mailboxes.

26.84.1 Cut-Through Paging - Configuration

CTP is controlled at the mailbox level through FCOS bits. There are no other configuration changes to the system - the NuPoint Voice system and Pager line groups are both configured normally.

CTP-specific FCOS Bits

The CTP FCOS bits are as follows:

- **171 Cut-through Paging**: When added to a mailbox's FCOS, it activates CTP for the mailbox. The caller/user can leave a telephone number or a message but not both telephone number and a message at the same time.
- 172 Cut-through Paging and Messaging: When added to a mailbox's FCOS, it activates CTP for the mailbox. The caller/user can leave a telephone number, a message, OR both a telephone number and a message.
- 173 Receive Cut-through page Notify Receipt: When added to a mailbox's FCOS, the mailbox will receive a notification receipt for each CTP page. Otherwise, the mailbox will not receive a notification receipt for each CTP page.

Other FCOS Bits

Other FCOS bits also affect the functionality of the CTP feature:

- **70 User Options Menu** and **77 Change Pager Schedule**: CTP paging is an extension of regular paging, therefore, paging must also be configured.
- 10 Enhanced Outcall Paging Options: English prompts. CTP is only supported in English, therefore, the English prompts FCOS bit should be set.
- 4 Outside Caller Functions: If On, the caller must enter the feature activation key ("I" the 4 key) to activate CTP. If Off, the caller can enter the telephone number directly, without using the feature activation key.

- 5 Play Outside Caller Menu Prompts: If the outside caller menu is off, the outside caller will not receive outside caller function prompts. Note FCOS bit 5 requires that FCOS bit 4 be set.
- 75 Audit Receipt Message: If not configured (not enabled), the page recipient configured for page receipt notification will not be able to play the message associated with the page receipt. A mailbox configured with page receipt notification should be configured with FCOS bit 75 set on.

Configuring a CTP Mailbox

To configure a CTP Mailbox:

1. Define an FCOS for CTP (see Related Topics):
2. Copy/add all FCOS bits from your regular pager mailbox's FCOS to the CTP FCOS.
3. If not already included, add FCOS bit **10** (Enhanced Outcall Paging Options: English prompts) to the CTP FCOS. This is because the feature is only supported in English. It is a good idea to delete all other language prompts from the CTP FCOS.
4. Add the required CTP features using the feature bits from the list below:

   - **171:** A mailbox which can receive a telephone umber or a recorded message but not both; no page notification receipt.
   - **172:** A mailbox which can receive a telephone number and/or a recorded message; no page notification.
   - 1**71 & 173:** A mailbox which can receive a telephone number or a recorded message but not both; with page notification receipt.
   - **172 & 173:** A mailbox which can receive a telephone number and/or a recorded message; with page notification receipt.
5. Define a Mailbox.
6. Assign the CTP FCOS you defined in step 1 to the mailbox.
7. Set the message waiting type to "5". This is required for all pager mailboxes (CTP or regular).
8. Set all other pager parameters as usual.

26.84.2 Cut-Through Paging - Operation

There are five parts to the user interface for CTP:

- Mailbox Owner Greeting Setup
- Feature Activation Key
- Outside Caller Interface
- System User Interface
- CTP Recipient (Mailbox Owner) interface

CTP Mailbox Owner Greeting Setup

The NuPoint Voice greeting does not prompt the caller to access CTP so the CTP mailbox owner's greeting should inform the caller that CTP is available.

Feature Activation Key

The feature activation key defined for CTP is "I" (the 4 key) on the telephone set. This key is used by the caller/system user to access CTP.

Outside Caller Interface

This section describes outside caller CTP access scenarios. Depending on mailbox configuration, the outside caller can access CTP at two different points within the NuPoint Voice session: immediately after the mailbox owner greeting OR after recording a message. As previously mentioned, it is the responsibility of the mailbox owner to inform the caller about CTP in his/her greeting.

Scenario 1: Leave a telephone number (activate CTP), for a CTP Mailbox that has Outside Caller Functions On and Outside Caller Menu On.

1. Dial the desired party. If the called party is unavailable, you are forwarded to the NuPoint Voice system.
2. After the mailbox owner greeting, press "I" (the 4 key). NuPoint Voice prompts you to leave a telephone number.
3. Enter your telephone number (1-25 digits) followed by a "#". If you do nothing, NuPoint Voice times out and prompts you again for the telephone number. After the second time out NuPoint Voice hangs up.
4. After the telephone number is entered, NuPoint Voice repeats the telephone number entered. NuPoint Voice prompts you with options as before; including the new option to delete and re-enter your telephone number.
5. If you do not wish to delete and re-enter your telephone number, skip to step 8.
6. To re-enter your telephone number, press "I" (the 4 key). NuPoint Voice prompts you to leave a telephone number.
7. Enter your telephone number (1-25 digits) followed by a "#". After the telephone number is entered, NuPoint Voice plays it back.
8. At the prompt, enter "X" (the 9 key). NuPoint Voice confirms sending your telephone number with, "Your page sent."
9. Hang up.

Scenario 2: Leave a telephone number (activate CTP), for a CTP Mailbox which has Outside Caller Functions Off:

1. Dial the desired party. If the called party is unavailable, you are forwarded to the NuPoint Voice system.
2. After the mailbox owner greeting, enter your telephone number (1-25 digits) followed by a "#". The feature activation key ("I")

   is not required when the outside caller functions are turned off. If you do nothing, NuPoint Voice assumes you are recording a message.
3. If a telephone number is entered, NuPoint Voice repeats the telephone number entered. NuPoint Voice confirms the sending of your telephone number with "Your page sent."
4. If the line group is configured for multiple messages, NuPoint Voice will prompt the caller to send another message or forward to the attendant. Otherwise, NuPoint Voice hangs up.
5. Hang up.

Scenario 3: Leave a telephone number after recording a message (Note: this option is only available if he CTP mailbox is configured with FCOS bit 172 and Outside Caller Functions On and Outside Caller Menu On)

1. Dial the desired party. If the called party is unavailable, you are forwarded to the NuPoint Voice system.

2. After the mailbox owner greeting, record a message. NuPoint Voice prompts you with options as before; including the option to enter your telephone number.
3. Press "I" (the 4 key). NuPoint Voice prompts you to leave a telephone number.
4. Enter your telephone number (1-25 digits) followed by a "#". If you do nothing, NuPoint Voice times out and prompts you again for the telephone number. After the second time out NuPoint Voice hangs up.
5. After the telephone number is entered, NuPoint Voice repeats the telephone number entered. NuPoint Voice prompts you with options as before; including the new option to delete and re-enter your telephone number.
6. If you do not wish to delete and re-enter your telephone number, skip to step 9.
7. To re-enter your telephone number, press "I" (the 4 key). NuPoint Voice prompts you to leave a telephone number.
8. Enter your telephone number (1-25 digits) followed by a "#". After the telephone number is entered, NuPoint Voice plays it back.
9. At the prompt, enter "X" (the 9 key). NuPoint Voice confirms sending your telephone number with, "Your page sent."
10. Hang up.

Scenario 4: Leave a telephone number after recording a message (Note: this option is only available if the CTP mailbox is configured with FCOS bit 172 and Outside Caller Functions Off):

1. Dial the desired party. If the called party is unavailable, you are forwarded to the NuPoint Voice system.
2. After the mailbox owner greeting, record a message.
3. Enter your telephone number (1-25 digits) followed by a "#" before the end of recording timeout. If you do nothing, NuPoint Voice times out the recording. After the telephone number is entered, NuPoint Voice plays back the number.
4. NuPoint Voice confirms sending your telephone number and message with "Your message and page sent".
5. If the line group is configured for multiple messages, NuPoint Voice will prompt the caller to send another message or forward to the attendant. Otherwise, NuPoint Voice hangs up.
6. Hang up.

Scenario 5: Leave a telephone number before recording a message. (Note: this option is only available if the CTP mailbox is configured with FCOS bit 172 and Outside Caller Functions On and Outside Caller Menu On.)

1. Dial the desired party. If the called party is unavailable, you are forwarded to the NuPoint Voice system.
2. After the mailbox owner greeting, enter "I" (the 4 key). NuPoint Voice prompts you to leave a telephone number.
3. Enter your telephone number (1-25 digits) followed by a "#". If you do nothing NuPoint Voice times out and prompts you again for the telephone number. After the second time out NuPoint Voice hangs up. After the telephone number is entered, NuPoint Voice plays it back.
4. At the prompt, press "D" (the 3 key). You are prompted to leave a message.
5. Record a message. NuPoint Voice confirms the completion of your recording.
6. At the prompt, enter "X" (the 9 key) to exit.
7. NuPoint Voice confirms the sending of your telephone number and message with “Your message and page sent.”

8. Hang up.

Scenario 6: Leave a message only, dial the party as always and record your message after the NuPoint Voice recording beep.

System User Interface

The CTP feature is only available for single-addressee messages. It is not available for multiple-addressee messages.

Scenario 1: Leave a telephone number (activate CTP):

1. Dial NuPoint Voice and enter as a system user.
2. Select to make a new message as usual, however, address the message to one addressee only.
3. After the recording beep, enter "I" (the 4 key). NuPoint Voice prompts you to leave your telephone number.
4. Enter your telephone number (1-25 digits) followed by a "#". If you do nothing NuPoint Voice times out and prompts you again for the telephone number. After the second time out NuPoint Voice returns to the "Make" menu.
5. After the telephone number is entered, NuPoint Voice repeats the telephone number entered. NuPoint Voice prompts you with options as before; including the new option to delete and re-enter your telephone number.
6. If you do not wish to delete and re-enter your telephone number, skip to step 9.
7. To re-enter your telephone number, press "I" (the 4 key). NuPoint Voice prompts you to leave a telephone number.
8. Enter your telephone number (1-25 digits) followed by a "#". After the telephone number is entered, NuPoint Voice plays it back.
9. At the prompt, press "X" (the 9 key). NuPoint Voice confirms sending your telephone number with "Your page sent."
10. Hang up.

Scenario 2: Leave a telephone number after recording a message (Note: this option is only available the CTP mailbox is configured with FCOS bit 172):

1. Dial NuPoint Voice and enter as a system user.
2. Select to make a new message as usual, however, address the message to one addressee only.
3. Record your message. NuPoint Voice prompts you to leave your telephone number.
4. Press "I" (the 4 key). NuPoint Voice prompts you to leave your telephone number.
5. Enter your telephone number (1-25 digits) followed by a "#". If you do nothing NuPoint Voice times out and prompts you again for the telephone number. After the second time out NuPoint Voice returns to the "Make" menu.
6. After the telephone number is entered, Nupoint Voice plays it back.
7. At the prompt, press "X" (the 9 key). NuPoint Voice confirms sending your telephone number and message with "Your message and page sent.
8. Hang up.

Scenario 3: Leave a message only, enter NuPoint Voice as a system user and address and record you message as always.

CTP Recipient Interface

The User Interface for the CTP recipient is divided into two areas: Pager Interface and Mailbox Interface. The Pager Interface describes what CTP recipients receive through their pagers. The Mailbox Interface describes what CTP recipients receive in their mailboxes.

CTP Recipient Pager Interface

The cut-through page is only sent when the current time is within the mailbox's configured page “start" time and "stop" time window. The cut-through page will be sent only once (pager frequency = 1). If the cut-through page is unsuccessful, then the page will follow the regular page recovery process as defined for the recipient's mailbox.

The telephone number entered by the caller/user will be sent as a post-pager string prefix with a "greet" command. The "greet” command signals NuPoint Voice not to send the telephone number until the pager has answered. The telephone number will override the recipient's default post-pager string (predefined m the mailbox configuration). If the recipient's pager is analog, the pager unit beeps and then plays the DTMF tones for the telephone number to call. If the recipient's pager is digital, the digital readout displays the telephone number to call. If the recipient's pager is voice, the pager says "Please call NNX-XXXX.," where NNX-XXXX is the telephone number entered by the caller/user.

If the page recipient's mailbox is configured for notification receipt, the recipient will receive one page if the caller/user leaves both a telephone number and a message, however, if the page recipient's mailbox is configured for no notification receipt, the recipient will be paged twice if the caller/user leaves both a telephone number and a message—once for the telephone number and once for the message.

CTP Recipient Mailbox Interface

The messages received in the CTP recipient's mailbox depend on the caller/user action and the mailbox configuration.

Case 1 - Caller/user leaves only a telephone number:

- If the mailbox is configured for no page notification receipt, the mailbox will have no page notification receipt and no message.
- If the mailbox is configured for page notification receipt, the mailbox will have one page notification receipt.

Case 2 - Caller/user leaves only a recorded message:

- If the mailbox is configured for no page notification receipt, the mailbox will have one message.
- If the mailbox is configured for page notification receipt, the mailbox will have one message.

Case 3 caller/user leaves a telephone number and a recorded message:

- If the mailbox is configured for no page notification receipt, the mailbox will have no page notification receipt and one message.
- If the mailbox is configured for page notification receipt, the mailbox will have one page notification receipt and no message.

NuPoint Voice Interface

CTP results in two NuPoint Voice interface changes for the CTP mailbox owner.

1. When the CTP mailbox owner accesses NuPoint Voice, the greeting now lists the number of page receipts, number of unplayed messages, and the total number of messages. If there are no page receipts, the greeting will list the number of unplayed messages and the total number of message, as before.
2. When the CTP mailbox owner listens to the page notification receipt, NuPoint Voice says:

   "Receipt for page received <time stamp>. You were paged by NNX-XXXX. <recorded message>."

   <time stamp>: gives the time the receipt was received.

   <recorded message>: plays the recorded message. If nothing was recorded, <recorded message> will be empty.

26.85 Overview - Language Prompts

Description

Your NuPoint UM base license provided up to three "full sets" of system prompts in different languages, along with "overlay" prompts that can customize the basic prompts. The default language for NuPoint UM is North American English and this full set is automatically installed when you install NuPoint UM. Your base license then allows you to install up to two other languages. If more languages are required, you may license and install a maximum of 25 language prompt sets.

Prompt Languages

Prompts are available in multiple languages as well as a "Numeric Full Set", which supplies the full prompt set with numerical values, and counts as a separate language license.

If your system needs to use a language other than NA English, and you have a spare language license, you can install the full set language prompt software blade. To uninstall a language used in a line group or LCOS language, you must manually update the language selected in the line group or LCOS. (For detailed instructions on how to manage software, refer to the *NuPoint Unified Messaging Technician's Handbook*.)

Overlay Prompts

NuPoint UM also provides prompt overlays, which are customized prompt sets that replace certain prompts in the base language. For example, there are many customized hotel overlays, each of which replaces the standard NuPoint UM prompt with a custom prompt for that particular hotel. (For example, "Welcome to the Message Center" may be replaced by "Welcome to the Holiday Inn Select Hotel".) Overlay prompts do not require licensing.

Numeric overlays replace all alphabetic prompts with numeric ones. (For example, "Press P to play the message." becomes "Press 7 to play the message." when a numeric overlay is applied.

Configuration

After the prompts have been installed on the system, they can be activated on the system in one of these ways:

- **Apply to Entire Line Group**:
  - Specify the default prompt languages for the entire line group. You can specify a single language for a uniligual system or five languages for a multilingual system. When users call a multilingual system and reach the Message Center auto attendant or NuPoint Receptionist application, they are asked to select their preferred language for NuPoint prompts. For example, if you call an English-French multilingual system, you will be asked to select either English or French. You will then receive prompts only in that language.
- **Apply to Individual Mailboxes**:
  - You can define a prompt language in an LCOS and then assign that LCOS to individual mailboxes; use this option if some users require a different language or prompt set. For example, you can install the optional Numeric Full Set prompt language along with the default mnemonic prompts ("Press P to play"). Control which users receive the "Press 7 to play" prompts by assigning the LCOS that contains the numeric prompt set to their mailboxes.

Operation

Mailbox settings always override the Line Group setting. For example, if mailbox 2002 (French) calls in to Line Group 1 (English), Line Group 1 responds with a French prompt.

Mailboxes that have an LCOS setting of "default" always receive prompts in the language assigned to the Line Group.

Callers who do not have a mailbox on the system are handled differently depending on the Line Group configuration:

- **Uniligual Service** - If the line group has one prompt language, callers are greeted initially in that language. The language of subsequent prompts is determined by the mailbox number they select.
- **Multilingual Service** - If the line group has two or more prompt languages, callers are asked to select their preference. The language of subsequent prompts is determined by the language they select. If a mailbox number with a custom LCOS language setting is then selected, the prompt language is determined by the mailbox itself (not by the Line Group); this occurs because mailbox settings override the Line Group setting.

Note:
To override the LCOS mailbox settings (and have a multilingual system play prompts in the selected language rather than the mailbox language), assign an FCOS with feature bit 51, Do Not Switch Languages for Outside Caller, to the mailbox.

Prompts Example:

ABC Company has two line groups that respond to incoming calls.

- Line **Group 1** provides uniligual service in French and has an LCOS with NA English assigned.
- Line **Group 2** provides multilingual service in English and French and has an LCOS with French assigned.

The company has the following internal mailboxes:

Mailbox #	LCOS Language assigned:
2000	Default
2001	NA English
2002	Canadian French

When this Mailbox...	...calls this Line Group...	... prompts are in this lang uage:
2001 (English)	1 (English)	English
2001 (English)	2 (English and French)	English
2002 (French)	1 (English)	French
Caller who has no mailbox on the system	1 and then selects mailbox 2001 (English)	Initial welcome message is in French , and asks the caller to select a ma ilbox. After the caller selects 2001, prompts change to English to match the mailbox.
Caller who has no mailbox on the system	2 and then selects French as the pro mpt language	Initial welcome message is in Englis h and French, and asks the caller to select a language preference. After the caller selects French, prompts change to French.

Text to Speech Prompts

The Text to Speech prompts language provides the conversion of email text to spoken language in the Advanced UM feature and also provides prompts in the Speech Auto Attendant feature. These prompts are mandatory for both features.

26.85.1 Activate Language Prompts

You can modify a line group or LCOS so that users receive prompts in an alternate language. In addition, you can specify up to five languages for a line group in order to create a "Multilingual Service" that asks users to select their preference (for example, English, German and French) when they initially reach the Message Center or Receptionist application.

Note:

- Before you can specify alternate language(s) for a line group or an LCOS, you must install the alternate-language prompt software.
- To program language prompts for a Centrex or UI tenant group, you must use the Text Console. See Activate Language Prompts for Tenant Groups.

LCOS Language Configuration with One Language

To program an LCOS with a single alternate language:

1. In the navigation tree, select **Class of Service > Limits COS**.
2. Select the LCOS you want to modify and then click **Edit**.
3. In the Limits list box, select **Language**.
4. In the **Language** list, select the language to assign to this LCOS.
5. Click **Save**.
6. Assign the custom LCOS to the selected mailboxes.

Line Group Language Configuration with One Language

To program a line group with a single alternate language for unilingual service:

1. In the navigation tree, select **Active Configuration > Line Groups**.
2. Select the checkbox beside the line group whose languages you want to configure.
3. Click **Edit**.
4. Under **Prompt Language**, select the desired language from the **Language 1** drop-down box.

   Leave all other Prompt Language fields disabled.
5. Click **Save**.

Line Group Language Configuration with Up To Five Languages (Multilingual Service)

To program a line group with five alternate languages for multilingual service:

1. In the navigation tree, select **Active Configuration > Line Groups**.
2. Select the checkbox beside the line group whose languages you want to configure.
3. Click **Edit**.
4. Select the desired primary language from the **Language 1** drop-down box.
5. Select up to four other languages from the **Language 2-5** drop-down boxes.

6. For the **Language Selection Prompt**, do one the following:

   - Select **Automatic** to have the language selection prompt generated automatically based on the languages specified. To suppress the prompt for the primary language (and keep the message brief), select **Say 2nd language prompt only** .

     —OR—
   - Select **Custom** to use a customized language selection prompt.
   - Record the prompt in the specified languages (for example, "For service in English, press 1. Pour le service in français, appuyez sur 2.") in 8 KHz, 8-bit, mono u-law format and save the file to an accessible location.
   - Click **Import**, browse to the location of the file, select it and click **OK**.
7. Enter the **Language Selection Timeout**, in seconds (default is 3 seconds). If a caller fails to select a language within the timeout period, the system will automatically use the primary language.
8. Click **Save**.
9. Record a multilingual corporate greeting for the NuPoint system hunt group pilot number though the NuPoint administrator mailbox. Record the greeting in the primary language followed by the same greeting in the other languages; for example: "Welcome to Mitel Networks; Bienvenue à Mitel Networks; Bienvenido a Mitel Networks."
10. Call into the NuPoint system hunt group pilot number and ensure that the prompts are played correctly.
11. Instruct mailbox users to record multilingual greetings for their mailboxes. Again, users should record their mailbox greetings in the primary language followed by the same greeting in the other languages; for example: “You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message; Usted ha llegado al buzón de voz de Jean Julian , por favor deje un mensaje."

When an external caller connects with the voice mail hunt group pilot number, the system plays your multilingual corporate greeting and then prompts the caller to select the desired language. For example: "Welcome to Mitel Networks; Bienvenue à Mitel Networks. For Service in English, press 1; Pour le service en français, appuyez sur 2; Para el servicio en español, presione 3."

When a caller reaches a user's mailbox, the system plays the multilingual mailbox greeting: "You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message; Usted ha llegado al buzón de voz de Jean Julian, por favor deje un mensaje."

The following conditions apply to the Multilingual Service:

- The multilingual service does not apply to Speech Auto Attendant (SAA).
- The multilingual service applies to calls to the NuPoint voice mail hunt group pilot number.
- Callers select multilingual prompts at the system-level only, not at the mailbox level.
- If a mailbox has a custom LCOS language setting, this overrides the Line Group language setting.
- The caller only selects the prompt language once, before the first system prompt is played.
- Mailbox owners are not prompted to select a prompt language when they log into their mailboxes.
- The system plays the prompt languages in the order they have been programmed. For example, if you select the English as the primary language, French as the secondary language, and Spanish as the tertiary language, the system-generated automatic prompt plays: "For service in English, press 1; Pour le service en français, appuyez sur 2; Para el servicio en español, presione 3."
- If the caller selects a language, terminates the call and then calls back again within sixty seconds, the system will remember the caller's preference and play prompts in the previously selected language.

If the caller waits longer than sixty seconds before calling back, the system will the play the regular language selection prompt.

26.85.2 Activate Language Prompts for Tenant Groups

Use the text console to program language prompts for tenant groups associated with Centrex and Unified Integration applications. Use the web console for *all* other implementations.

Tenant Group Language Configuration with One Language

To program a Centrex or UI tenant group with a single alternate language for uniligual service:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(H) Configure Unified Integration**,
2. Select **(G) Tenant Group Number =** and enter a **number** (1-24) for the tenant group you want to program.
3. Select **(L) Default prompt language =** to display the tenant prompts languages menu.
4. Select **(P)** to display the primary prompt language selection menu.
5. Select a language option from the list.
6. Select **(X)** to exit and save your changes.

Tenant Group Language Configuration with Five Languages (Multilingual Service)

Note:
If you create call flow for a tenant group with multilingual service, you must set the Prompt Language to "Auto" and not include the "Language Router" action.

To program a Centrex or UI tenant group with a single alternate language for multilingual service:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(H) Configure Unified Integration**,
2. Select **(G) Tenant Group Number =** and enter a **number** (1-24) for the tenant group you want to program.
3. Select **(L) Default prompt language =** to display the tenant prompts languages menu.
4. Select **(P)** to display the primary prompt language selection menu, and then select a language option from the list.
5. Select **(S)** to display the secondary prompt language selection menu, and then select a language option from the list.
6. Select **(X)** to exit and save your changes.
7. Record a multilingual corporate greeting for the NuPoint system hunt group pilot number though the NuPoint administrator mailbox. Record the greeting in the primary language followed by the same greeting in the other languages; for example: "Welcome to Mitel Networks; Bienvenue à Mitel Networks".

8. Call into the NuPoint system hunt group pilot number and ensure that the prompts are played correctly.
9. Instruct mailbox users to record multilingual greetings for their mailboxes. Again, users should record their mailbox greetings in the primary language followed by the same greeting in the other languages; for example: “You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message."

When an external caller connects with the voice mail hunt group pilot number, the system plays your multilingual corporate greeting and then prompts the caller to select the desired language. For example: "Welcome to Mitel Networks; Bienvenue à Mitel Networks. For Service in English press 1; Pour le service en français, appuyez sur 2."

When a caller reaches a user's mailbox, the system plays the multilingual mailbox greeting: "You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message."

The following conditions apply to the Multilingual Service:

- The multilingual service does not apply to Speech Auto Attendant (SAA).
- The multilingual service applies to calls to the NuPoint voice mail hunt group pilot number.
- Callers select multilingual prompts at the system-level only, not at the mailbox level.
- If a mailbox has a custom LCOS language setting, this overrides the tenant group language setting.
- The caller only selects the prompt language once, before the first system prompt is played.
- Mailbox owners are not prompted to select a prompt language when they log into their mailboxes.
- The system plays the prompt languages in the order they have been programmed. For example, if you select the English as the primary language and French as the secondary language, the system-generated automatic prompt plays: "For service in English, press 1; Pour le service en français, appuyez sur 2."
- If the caller selects a language, terminates the call and then calls back again within sixty seconds, the system will remember the caller's preference and play prompts in the previously selected language. If the caller waits longer than sixty seconds before calling back, the system will play the regular multilingual greeting.

26.86 Overview

NuPoint Fax is an optional, software-only feature (no fax card required on the server) that allows NuPoint Voice users and outside callers to exchange faxes through user mailboxes and special mailboxes. NuPoint Fax provides a set of fax-related features and limits that you can assign to NuPoint Voice mailboxes.

With NuPoint Fax, fax documents are stored as electronic fax messages in NuPoint Voice mailboxes. From there, faxes can be delivered to any fax machine at any time, distributed to other mailboxes, sent over a network, or viewed on a PC (in the Messages tab of the Web View Interface).

The Fax feature works in a network configuration where the NuPoint Unified Messaging server is integrated directly with a Mitel MiVoice Business or with another PBX through a Dialogic Media Gateway (formerly PIMG). For more information, see Fax Scenarios.

Note:
Using Fax with the Web View Interface requires a Web session (you must have an Internet connection).

NuPoint Fax provides a solution to many of the problems inherent in typical fax communication:

- Callers sending a fax do not have to wait due to the receiving fax machine being busy with another transmission.
- Faxes are stored in password-protected user mailboxes. Faxes do not sit at the fax machine for anyone to read.
- Recipients receive notification when a new fax arrives. Incoming faxes do not sit for days because recipients do not know they are there.
- Faxes can be annotated with voice messages (also called voice cover sheets), relieving the sender of typing out explanatory notes.
- The recipient decides when and where a fax is printed out. For example, a NuPoint Fax user away from the office can call their NuPoint Voice mailbox and direct a fax, deposited there by someone else, to be delivered to a hotel, an airport, or another location where there is a convenient fax machine. After reading the fax, the user can call back into their mailbox and send the fax to another party, for example, a prospective client waiting for a quote.

For end-user features and operating information, see the NuPoint Unified Messaging *Web View Help* and *Messaging User Guide.*

26.86.1 About NuPoint UM Fax Applications

NuPoint UM Fax applications include Fax Mail, Outbound Fax, Fax Broadcast, Guaranteed Fax, Fax Publishing, and Walkaway Fax. You can use one or more of these applications, in any combination. For more information about planning and configuring these applications, see Fax Planning.

Fax Mail

Fax Mail is the most general and widely used application of NuPoint Fax. With Fax Mail, incoming faxes are stored electronically as "fax messages" in a user's mailbox—the same mailbox that stores voice messages. Users are then notified of their new fax messages in the same manner as with voice messages (for example, message waiting light, pager, stutter dial tone).

By calling into their mailboxes, users can retrieve their fax messages at any time by sending them to any fax machine. In addition, users can call into their mailboxes from fax phones and retrieve their fax messages "online" at that fax machine. Users of Fax Mail have the same options that are available to them through voice mail: fax messages can be played, answered, or given to another mailbox, distribution list, or off-system telephone (fax) number. For instructions on how users can manage their fax messages from the Web View Interface and TUI, refer to the *NuPoint Unified Messaging Web View Help* and the *Messaging User Guide*.

Outbound Fax

Sending fax messages (outbound messages) requires that the fax group be assigned to an outdial line group, such as a Pager group. Users can send fax messages using any of the following components of NuPoint UM:

- **the Telephone User Interface (TUI):** Use the TUI to send a fax message, or a combined voice and fax message. For instructions, see the *NuPoint Unified Messaging User Guide.*
- **the Web Vew:** Use the Compose Fax button on the Messages tab of the Web View interface. For detailed instructions, see the *Web View help.*
- **the Fax Print Driver application:** Download and install this desktop tool (from DVD or Web View) to send a fax using any software that has a print function. For instructions, see the *NuPoint Unified Messaging User Guide.*

The Fax Printer Driver application runs on Windows 10 (64-bit), Windows 8 Professional (64-bit) and the following 32-bit and 64-bit variants of Windows 7:

- **Windows 7 Pro:** Regular and N
- **Windows 7 Enterprise:** Regular and N
- **Windows 7 Ultimate:** Regular and N

The features in the N Edition software are the same as their equivalent full versions, but do not include Windows Media Player. You can download Windows Media Player without charge for the N Editions.

Note:
The Fax Printer driver does not support files in TIFF format on Windows 7.0, Windows 8.0 and Windows 10. It does, however, support other common file formats (DOC, PDF, XLS, etc).

Destinations can include any other users' mailboxes or fax numbers. Users can receive confirmation by voice mail and email concerning whether their fax transmissions have succeeded or failed.

Fax Broadcast

Fax Broadcast allows a user to make and send a fax message simultaneously to multiple destinations using a distribution list. The destinations can include any other users' mailboxes, users on another NP Voice system connected with the NuPoint Net digital network, or outside telephone numbers. For example, a product manager could disseminate price changes to the sales force with a copy of the new price list and an attached voice message explaining the changes. Fax Broadcast messages can be scheduled for future delivery (when rates are lower), and the NuPoint Unified Messaging server can automatically retry calls to numbers that are busy or do not answer.

Guaranteed Fax

With NuPoint Fax, delivery of incoming faxes can be guaranteed even when the company or department fax machine is busy, runs out of paper, or is otherwise disabled. One or more Guaranteed Fax mailboxes are assigned to a hunt group with the fax machine. When the machine is busy, the incoming faxes are routed to and stored in the mailboxes; the caller never realizes that the fax did not go directly to a fax machine. The mailboxes then automatically and continually try to deliver the stored faxes to the same or another fax machine.

Fax Publishing

You can configure a NuPoint Fax mailbox to deliver a voice message and a fax to a caller who accesses the mailbox. This provides a convenient way to publish frequently requested information to employee users, customers, or any outside callers.

The caller can reach the mailbox containing the appropriate information directly or be led by voice prompts through a mailbox tree or chain structure. The mailbox containing the fax can do either of the following:

- Play a voice cover sheet or a menu or both, giving the caller the choice to either receive the fax online or enter a telephone number for delivery of the fax.
- Immediately begin transmitting the fax.

Walkaway Fax

Walkaway Fax appears to the sender exactly like a regular fax machine. With this feature, callers dial a telephone number (from a fax machine or a PC running fax software) and immediately send a fax, without a voice cover sheet, directly into a user's mailbox. Callers do not have to respond to prompts or monitor the call. The walkaway Fax Mailbox listens for fax tone while playing a greeting, and if detected, receives the incoming fax. If none is detected, normal message recording ensues.

26.86.2 Fax Scenarios

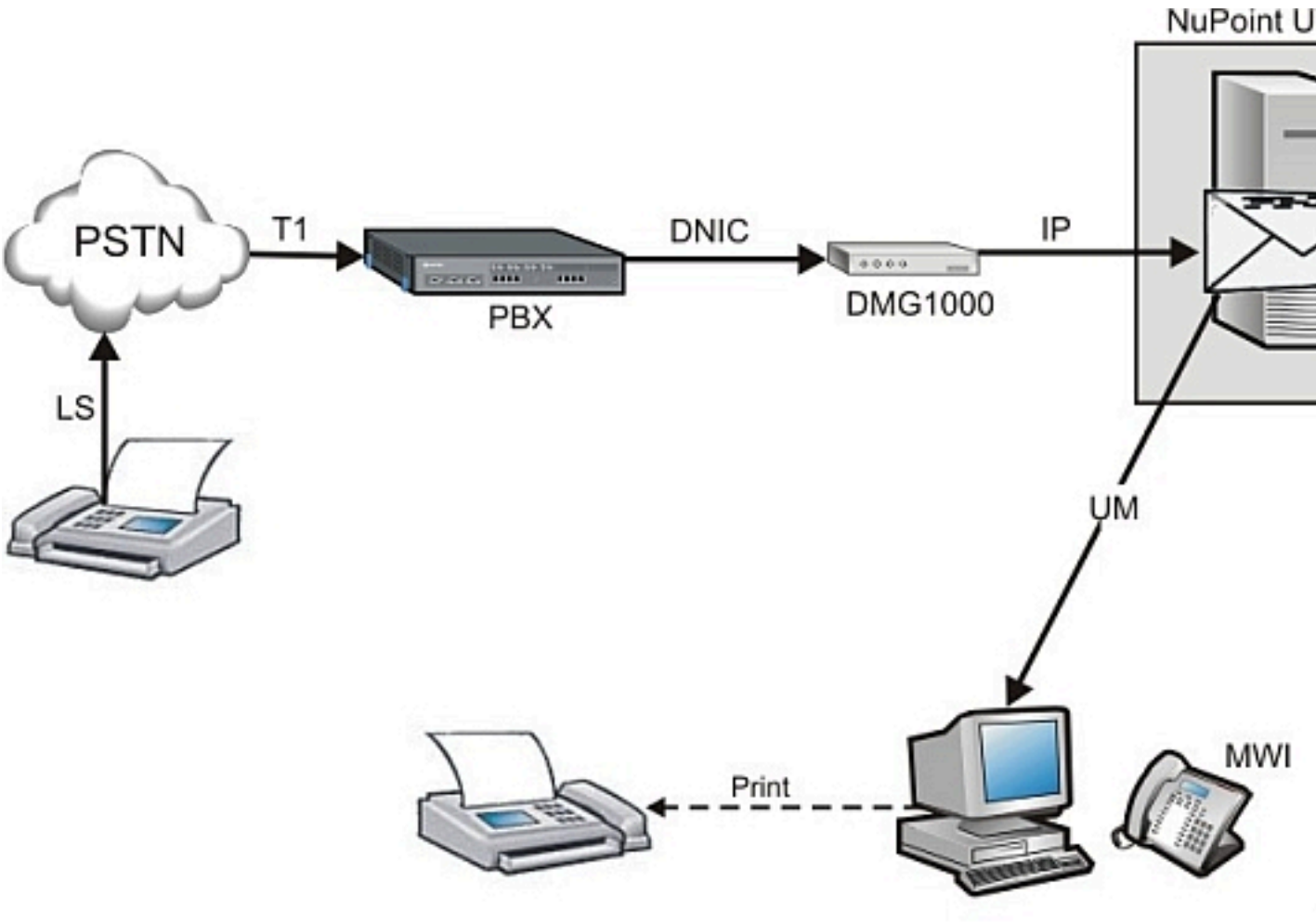
This section illustrates incoming and outgoing fax scenarios. The configuration procedures discussed in these scenarios can be found in the Installation and Configuration section.

Incoming Fax

Several incoming fax scenarios are possible with the NuPoint Unified Messaging Fax feature, where a user receives a fax, views it, and prints it. This section overviews some scenarios of fax reception and how they must be configured.

Note:
For information on user operation of the Fax feature with the Web View interface, refer to the NuPoint Unified Messaging *Web View Help*; and for information on user operation of the Fax feature with the TUI, refer to the NuPoint Unified Messaging *User Guide*.

The Incoming Fax Reception diagram shows the fax document travelling from the TDM to the IP domain via a T1 trunk before reaching the NuPoint Unified Messaging server. NuPoint Unified Messaging Fax is pass-through implementation of FAX over IP (FoIP). The illustration below shows the PBX being integrated with a NuPoint Unified Messaging server, using a PIMG box, but direct integration with a Mitel MiVoice Business ICP is also supported.



Incoming Fax Reception

A typical incoming fax scenario consists of the following flow of events:

1. The far-end sends a fax by dialing the fax number of the NuPoint Unified Messaging recipient. This is typically a Direct Inward Dial (DID) number that the recipient has for their incoming faxes.
2. The call arrives at the PBX via a T1 trunk. The PBX has been programmed to route this DID number to a (phantom) set that is always forwarded to the voice mail hunt group.
3. The call is routed to the PIMG via DNIC integration.
4. The call then lands on a voice mail port on the NuPoint Unified Messaging server. This port has Fax resources allocated to it.
5. The Fax is then decoded and stored in the recipient's mailbox as a new message.
6. The NuPoint Unified Messaging server then lights the Message Waiting Indicator (MWI) of the recipient's phone.
7. The recipient dials into their voice mail and sees that there is a fax message; or the user checks the Messages tab in their Web View (must be a licensed UM Standard Web View user) and sees that there is a new fax message; or the user checks their e-mail inbox (UM Standard SMTP option) and see that there is a new fax message.
8. The recipient then uses the Web View (UM Standard Web View) and a TIFF or PDF viewer to view the fax.

9. The recipient uses the printing functionality in the TIFF Viewer to send the fax to a printer to keep a hard copy of the fax.

Scenario 1 - Setting up Incoming Fax Reception for Departmental Fax Numbers (Public Fax)

ACME Manufacturing needs three main fax numbers that it wants to publish. One is for sales, one for support and one for the production floor. These are 727-SALE (7253), 727-HELP (4357) and 727-ENGI (3644) respectively. Incoming faxes to one of these numbers will be distributed to interested personnel in that department. To configure this scenario with NuPoint UM Fax, the tasks are as follows:

1. Obtain the DID numbers from the local PSTN.
2. Program (phantom) sets on the PBX that hosts the NuPoint Unified Messaging server, with DNs 7253, 4357 and 3644.
3. Configure these sets to always forward to the NuPoint Unified Messaging voice mail hunt group.
4. Program DID routing to forward calls to particular (phantom) sets. Typically, this is done by simply absorbing the NXX part of the DNIS and routing the call to the extension matching the remaining digits.
5. Create three mailboxes on the NuPoint Unified Messaging server, with numbers 7253, 4357 and 3644.
6. Give them an FCOS with bits: 122 (broadcast), 190 (receive fax), 198 (receive fax only), 203 (walkaway fax).
7. Create one distribution list for each mailbox.
8. Add mailboxes of interested parties to the particular lists. Give these interested parties either UM basic or UM+MWI.
9. Define a fax group and associate it with a line group.
10. Now whenever an inbound fax lands on the SALE mailbox, those sales personnel on the SALE distribution list will receive the fax in their mailbox. They can then read the fax either in their Email Inbox (UM basic) or by using the Web View interface (UM+MWI).

Scenario 2 - Setting up Fax Reception for a Personal Fax Number (Personal Fax)

Mike in Sales would like to have his own fax number, 727-MIKE (6453), that he can give to his clients. This number is different than the DID number to his phone: 727-6452. This is so that he can receive confidential faxes from clients without sharing them with his colleagues. To configure private fax reception for Mike:

1. Obtain the DID number 727-6453 from the local PSTN.
2. Program a (phantom) set on the PBX with the directory number 6453.
3. Configure this set to always forward to the NuPoint Unified Messaging voice mail hunt group.
4. Program DID routing to forward calls to this set. Typically this is done by simply absorbing the NXX part of the DNIS and routing the call to the extension matching the remaining digits.
5. Create a mailbox on the NuPoint Unified Messaging server with the number 6453.
6. Assign the mailbox an FCOS with bits: 122 (broadcast), 190 (receive fax), 198 (receive fax only), 203 (walkaway fax).
7. Create one distribution list for this mailbox.
8. Add Mike's mailbox (6452) to this distribution list.
9. Give Mike either UM Standard SMTP or UM Standard Web VIew (to be able to use the Web View Interface).

Scenario 3 - Setting up Fax Reception for Multiple Mailboxes (Personal Fax)

Mike's office neighbours, seeing that Mike has his own DID number for fax, may want the same feature. Not everyone is as highly productive as Mike, but ACME would like to give everyone the ability to receive confidential/personal faxes without spending money for a DID. To provide personal fax reception to others without spending money on DIDs:

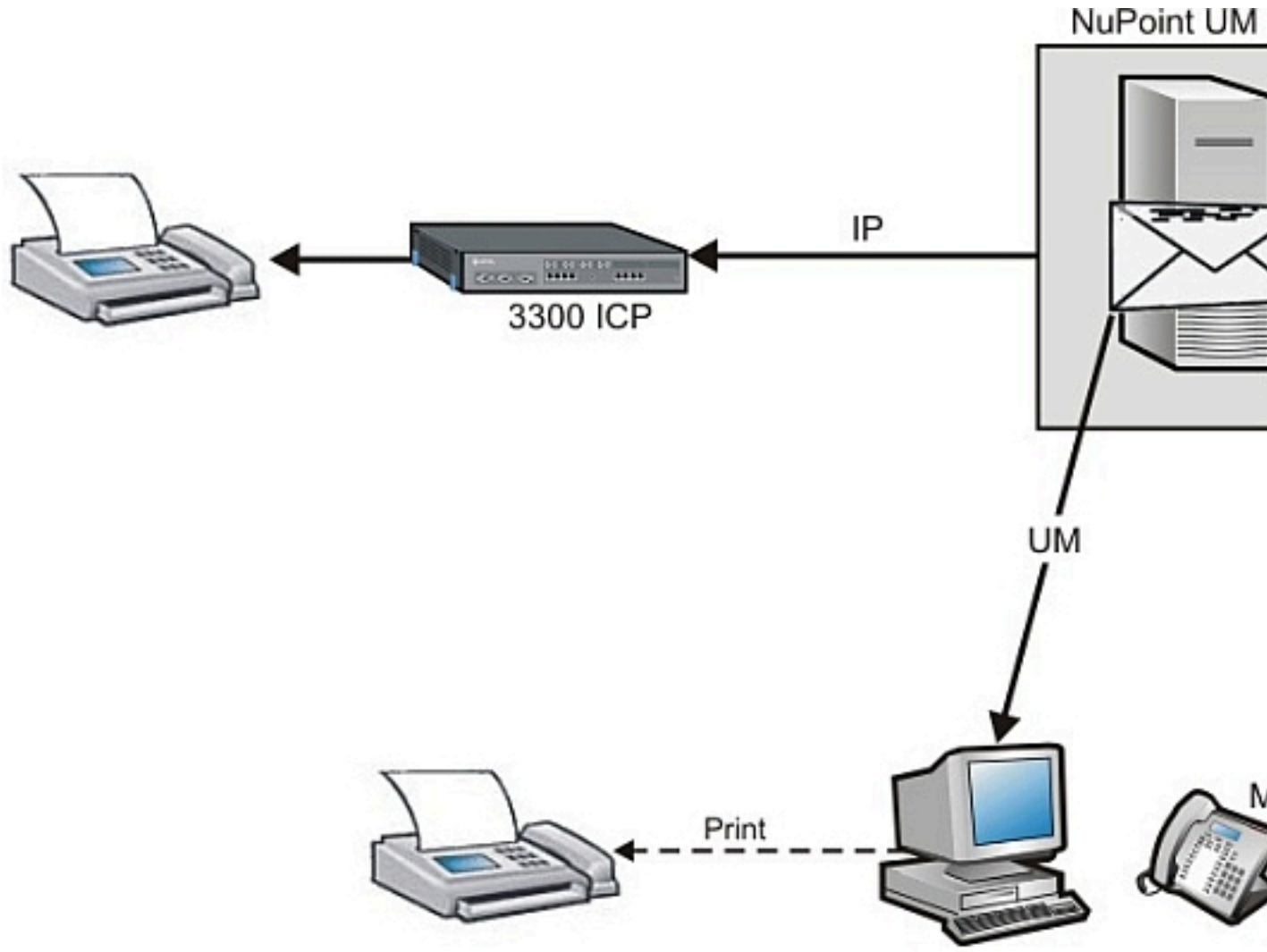
1. Give FCOS bits: 190 (Receive Fax Messages), and 203 (Walkaway Fax for Callers) to those wishing to receive faxes.
2. Tell these users to change their voice mail greetings to instruct callers about how to send them a fax: "Hello, this is Bob. If you would like to send me a fax, please press the SEND button now."

To send a fax to one of these mailboxes, the caller would call that person's extension. When the extension forwards the call to voice mail, upon hearing the greeting, the caller can press the SEND button on their fax machine.

Outgoing Fax

Several outgoing fax scenarios are possible with the NuPoint Unified Messaging Fax feature, where a user forwards a fax to email, sends to a fax number, or replies by email to a fax message. This section overviews user operation of the Fax feature, using the Web View interface and the TUI. For detailed end-user instruction, refer to the NuPoint Unified Messaging *Web View Help* and the *Messaging User Guide*.

The illustration below shows a MiVoice Business ICP directly integrated with a NuPoint Unified Messaging server.



Scenario 1 - Sending a Fax to a Fax Machine

A user can send a fax that they have received to a fax machine so that they have a hard copy of the fax or so that others can receive the fax. A fax can be sent to multiple fax machines.

From the Web View

For detailed user instructions about sending a fax from the Web View interface, refer to the NuPoint Unified Messaging *Web View Help.*

1. A received fax is stored in the recipient's mailbox as a new message.
2. NuPoint Unified Messaging lights the MWI of the recipient's phone.
3. The recipient dials into their voice mail and sees that there is a new fax message, or the user checks their Message tab in the Web View interface (must be a licensed UM Standard Web View user) and sees that there is a new fax message.
4. The recipient uses the Web View to view the fax (this launches the TIFF viewer available on the recipient's PC).
5. The recipient decides to send the fax to the local fax machine.

6. The recipient selects the fax message and presses the "Send Fax" button in the Web View interface, enters the number of the fax machine, and sends the fax to that machine.

From the TUI

For user instructions about sending a fax message to a fax machine from the TUI, refer to the NuPoint Unified Messaging *User Guide*.

1. A user has a fax in their mailbox that they would like to send to a fax machine.
2. The user dials into their voice mail and the TUI gives them the option to send the fax message to a fax number.

Scenario 2 - Forwarding a Fax to E-Mail

From the Web View interface or the user's email account, a user can forward a fax message by e-mail, as a .TIF attachment. Refer to the NuPoint Unified Messaging *Web View Help.*

Scenario 3 - Reply to a Fax by E-Mail

From the Web View interface or the user's email account, a user can reply to a fax message by e-mail, with or without the fax as a .TIF attachment. Refer to the NuPoint Unified Messaging *Web View Help.*

26.86.3 NP Fax - Conditions

In addition to the following conditions, refer to the NuPoint Unified Messaging *Engineering Guidelines* for recommendations about implementing a Fax solution.

- The system must have a fax group assigned to an outbound line group to deliver faxes send faxes. Additionally, a “fax pager index” must be set in the user’s mailbox.
- The system must have a fax group assigned to an inbound line group to receive faxes.
- The Fax feature supports fax reception from G3-compliant fax machines that produce CNG tone.
- To minimize packet loss and jitter, it is recommended that the NuPoint Unified Messaging server be connected to the PBX or MiVoice Business Gateway via one hop only.
- NuPoint Fax can be configured on any NuPoint UM server. Note that Fax only operates on the active server in an Active/Passive configuration.
- A maximum of six Fax channels can be configured on a NuPoint Unified Messaging server.
- If all six Fax channels are in use when a user is sending a fax, the fax is queued for re-try. When an outside caller sends a fax and all channels are busy, that caller receives an "unsuccessful transmission" message.
- You must have an Internet connection to use Fax with the Web View interface (requires a Web session).
- NP View is not supported for use with NuPoint Fax.
- NuPoint Unified Messaging does not support a specific TIFF or PDF viewer for reading faxes. If a user has difficulty reading faxes with a viewer, it is recommended that they refer to the help documentation for that viewer or try using a different viewer.
- Apple QuickTime Player is not supported within the Web View interface for users to display fax .tif files. It is recommended that Quick-Time be configured not to play .tif files, on the user's PC. For this procedure, refer to the *Web View Help*.

- Tenanting: Each tenant has their own line groups. Each may also need to have their own fax DID. This can be accommodated by one or more fax groups since one fax group can be associated with many line groups. Keep in mind that there are only 6 fax channels on one server that can be shared.
- Migration of Fax from a NuPoint Messaging Release 7.0 system is supported; however, as with line groups, fax group definitions are not migrated and must be reprogrammed manually. Note that all fax ports must be configured in the range of 5:0 to 5:5. The Cover Page FCOS is supported after conversion. Migration from a Release 7.0 system will handle all FCOS relating to inbound Fax features. For more information about migrating from a Release 7.0 system, see the *NuPoint Unified Messaging Technician's Handbook*.
- Fax messages are supported in the NuPoint Unified Messaging system backup and restore operations.
- The Event Recorder will contain all Fax-related error messages. For more information about Event Recorder, see the *NuPoint Unified Messaging Technician's Handbook*.
- NuPoint UM does not support the use of the NP Fax feature as a fax server.

26.87 Overview

This section provides information to help you understand and plan the changes that you must make to your software configuration when you add NuPoint Fax applications to your NuPoint Unified Messaging server. It describes all of the software options for NuPoint Fax, and explains how they are used in the various applications.

The following topics are discussed:

- Planning Outside Caller Access
- Fax Class of Service Parameters
- Adding NP Fax options to Class of Service
- Planning Fax Mailboxes

26.87.1 Fax Class of Service Parameters

The system administration menus contain NuPoint Fax configuration parameters for feature, limit, and network classes of service (FCOS, LCOS, and NCOS). All of these options are described below. Read through the descriptions before completing the Fax worksheets. Some of the options are similar to those for voice messaging, some are not unique to fax handling but must be assigned to a mailbox for using Fax with the Web View Interface, and some are unique to fax handling. When you assign a NuPoint Fax feature to a mailbox, the appropriate user and outside caller prompts are enabled automatically. The voice prompts are described in the NuPoint Unified Messaging *User Guide*.

Note:
FCOS assignments take effect only after one or more fax channels have been assigned to a line group.

FCOS Feature Bits for Fax

The feature bits described below are used with NuPoint Fax.

110 Make/Give to Telephone Number

Allows a mailbox owner to make or give a message to a telephone number outside the mailbox system; known as “call placement.” This feature bit is required for a user to send faxes to external numbers. It is not required if faxes will be sent to internal numbers only. This feature bit is required for the fax printing feature.

190 Receive fax messages (master feature)

This feature allows a mailbox to receive fax messages. When callers reach the mailbox, they are first prompted to leave a voice message (cover sheet), then prompted to press L to leave a fax with the voice message. Callers can ignore the message prompt and press L to leave a fax without a voice cover sheet. When the user accesses the mailbox, the user is informed that there is a message with a fax there and given options to retrieve the fax online or direct the fax to a fax machine after hearing the voice message.

Note:

- Mailboxes must also include one or more of the fax delivery features (193, 194, 195, 237) to permit the users to retrieve faxes stored in the mailboxes.
- If feature bit 240 is enabled, callers do not need to press L to begin sending a fax; the system will detect an incoming fax when it does not hear speech.
- If feature bit 290 is also assigned to the mailbox, users can view fax messages through the Web View interface.

191 Make fax messages

When this feature is assigned to a mailbox, the mailbox owner can make a voice message, and then press L to leave a fax with the message. The fax is then delivered to the addressed party or parties with the voice message.

192 Give fax messages

This NuPoint Fax feature allows users who are able to receive faxes in their mailboxes to forward the faxes along with voice comments directly to other users or to outside lines. They cannot include another fax as a comment.

Note:
This feature requires feature bit 190.

193 Deliver fax to default fax phone number

This feature allows a user to have faxes delivered to a personal (default) fax telephone number after listening to the voice annotation. This number can be a department or company fax machine and is entered by the system administrator during configuration. When the user selects this option, another menu is played giving further options to schedule delivery, cancel delivery, or deliver the fax now.

Note:
This feature requires bit 190. The system must have a fax group connected to an outbound line group to deliver faxes to phone numbers.

194 Deliver fax online

This feature permits users accessing their mailboxes from a fax phone to receive stored faxes online.

Note:
This feature requires feature bit 190. The system must have a fax group connected to an inbound line group to deliver faxes online.

195 Deliver fax to designated telephone number

When this feature is included in a mailbox and the user wishes to retrieve a fax or deliver it to someone else after listening to the voice annotation, the prompt "Press I to input a number for this fax" is included in the fax transmittal options menu. After the user selects "I" and inputs the number, another menu is played giving the choices of scheduling the delivery, canceling it, or having the fax delivered now.

Note:
This feature requires bit 190 for fax functionality and bit 95 to schedule fax delivery. The system must have a fax group connected to an outbound line group to deliver faxes to phone numbers. Additionally, a “fax pager index” must be set in the user’s mailbox.

196 User changeable default fax phone number for fax delivery

This feature allows users to change their personal (default) fax delivery numbers through the user options menu in their mailboxes.

Note:
This feature requires bit 193.

197 Fax on demand

This feature is for Fax Publishing. When it is assigned to a greeting only mailbox, the caller is greeted and given a prompt to get ready to receive the fax deposited in the mailbox, either online or at another number. The mailbox LCOS and RCOS control the delivery features.

Note:
This feature requires feature bit 194 and/or 195.

198 Receive fax messages only

This feature prevents a mailbox from receiving voice messages and allows it to receive only fax messages. It is used for both Guaranteed Fax and broadcast mailboxes in Fax Mail. No greeting or prompts are played to the calling party and only faxes are recorded. A fax session starts immediately when the server answers the call.

A Guaranteed Fax mailbox must have both this bit (198) and message delivery enabled.

Note:
This feature requires feature bit 190.

199 Automatic receipt for successful fax message sent

When this feature is included in a mailbox and the user schedules a fax delivery, a receipt with a time stamp is automatically placed in the mailbox indicating whether the transmission succeeded or failed. When this feature is *not* included in a mailbox, a receipt is issued only if the transmission fails.

Users can also receive email notification concerning the status of the fax transmission. To receive confirmation of successful and failed fax transmissions, configure an email address and enable this feature for the user's mailbox. To receive confirmation of successful fax transmissions only, configure an email address but leave the feature disabled.

Note:
This feature requires feature bit 190 and feature bit 193 or 195.

200 Fax cover page

This feature causes the system to send a cover page with outgoing faxes. The cover page identifies the user as the fax recipient at the company or department fax machine. Mailbox owners can fax a personal cover page into their mailboxes which the system sends each time they retrieve faxes. When a cover page is deposited in the system administrator's mailbox, it becomes the company fax cover page and it is delivered with faxes retrieved by users who do not have a personal cover page. If neither a personal cover page nor a company cover page is available, the system generates a default cover page.

If this bit is not enabled in an FCOS, the system does not send any cover sheet with outgoing faxes.

Note:
Feature bit 230 disables the mailbox personal fax cover page option so that mailbox owners cannot override the company or default cover page.

203 Walkaway fax

A mailbox with this feature is set to expect calls from fax machines rather than from live callers. When a call is routed to a mailbox with this feature, CNG (tone transmitted by a fax machine when it calls another fax machine) detection is enabled while the mailbox greeting is playing. If the system detects fax tone, it processes the incoming fax. If it does not detect fax tone, it plays the recorded mailbox greeting and prompts. This permits callers to dial into a user's mailbox and immediately send a fax without a voice cover sheet, and without having to respond to prompts or monitor the call.

Feature bit 256 causes the system to play a brief introductory prompt for walkaway fax mailboxes.

Note:
When feature bit 203 is active, the system listens for fax tone (CNG) in order to act like a receiving fax machine when the call is initiated by a sending fax machine.

When feature bit 240 is active, the system always defaults to accepting a fax when it does not detect voice. This is similar to the function of bit 203, however, callers will hear fax signals if their voice recording times out.

This feature requires feature bit 190.

206 Fax delete

This feature automatically deletes a fax from a mailbox after it has been delivered. It is used in Guaranteed Fax to prevent re-sending the same message to the fax machine.

Note:
Feature bit 237 (Automatically deliver fax to default number) overrides this feature. 237 is for user mailboxes, not guaranteed fax mailboxes. Do not use both bits in the same FCOS.

207 Fax verify

This feature is assigned to Guaranteed Fax mailboxes which are on the same hunt group as the fax machines. It checks incoming faxes with those already stored in the mailbox to prevent the same fax from rotating through the hunt group and getting stored in the mailbox again when the fax machine is down or busy.

230 Deny change to fax cover page

This feature disables a mailbox owner's ability to create a personal fax cover page. If feature bit 200 is enabled, the system will send either a company cover page (if one has been placed in the administrator's mailbox) or the system default cover page. This feature has no effect if bit 200 is not enabled.

235 Display from field on fax cover page

This feature adds the "From" field to the default fax cover page. The field identifies the *system* that the fax came from, such as, "ABC Communications Fax Service." It does not identify the mailbox owner. The text of the "From" field is set in the Fax Service and Promotional Message Menu.

236 Display promotional field on fax cover page

This feature adds a promotional message field to the default fax cover page. The text of the promotional message field is set in the Fax Service and Promotional Message Menu.

237 Automatic fax retrieval

This feature allows the mailbox owner to have faxes downloaded automatically to a pre-configured default fax number when faxes arrive in the mailbox. The fax or voice/fax message is automatically moved to the saved queue and the message waiting indicator is not triggered. This feature is intended to make it easier for mailbox owners who regularly use the same fax machine to retrieve their faxes. The mailbox owner can also enable or disable this feature from the user options menu.

Note:
When this feature is active, the mailbox owner should check the target fax machine frequently, since fax messages do not activate a message waiting indicator.

This feature overrides feature bit 206 (Discard fax message after delivery). 206 is for guaranteed fax mailboxes only. Do not include both bits in the same FCOS.

239 Retrieve all unplayed faxes

This feature makes it easier for mailbox owners to get their faxes. If they do not have automatic fax delivery enabled, they have the option to have all faxes concatenated and sent at once. The user selects the "retrieve all faxes" option from the user options menu and all the faxes are automatically sent to the user's default fax number.

Note:
This feature requires one or more of feature bit 193, 194, or 195.

240 Receive fax on record time-out

This feature makes it easier for callers to send fax-only messages and voice/fax messages. In the case of fax-only messages, a caller can dial into a mailbox, press start, and walk away. In the case of the voice/fax message, the caller does not need to press L to send the fax.

Note:
When feature bit 203 is active, the system listens for fax tone (CNG) in order to act like a receiving fax machine when the call is initiated by a sending fax machine. Without bit 203, callers to a mailbox must press L to indicate that they want to leave a fax.

When feature bit 240 is active, the system always defaults to accepting a fax when it does not detect voice. This is similar to the function of bit 203, except that the user does not have to press L to leave a fax. However, callers will hear fax signals if their voice recording times out.

This feature requires feature bit 190.

256 Enable fixed greeting for walkaway fax

The feature bit causes walkaway fax mailboxes to play the prompt, “Press 1 or wait…” before playing the mailbox greeting.

290 Enable UM Standard Web View

This feature bit must be assigned to a user's mailbox along with feature bit 190 (Receive Fax Messages) for the user to receive and view Fax messages in the Messages tab of the Web View Interface.

LCOS Limits for Fax

The following fax limits can be included in limits classes of service (LCOS).

Number of digits for fax phone number for fax delivery

This limit restricts the user to the set number of dialing digits when retrieving or redirecting a fax to a designated number. For example, 3 or 4 digits would only allow faxes to be redirected to an internal extension, but 11 or 12 digits would let the user send faxes long distance. If no digits are specified, then the number of digits defaults to that entered for the outside caller dialing plan in the Online Configuration Menu.

Note:
This limit works in conjunction with RCOS NPA/NXX screening.

Number of fax messages per mailbox

This limit is the maximum number of faxes that can be stored in a mailbox at any one time.

CNG tone detection length

This limit is the number of seconds that the NuPoint Unified Messaging server waits to detect the CNG tone from a calling fax machine when walkaway fax is enabled (feature bit 203). This limit should be set to zero except for sites with very noisy phone circuits.

Fax delivery retry frequency

This limit is the number of times the server attempts to send a fax message until it is successfully sent. The system retries fax delivery when it encounters ring no answer, busy, or no available fax resource.

Fax delivery retry interval

This limit is the number of minutes the system waits between retries on delivering a fax message.

Played fax message retention

This limit is the maximum number of hours that played faxes can be stored in a mailbox.

Unplayed fax message retention

This limit is the maximum number of hours that unplayed faxes can be stored in a mailbox.

Urgent fax message retention

This limit is the maximum number of hours that urgent faxes can be stored in a mailbox.

Fax receipt retention

This limit is the maximum number of hours that fax receipts can be stored in a mailbox.

Call Placement limits

Call Placement limits include the same limits and retry intervals and message phone length. Use these parameters to configure fax behavior when using the **Fax Printer Driver** or **Web View** to send faxes.

NCOS Networking Features for Fax

The following options determine a user's fax capability over an NP Net network to other NuPoint Unified Messaging servers. These are entered as part of the network class of service (NCOS).

10 Make fax messages to the network

This feature allows a user to make a fax message and send it over the network.

11 Give fax messages to the network

This feature permits users to forward fax messages deposited in their mailboxes to users on another system over the network. It does not allow users to make a fax message to the network.

12 Answer fax messages to the network

A user with this feature can reply to a fax message that was sent from another system over the network. If feature bit 38 is activated, the original message, voice and fax, will be sent with the reply back across the network.

NuPoint Fax and RCOS

Like all other types of outbound calls, outbound NuPoint Fax calls are controlled by the Restriction Class of Service of the sending mailbox. A mailbox owner cannot have a fax delivered to a phone number that is blocked in their RCOS.

26.87.2 Adding NP Fax Options to COS

Add NP Fax options to mailboxes exactly as you would voice message options. You can include them in existing or new FCOS, LCOS, and NCOS. You must generate new COS for applications that are exclusive to NP Fax, such as Guaranteed Fax and Fax Publishing.

Here are some fax mail FCOS options:

- VIP FCOS + 190-196 and 200: User can receive and send fax messages and include a cover sheet. Callers must use the phone keypad to send a fax.
- **VIP FCOS + 190-196, 200, and 203:** Same as above, but callers can also send walkaway fax messages.
- **VIP FCOS + 198 and 200:** Fax only mailbox; receives fax messages with no voice annotation and supports a cover page. Use bits 193-195 to retrieve messages.

To plan adding Fax options, refer to the NP Fax COS Planning Worksheet (below). The Fax FCOS and NCOS bits and names are included at the top of the worksheet for your reference.

If you add fax features to an existing COS without renumbering the COS, existing mailboxes with that COS assigned will take on the added fax features. If you create a new COS by copying an existing one and modifying it, you must assign the new COS to mailboxes

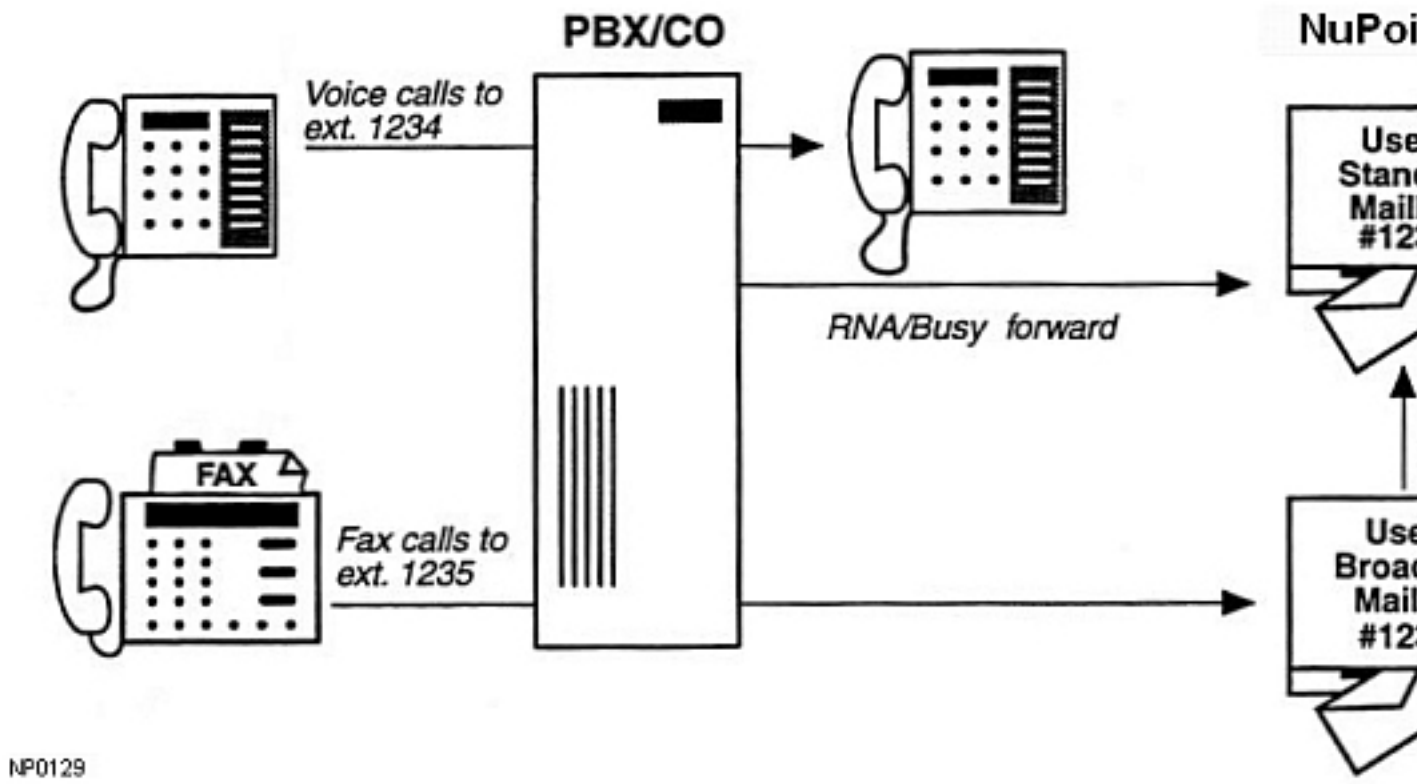
Note that there are entries for users' standard mailboxes and users' broadcast fax mailboxes. If a user is likely to receive many fax calls, they should have a separate extension for faxes that has an associated broadcast mailbox. The broadcast mailbox contains a distribution list consisting of only the user's standard NP Voice mailbox. Messages or faxes left in the broadcast mailbox are immediately transferred to the user's standard mailbox, as shown below.

To prevent broadcast mailboxes from filling up, the FCOS should not include the Receive message bit.

To prevent broadcast mailboxes from filling up, the FCOS should not include the Receive message bit.

To prevent broadcast mailboxes from filling up, the FCOS should not include the Receive message bit.

Broadcast Mailbox Fax Mail Application



NP Fax COS Planning Worksheet (Sample)

FaxMemo COS Planning Worksh

Fax Feature Bits

Number	Description
190	Receive Fax Messages
191	Make Fax Messages
192	Give Fax Messages
193	Deliver Fax to Default Fax Phone Number
194	Deliver Fax Online
195	Deliver Fax to Designated Phone Number
196	User Changeable Default Fax Phone Number for Fax Delivery
197	Fax on Demand
198	Receive Fax Messages Only
199	Automatic Receipt for Fax Sent
200	Personal Fax Cover Page
203	Walkaway Fax
206	Fax Delete

Fax Feature

207	Fax Ve
230	Deny C
235	Add "Fr
236	Add "Pr
237	Automa
239	Retriev
240	Receiv
256	Enable
290	Enable

Fax NCOS Bi

Number	
10	Make F
11	Give Fa
12	Answer

COSs for User's Normal Mailbox

FCOS # to Modify	New FCOS Number	New FCOS Name	FAX
10	22	VIP Fax	190, 196, 200, 203

LCOS Number	Number of Digits for Fax Delivery	# Fax Msgs per Mailbox	Fax Delivery Retry Frequency	Fax Delivery Retry Interval	CNG Tone Detection Length	Played Fax Msg Retention	
1	11	5	5	2	0	336	

NCOS # to Modify	New NCOS Number	New NCOS Name	FAX
1	1	Network Fax	10, 11, 12

NP Fax COS Planning Worksheet (Blank)

FaxMemo COS Planning Works

Fax FCOS Bits

Number	Description
190	Receive Fax Messages
191	Make Fax Messages
192	Give Fax Messages
193	Deliver Fax to Default Fax Phone Number
194	Deliver Fax Online
195	Deliver Fax to Designated Phone Number
196	User Changeable Default Fax Phone Number for Fax Delivery
197	Fax on Demand
198	Receive Fax Messages Only
199	Automatic Receipt for Fax Sent
200	Personal Fax Cover Page
203	Walkaway Fax
206	Fax Delete

Fax FCOS Bi

207	Fax V
230	Deny
235	Add "
236	Add "
237	Auton
239	Retrie
240	Rece
256	Enabl
290	Enab

Fax NCOS B

Number	
10	Make
11	Give
12	Answ

COSs for User's Normal Mailbo

FCOS # to Modify	New FCOS Number	New FCOS Name	FA

LCOS Number	Number of Digits for Fax Delivery	# Fax Msgs per Mailbox	Fax Delivery Retry Frequency	Fax Delivery Retry Interval	CNG Tone Detection Length	Played Fax Msg Retention

26.87.3 Planning Fax Mailboxes

Planning and configuration for mailboxes in each NuPoint Fax application is slightly different. This section contains information and sample worksheets for mailbox configuration for each application:

- Fax Mail
- Fax Broadcast
- Guaranteed Fax
- Fax Publishing

A worksheet is also supplied for Fax Cover Page planning.

Note:
There is no separate worksheet for Walkaway Fax. You can add Walkaway Fax to any of the other NuPoint Fax applications by enabling the appropriate feature bits (190, 203, 256) in an FCOS.

Fax Mail Mailbox Configuration

The Fax Mail Mailbox Worksheet associates mailboxes with COS options. A sample worksheet is shown below. You can photocopy and complete a blank Fax Mail Mailbox Worksheet (below) following the sample worksheet and the instructions given here.

List all the mailbox owners and their current mailbox numbers on the sheet. Add the new COS numbers for the current mailboxes. If you are going to use broadcast mailboxes, add those mailbox numbers and the COS to be assigned to them. Remember that the broadcast mailboxes must be new boxes. If possible, use a numbering scheme for the broadcast mailboxes that is easy for the users to remember when they need to give their fax numbers out to callers.

Fax Mail Mailbox Worksheet (Sample)

Fax Mail Mailbox Worksheet

Mailbox Owner's Name	Current Mailbox to Update					Fax Broadcast Mai Create		
	Number	FCOS	LCOS	NCOS	Default Telephone Number for Fax Retrieval	Number	FCOS	LCO
Smith	3511	10	1	1	555-3200	6511	21	3
Pacheque	4673	10	1	1	555-3200	-	-	-

Prepared By: _____ Date: _____

Configured By: _____ Date: _____

Fax Mail Mailbox Worksheet

Fax Mail Mailbox Worksheet

Mailbox Owner's Name	Current Mailbox to Update					Fax Broadcast Mailbox		
	Number	FCOS	LCOS	NCOS	Default Telephone Number for Fax Retrieval	Number	FCOS	LCO

Fax Broadcast Mailbox Configuration

If you set up special distribution list mailboxes for fax broadcasting, use the Fax Broadcast Mailbox Worksheet at the end of this manual. A sample worksheet is shown below. Use one worksheet for each distribution list mailbox. Enter the mailbox number to create or modify and the COSs to assign to it, then list the mailboxes and owners' names for the distribution (broadcast) list.

Fax Broadcast Mailbox Worksheet (Sample)

Fax Broadcast Mailbox Worksheet

Mailbox No: 6777 Name: Sales Fax Broadcast

FCOS No: 20 LCOS No: 5 NCOS No: -

Distribution (Broadcast) List

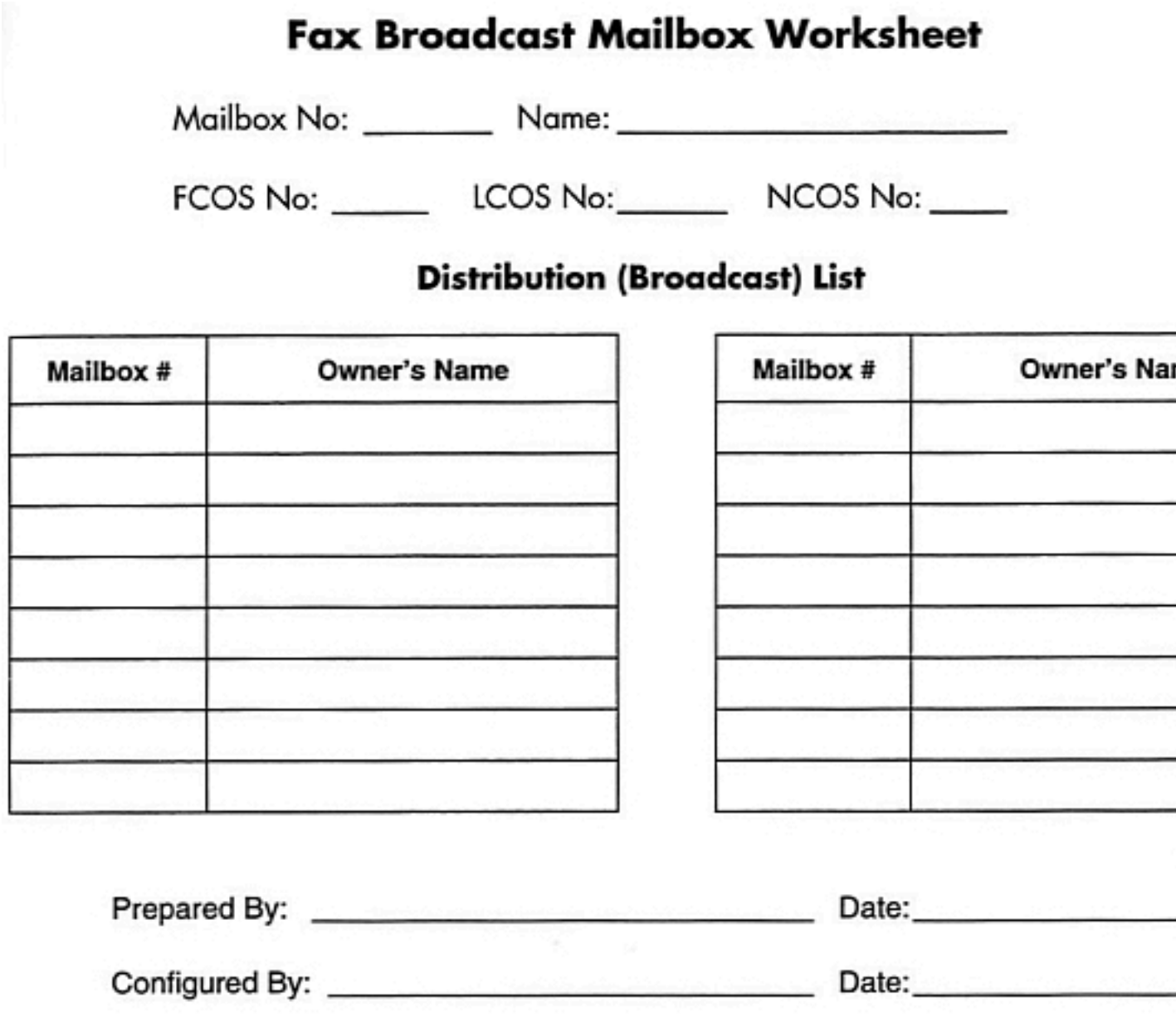
Mailbox #	Owner's Name
4212	Douglass
4256	Garcia
4235	Johnson
4354	Sojourner
4222	Budris
4343	Dayharsh
4274	Vilahu

Mailbox #	Owner's Na

Prepared By: _____ Date: _____

Configured By: _____ Date: _____

Fax Broadcast Mailbox Worksheet



Fax Broadcast Mailbox Worksheet

Mailbox No: _____ Name: _____

FCOS No: _____ LCOS No:_____ NCOS No: _____

Distribution (Broadcast) List

Mailbox #	Owner's Name

Mailbox #	Owner's Na

Prepared By: _____ Date:_____

Configured By: _____ Date:_____

Guaranteed Fax Mailbox Configuration

For Guaranteed Fax, use the VIP FCOS with bits 198, 206, and 207 and enable message delivery. This mailbox delivers one copy of each fax message it receives to your fax machine and deletes each fax after it is successfully sent to the machine.

A sample Guaranteed Fax Mailbox Worksheet is shown below. Blank worksheets for photocopying are at the end of this manual. Fill in the telephone numbers in the hunt group. For example, if your fax machine is on 555-3200, assign mailboxes to 555-3201, 555-3202, and so on. Enter the COS for the mailboxes and the fax number you want them to deliver faxes to.

Guaranteed Fax Mailbox Worksheet (Sample)

Guaranteed Fax Mailbox Worksheet

Fax Machine No./Name: 555-3200 Sales Order Entry

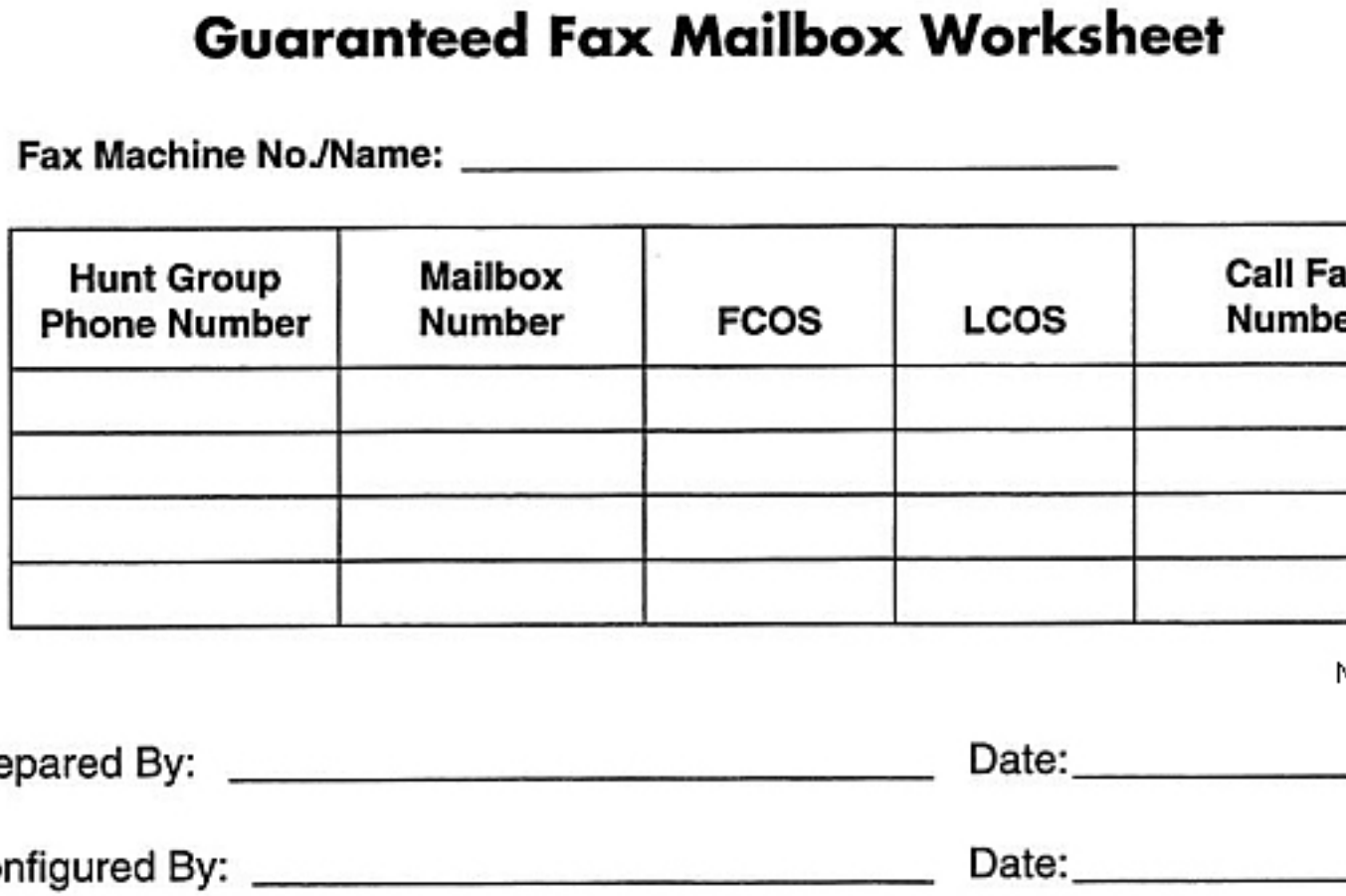
Hunt Group Phone Number	Mailbox Number	FCOS	LCOS	Call Fax Number
3201	3201	22	6	3200
3202	3202	22	6	3200

NP01

Prepared By: _____ Date: ____

Configured By: _____ Date: ____

Guaranteed Fax Mailbox Worksheet



Guaranteed Fax Mailbox Worksheet

Fax Machine No./Name: _____

Hunt Group Phone Number	Mailbox Number	FCOS	LCOS	Call Fa Numbe

Prepared By: _____ Date: _____

Configured By: _____ Date: _____

Fax Publishing Mailbox Configuration

For fax publishing, you can use any of these types of mailboxes:

Tree

A tree mailbox routes callers to other mailboxes when they press one of the keypad numbers. You must assign the proper features to the mailbox (refer to the Mailboxes section) create distribution list 01 in the mailbox with the “go to” mailboxes in keypad input order, and record a message in the mailbox directing the caller to press specific keypad numbers for different information. The “go to” mailboxes can also be tree mailboxes, branching the caller further for more specific information.

Chain

A chain mailbox accepts other mailbox numbers from the caller and branches to them. Refer to the Mailboxes section for chain mailbox features.

Greeting with fax

This mailbox plays your recorded greeting and directs the caller to receive the associated fax.

Greeting only

This type of mailbox can be used within a fax publishing and audiotext application to give a voice only information message, such as the initial welcome greeting to callers.

Fax on demand

Use a greeting only mailbox with bits 194, 195, and 197 to permit callers to receive a pre-stored fax online or at a caller-designated number.

Fax only

A fax only mailbox plays any greeting and immediately prepares to receive a fax. This can be used in larger fax publishing or audiotext applications to allow the caller to input a fax message.

A sample Fax Publishing Mailbox Worksheet follows. Blank worksheets are at the end of this manual. For tree and chain publishing, you need a separate worksheet for each mailbox. Number the worksheets and fill the sheet numbers in the “Continue on Sheet” or “Go to Sheet” columns, so you can follow the progression through the tree or chain.

Write out the greeting, if any, that you want recorded in the mailbox. Enter a description or title of the fax document you want stored in the fax transmittal mailbox or attach it to the worksheet.

Fax Publishing Mailbox Worksheet (Sample)

Fax Publishing Mailbox Worksheet

Mailbox No: 5223 Name: Fax Publishing Index Sheet No: 1

Mailbox Type (Check only one):

☐ Tree ☐ Chain ☐ Greeting Only ☐ Fax Only ☒ Greeting with F

FCOS No: _____ LCOS No: _____

Tree

Input	Go To Mailbox #	Continue on Sheet #
1		
2		
3		
4		
5		
6		
7		
8		
9		

Chain

Input	Go to She

Greeting: You have selected the index of all documents available in the fax publ
system

Fax Document: Index

Prepared By: _____ **Date:** _____

Configured By: _____ **Date:** _____

Fax Publishing Mailbox Worksheet

Fax Publishing Mailbox Worksheet

Mailbox No:____ Name:_____Fax Publishing Index: _____ Sheet N

Mailbox Type (Check only one):

☐ Tree ☐ Chain ☐ Greeting Only ☐ Fax Only ☐ Greeting wit

FCOS No:_____ LCOS No: _____

Tree

Input	Go To Mailbox #	Continue on Sheet #
0		
1		
2		
3		
4		
5		
6		
7		
8		
9		

Chain

Input	Go to S

Greeting: _____

_____

_____

_____

Fax Document: _____

Prepared By: _____ **Date:** _____

Company Fax Cover Page

The last item you need to plan is your company fax cover page. The cover page is delivered with all faxes, except faxes from users who have their own cover page. Lay out an 8.5" by 11" page with your design. You should include your company name, address, telephone number, and fax number. You can also add your company logo and a short message indicating that the fax is from your company.

Fax the company cover page into the system administrator's mailbox(es) from the User Options Menu. You can assign separate administrator's mailboxes, each with a different cover page, to each outbound line group with fax capability.

If you do not enter a company cover page, the system sends a default cover page for users with no personal cover page. The default cover page contains the mailbox owner's name, the number of pages in the fax, the time and date, and if desired, a from field and a promotional field.

Note:
If you enter a company cover page, it takes precedence over the default cover page and does not include the dynamic information provided on the default cover page.

If feature bit 200 is not enabled for a mailbox, the system does not send any cover page with faxes from that mailbox.

Company Fax Cover Page Worksheet (Sample)

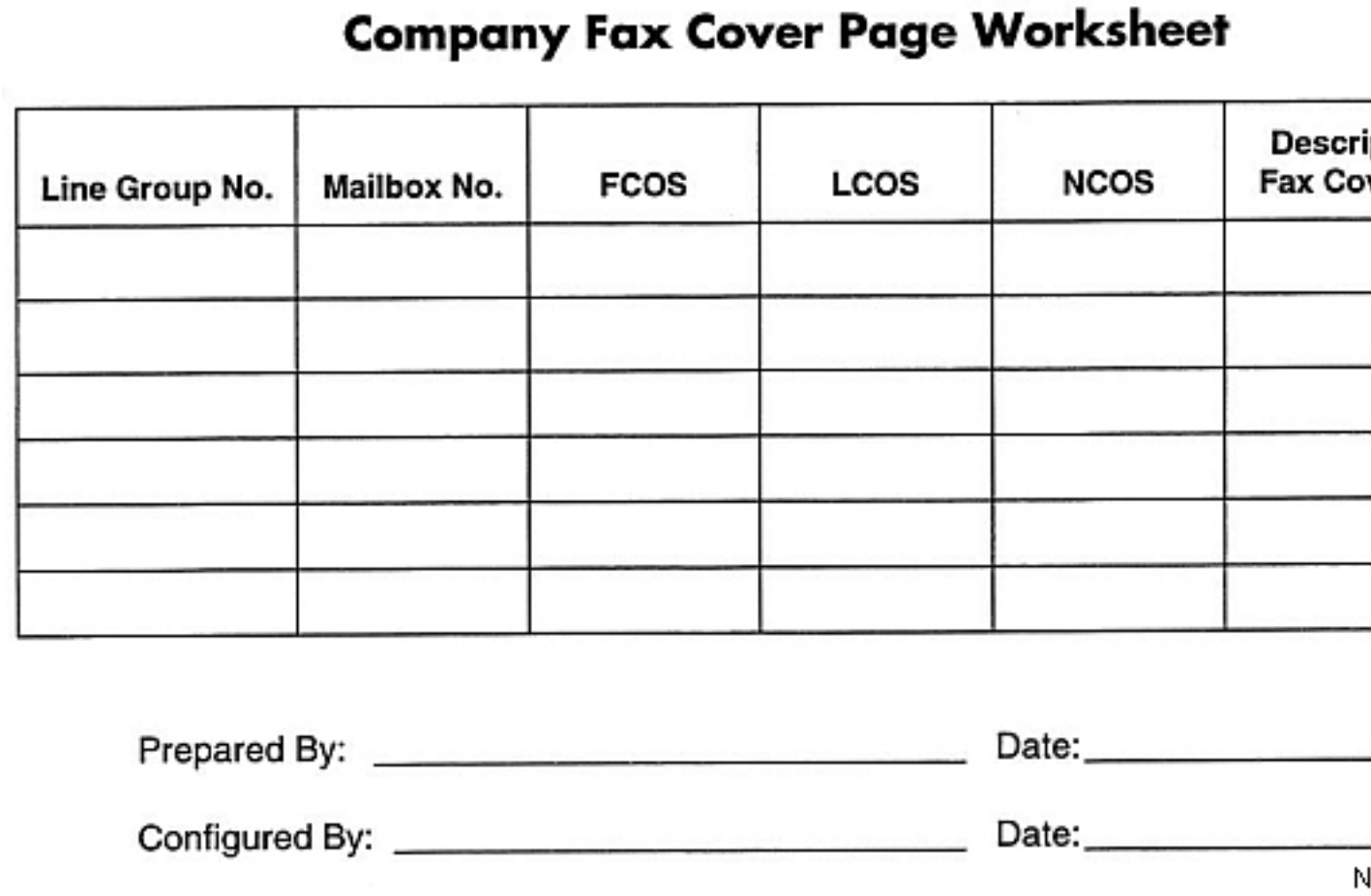
Company Fax Cover Page Worksheet

Line Group No.	Admin Mailbox No.	FCOS	LCOS	NCOS	Descrip Fax Cove
1	9998	10	1	1	ABC C
2	9991	10	1	1	Fax-It-T

Prepared By: _____ Date: _____

Configured By: _____ Date: _____

Company Fax Cover Page Worksheet



Company Fax Cover Page Worksheet

Line Group No.	Mailbox No.	FCOS	LCOS	NCOS	Descri Fax Co

Prepared By: _____ Date: _____

Configured By: _____ Date: _____

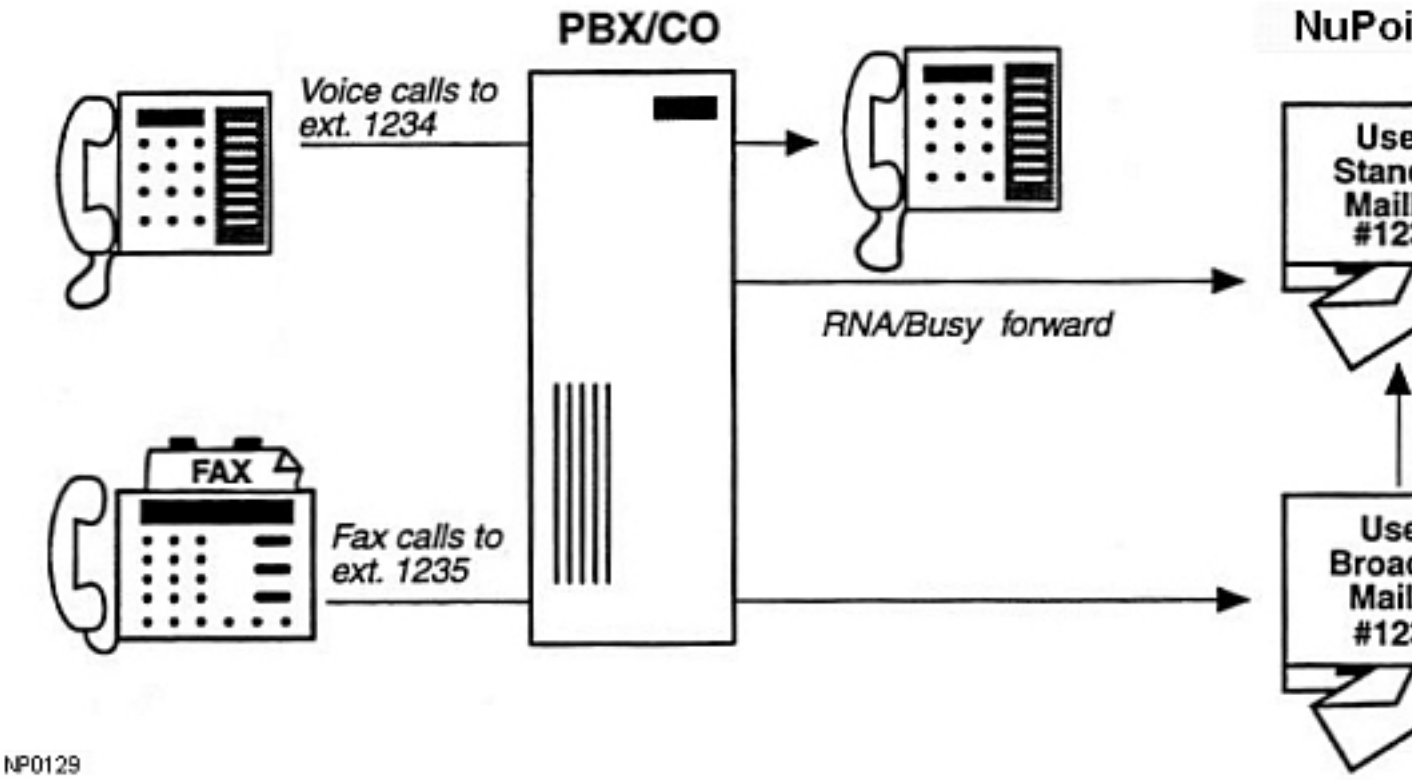
N

26.87.4 Planning Outside Caller Access

With the NuPoint Fax optional feature, outside callers can leave fax messages for mailbox owners just as if they were sending a fax to a fax machine. In most instances, callers believe they are dialing directly to a fax machine, and are not prepared to perform any special functions to deliver a fax. Therefore, for the fax mail application to be effective, the system must allow the callers to deposit faxes into the appropriate mailboxes without any unexpected requirements.

In most NuPoint Fax installations, mailbox owners have two mailboxes on the system. The first is their standard mailbox where they receive and play their messages. The second is a broadcast mailbox with walkaway fax enabled. This mailbox is transparent to the mailbox owner and automatically sends fax messages into the mailbox owner's standard mailbox upon message receipt, as shown below. The reason for the broadcast mailbox is to allow mailbox owners to publish a telephone number where callers can send a fax directly to them. This second number goes directly to the broadcast mailbox without first ringing at any telephone. This allows for a situation that is familiar to both the caller and the mailbox owner.

The Broadcast Fax Mailbox Setup

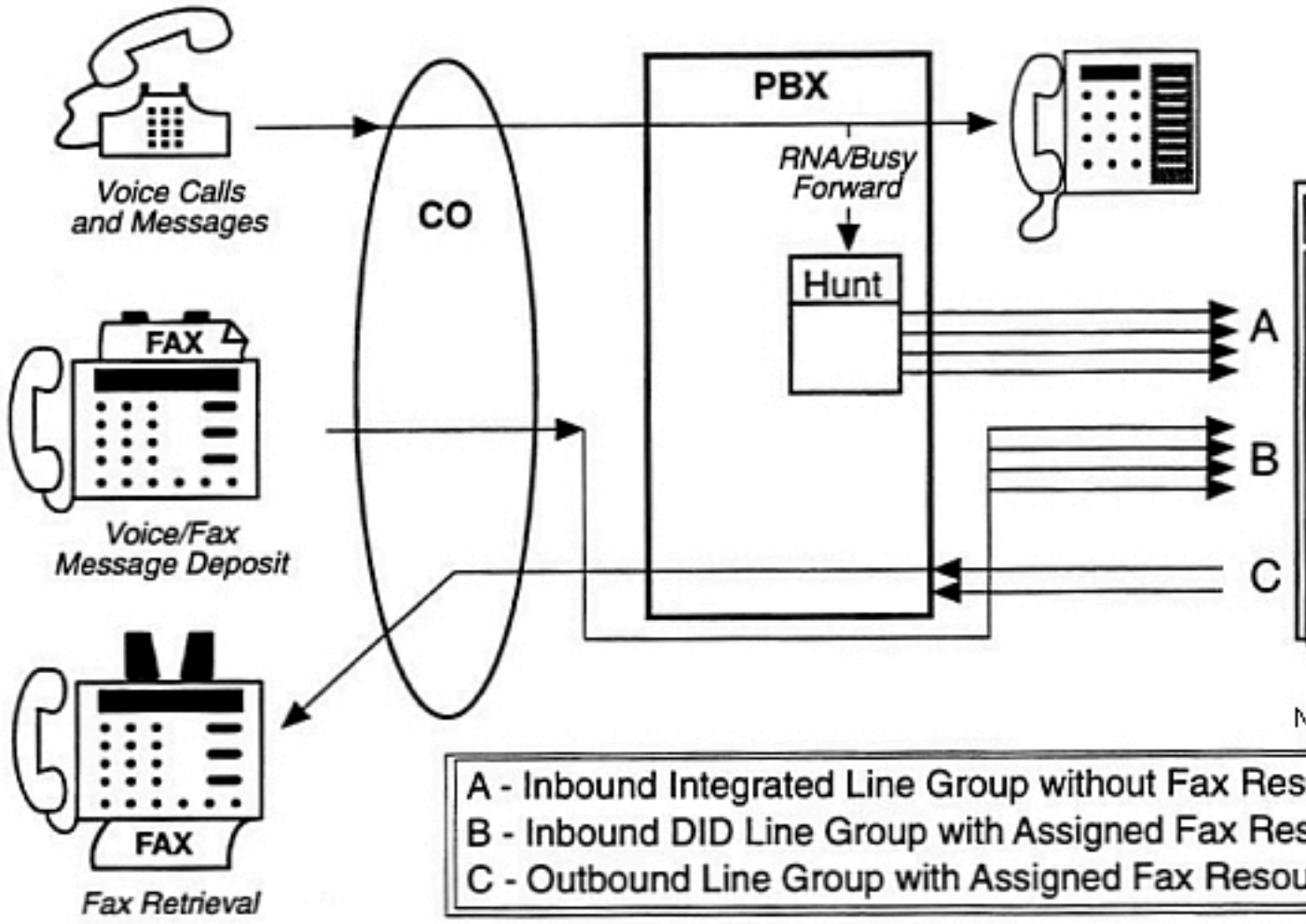


There are several ways that callers sending faxes can be routed to the correct mailboxes. These include DID routing, Switch Integration routing, Switch Tie Trunk Integration routing, and General Access. It is possible to combine two or more of these methods to meet user needs and cost requirements.

Note: The primary purpose of the call routing scenarios in this chapter is to show possible switch connections. There are many ways to configure line groups and assign fax resources. Fax resources can be dedicated to a single line group or shared by inbound and outbound line groups.

DID Fax Call Routing

The simplest routing method is to connect a second NuPoint Fax-equipped inbound line group to DID trunks directly from the CO. In this scenario, each mailbox owner that has fax mail capability is provided with a DID telephone number that allows a caller to deposit a fax message, or voice and fax message, into a broadcast mailbox on the system. Because the DID method involves additional trunks from the central office that bypass the PBX, it can be used in any switch environment. It does incur the expense of the DID lines and DID numbers for all users with NuPoint Fax capability.



Switch Integration Fax Call Routing

Fax Mail is supported by many of the PBX and Centrex integrations. Switch integration works the same way as DID fax call routing in that the caller is directed immediately to the appropriate mailbox. This method requires every person with Fax Mail capability to have a second DID number (both CO and PBX) that goes to a software-only *phantom* extension on the PBX. The phantom extension numbers must correspond to the broadcast mailbox numbers, and must be hard-forwarded to the NuPoint Voice pilot number. This method of fax call routing is shown below.

Method 1

The advantage of this method is that fax calls are answered immediately by the desired party's NuPoint Fax broadcast mailbox, and it does not require any trunks directly from the central office. However, it does require the expense of an additional DID number for each mailbox owner with fax capability.

Not all switches support a phantom extension capability. If your switch does not support this, then you must use another method. If your switch supports multiple in-bound line groups, you can use the second method of switch integration.

Method 2

Switch TIE Trunk Integration Fax Call Routing

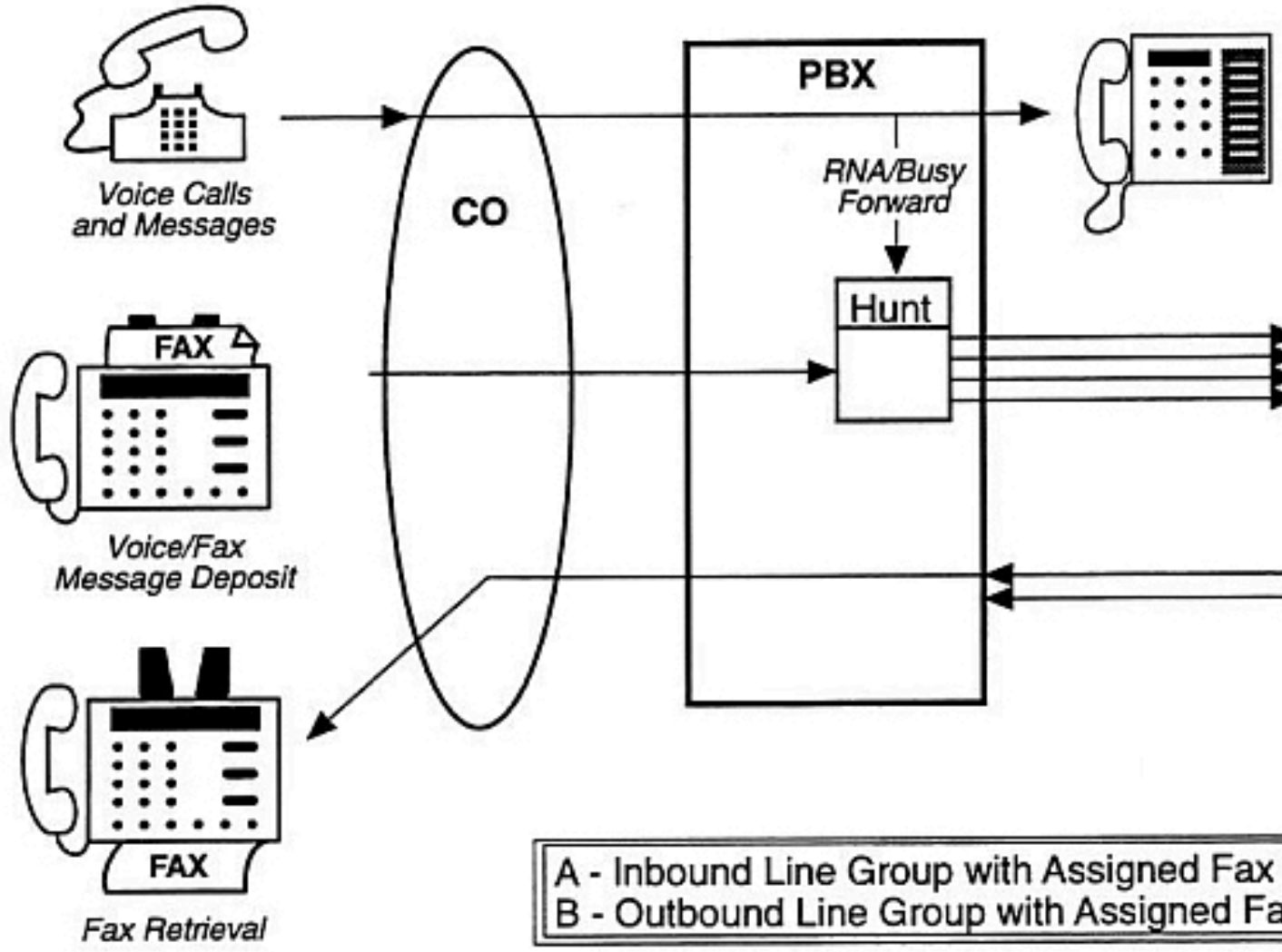
This method utilizes the tandem switching capabilities of many PBXs. If the integration routing method is not supported by your switch, this method still allows you to use a line group to the switch from the CO, but could require additional cards in the PBX. This method also requires everyone with fax capability to have a second DID number from the CO.

When the switch receives a call on one of the DID lines, it passes the call and its related information to the NuPoint Unified Messaging server over a set of TIE trunks. The call information allows the server to connect the caller to the appropriate mailbox.

One disadvantage of TIE trunk integration is that many PBXs do not allow callers to transfer on TIE trunks. If most of the calls on these trunks are fax calls though, few callers need to transfer.

General Access Fax Call Routing

The alternative to DID or switch integration routing is to have a single fax message number that, upon answering, requests that the caller enter the mailbox number of the party who will receive the fax. The figure below shows these calls routed directly to the inbound line group. The advantage of this access method is the security and screening that it offers, since only those who know the mailbox number can access it. This method is available on any PBX or key system with no special hardware or software requirements.



26.88 Overview

Before You Begin

Before you begin a configuration session:

- 1. You must purchase and install the Fax feature.
- 2. Plan your Fax configuration (see the Fax Planning section).
- 3. Ensure that you have the following items to use during configuration of Fax Applications:

- A NuPoint Unified Messaging server console (video monitor and keyboard) and module, with power on
- At least two telephones for configuration testing
- Completed worksheets. (Use the blank worksheets to help you configure Fax. Instructions for completing the worksheets are contained in the Fax Planning section. The configuration procedures assume that you have completed the appropriate worksheets.)

Configuration

Configuration of all fax applications consists of the following tasks:

1. **Define a Fax group**: add a group of virtual Fax channels, quantity determined by Fax feature licensing to a maximum of 6 channels.
2. **Assign the Fax group to Line Groups** that require Fax capabilities. Assign fax to incoming line groups (like NuPoint Voice) to allow for receipt of fax messages. Assign to outgoing line groups (Pager/Outdial) to allow for transmission of outbound fax messages. **Note**: Fax resources are shared among line groups. If all available lines are busy processing incoming fax messages, then no lines are available for outbound messages. In this case, the outgoing messages are queued for retry. (In the case of all lines being busy, the sender of a new incoming fax will receive an error message indicating an unsuccessful transmission.)
3. **Customize an FCOS and LCOS with the Fax feature bits and limits**.
4. **Assign the new COS values to the mailboxes** that require fax features. For outbound fax using the Fax Printer Driver application, configure mailbox Call Placement options.

This section supplies detailed instructions to perform these configuration tasks.

26.88.1 Configuring Fax Applications

These instructions assume that you have purchased and installed the Fax feature and familiarized yourself with the Fax Planning section. All Fax applications follow the same basic configuration. These instructions apply to the following applications:

- Fax Mail
- Walkaway Fax
- Fax Broadcast
- Guaranteed Fax
- Fax Publishing
- Outbound Fax

To configure Fax applications:

1. Complete the NuPoint Fax COS Planning Worksheet and the appropriate worksheet for your application:
2. Fax Mail Mailbox Worksheet
3. Fax Broadcast Worksheet
4. Guaranteed Fax Mailbox Worksheet
5. Fax Publishing Mailbox Worksheet
6. Define fax groups and assign them to the line groups that will be used for the fax application. You can use a shared fax group on an inbound line group to deposit faxes into the fax publishing system. You need a dedicated fax group for callers to retrieve faxes, either online or by entering a fax machine phone number.

Note:

- You should define the fax groups on the currently inactive configuration.
- If you are providing users with broadcast mailboxes for fax reception, you must customize one FCOS for fax users and another FCOS for the broadcast mailboxes. If you offer different levels of service to users, you might have to customize more than one FCOS.
- To enable users to download the Fax Printer from the Web View GUI, ensure that the FCOS does not include feature bit 303 (Disable Web View Downloads).

7. Based on your completed NuPoint Fax COS Planning Worksheet, customize an FCOS to include the following bits:

For Fax Mail:	For Walkaway Fax:	For Fax Broadcast	For Guaranteed Fax	For Fax Publishing	For Outbound Fax
190	190	122	198	194	110
191	203	190	206	195	193
192	256	198	207	197	195
193		203			290
194					
195					
196					
198					
199					
200					

For Fax Mail:	For Walkaway Fax:	For Fax Broadcast	For Guaranteed Fax	For Fax Publishing	For Outbound Fax
203					
230					
235					
236					
237					
239					
240					
256					
290					

8. Based on your completed NuPoint Fax COS Planning Worksheet, customize an LCOS with the following limits parameters:

For Fax Mail, Walkaway Fax, Broadcast Fax, and Fax Publishing:	For Guaranteed Fax and Outbound Fax:
Maximum number of digits allowable for fax phone number for fax delivery	Maximum number of fax messages per mailbox
Maximum number of fax messages per mailbox	CNG tone detection length (recommended value of zero)
CNG tone detection length (recommended value of zero)	Unplayed fax message retention

Fax delivery retry frequency	Urgent fax message retention
Fax delivery retry interval	
Played fax message retention	
Unplayed fax message retention	
Urgent fax message retention	
Fax receipt retention	

9. If you have NP Net installed on your server, customize an NCOS with the following limits parameters, based on your fax planning worksheet:

    - 10 (Make Fax Message to Network)
    - 11 (Give Fax Message to Network)
    - 12 (Answer Fax Message to Network)
10. Based on your completed Fax Mail Mailbox Worksheets, configure user mailboxes for Fax Mail. Mailboxes for Fax Publishing can be Tree, Chain, or Greeting Only.
11. (Optional) Set billing rates for NuPoint Fax.
12. Activate the configuration.
13. For each **Fax Broadcast** mailbox create distribution list 1 containing the recipients for faxes sent to that mailbox. Recipients can include local mailboxes, remote mailboxes on other NuPoint Unified Messaging servers connected by an NP Net network, or outdial telephone numbers.
14. To deposit the faxes into the **Fax Publishing** mailboxes, you must call the server from a fax machine. Log into each Fax Publishing mailbox as the mailbox owner (by pressing the star key before the mailbox number) and select the **8** key for user options, the **3** key for fax options, and then press the **5** key to leave a fax. When prompted, send the appropriate pages into the mailbox. Repeat for each mailbox in your Fax Publishing system. When a caller reaches one of the mailboxes, the server plays any recorded greeting in the mailbox and then tells the caller to get ready to receive the fax online or input a fax number to have the fax delivered.

26.88.2 Configuring Fax Applications

When NuPoint UM attempts to send a fax and encounters a busy line or a Ring-No-Answer (RNA) condition, it refers to the limits values set in the LCOS of the sending mailbox. You can configure the number of retries and the interval between retries. You can also limit the length of telephone number that can be faxed.

IMPORTANT!

- When faxes are sent using the **TUI**, settings must be configured in the **Fax Limits** menu.

- When faxes are sent using the **Fax Printer Driver** or Web View, settings must be configured in the **Call Placement limits** menu.

The TUI settings are set by default to try to send a fax once. If the fax fails, NuPoint UM will retry one more time after one minute has elapsed. If the retry fails, the system creates a fax receipt to notify you of the failure.

When using the Fax Printer Driver or Web View, the "RNA retry" default setting causes NuPoint to retry the fax 10 times at 60-minute intervals. (Note that in this case, a failure to send the fax will not provide a fax receipt for approximately 10 hours.) The "Busy retry" default setting causes NuPoint UM to retry up to 10 times at 10-minute intervals. The "Message Phone Length" parameter limits the length of the fax number you can dial. You can adjust these values as required.

To make the Fax Printer/Web View defaults the same as the TUI defaults (1 retry after 1 minute):

- Customize an LCOS to include the following **Call Placement limits**/settings:
  - RNA retry limit: 1
  - RNA retry interval: 1
  - Busy Retry limit: 1
  - RNA retry interval: 1

Note:

- If necessary, you can adjust the RNA and Busy retry limits if you want the fax to make more than one retry before failing.
- If the fax transmission itself fails (for example, fax machine error/power failure), NuPoint treats the fax attempt as a Ring No Answer.

26.88.3 Set Up a Fax Cover Page

You can have a different fax cover page for each line group by assigning a unique administrator's mailbox to each line group and storing a different cover page in each administrator's mailbox. This procedure assumes that you have already installed the NuPoint Fax feature and configured at least one Fax Application (see Configuring Fax Applications).

Note:

- If no personal or company fax cover page is configured, then the server does not auto-generate a default cover page.
- If feature bit 200 is not enabled in the FCOS for the faxing mailbox, the system will not send any cover page.

Cover Page Options

NP Fax provides three cover page options for faxes sent out from the server:

1. Each mailbox owner can have a **personal fax cover page**. This option allows a mailbox owner to fax their own cover page into their mailbox (via the User Options Menu). The system sends the personal cover page with any fax sent from the mailbox to a telephone number. Faxes retrieved online do not include a cover page.
2. The system can send a **company cover page**. If a cover page is put in the administrator's mailbox, it becomes the cover page for all faxes sent from that line group for all mailboxes that do not have a personal cover page. You can assign separate administrator's mailboxes, each with a different cover page, to each outbound line group with fax capability.
3. The mailbox owner can use a **TIFF file as a custom cover page**. The system uses the default cover page unless the user selects the custom cover page when composing a fax.

Setting Up a Company Fax Cover Page

To set up a company fax cover page:

1. Plan the layout of the cover page on 8.5 x 11 paper. Include the following information:
   - Company Name
   - Address
   - Telephone Number
   - Fax Number
2. Make sure that the administrator's mailbox has an FCOS with the bit 200 (fax cover page) enabled.
3. Dial into the system administrator's mailbox from a fax phone and reach the User Options Menu. Press the **3** key for Fax Delivery Options and then the **2** key for Fax Cover Page. When prompted, fax the cover page into the mailbox.

26.88.4 Viewing Fax Messages

Fax-viewing is supported in Standard UM and in the Web View using either a TIFF or PDF viewer. Which application is required depends on the Fax Download Setting.

To allow a user to view Fax messages with their Web View interface, you must assign feature bits 190 and 290 to the user's mailbox.

Note:

- A TIFF or PDF viewer is not delivered as part of the NuPoint Messaging software or Fax feature option. For TIFFs, users should use the MS Paint or Photo Viewer application included with their Windows operating system. For PDFs, users should download Adobe Acrobat Reader from the internet.
- The Apple QuickTime Player is not supported within the Web View interface for users to display faxes in TIFF format. Quick-Time should be configured not to play TIFFs on the user's PC. For this procedure, refer to the *NuPoint Unified Messaging Web View Help*.
- To print fax messages, feature bit 110 (Make/Give to Telephone Number) must be enabled in the user's mailbox.

26.88.5 Managing Fax Groups

Add a New Fax Group

To add a new fax group:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Fax Groups**. A list of defined fax groups is displayed.
4. Click **Add**.
5. In the **Number** field, enter a number (1-42) for this fax group.
6. In the **Module** list, select the number of the module (1-4) that you want included in this fax group.

Note:
Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0. For post-Release 6.0 platforms, there is only one module and it is automatically selected.

1. To add Channels to this group, click **Add** in the Fax Channels section. The Add Channels to Fax Group dialog box is displayed. **Note**: The Add button is enabled only when your system has sufficient licenses and fax channels available.
2. Select one or more channels from the **Available Channels** list and then click **Add**. **Note**: Number of selected channels cannot exceed quantity of available licenses.

To assign a fax group to an existing line group (optional):

1. In the Connection to Line Groups section, click **Add**. The Connect Fax group to Line Group dialog box is displayed.
2. In the **Line Groups** list, select a line group with which to associate this fax group, and then click **Add**. The selected line group is added to the Line Groups list.
3. Click **Save** to add the new fax group.
4. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

Edit a Fax Group

To edit an existing fax group:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Fax Groups**. A list of defined fax groups is displayed.
4. Select the fax group you want to edit and then click **Edit**.
5. Edit the fax group fields as required and then click **Save**. **Note**: Module number is editable only if there are no channels added.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

Delete a Fax Group

To delete a fax group:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Fax Groups**. A list of defined fax groups is displayed.
4. Select the group you want to delete by selecting its check box, and then click **Delete**. A confirmation message is displayed.
5. Click **Yes** to delete the selected fax group.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

Set Up General Fax Limits

To set up general fax limits:

- Refer to the Fax limits section of the LCOS Parameters and Defaults list.
- To set up fax limits when using the Fax Printer Driver or Web View refer to Configuring Ring No Answer and Busy Behavior.

Configure a Mailbox for Fax

To configure a mailbox for fax:

- Refer to the Edit Mailboxes procedure and to the Mailbox Parameters - Web Console list.

26.88.6 Define a Fax Group

Use this procedure to define a fax group with virtual fax channels. The number of channels you have is determined by licensing, up to a maximum of six channels. The numbering scheme of "slot:channel" is maintained for backward compatibility with older NuPoint Unified Messaging servers. For the purposes of defining a fax group, all fax channels reside in **slot 5** (5:0 to 5:5).

You can enable fax capabilities by assigning the fax group to up to 24 line groups. For incoming fax, associate the fax group with an incoming line group (like NuPoint Voice). For outgoing fax, associate the fax group with an outgoing line group (like Pager). See other topics in this section for procedures to associate fax groups with line groups.

To define a fax group:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, and then **(G) Offline Menu**.
2. From the Offline Menu, select **(G) Define Line Groups, Fax Groups**.
3. Select **(F) Define Fax Groups**. You can select menu options (S) and/or (U) to display information about existing fax groups.
4. Select **(G) Current Group=** and enter a **number** (1-24) for the fax group you are defining.
5. Select **(M) Module of Current Fax Group** and enter the **number** of the module (1-2) to include in the fax group.
6. Select **(A) Add Channels to Current Fax Group** and enter the slot number (always 5) and channel number (0-5) to add to the fax group, separated by a colon. For example:

Entry:	Specifies:
*	*All channels in the given module*
5:*	*All channels in slot 5*
5:0 - 5:2	Channels *0 to 2 in slot 5*
5:0, 5:2, 5:4	*Channels 0, 2, and 4 in slot 5.*

1. To drop channels from a fax group, select (D) Drop Channels from Current Fax Group and enter the channels to remove, using the same format described in step 6.

2. Repeat the procedure for each fax group you want to define. (If you have line groups that have cards in more than one module and you want to give those line groups fax capability, then you must define a fax group for each module.)
3. Exit from the Fax Group Menu. If you want to assign the new fax group to a Line Group now, exit back to the Line Groups menu and go to Assign Fax Group to Line Group.

26.88.7 Assign Fax Group to Line Group

To assign fax group to line groups:

1. If you are not already there, navigate to the Line Groups menu by selecting **(S) System Maintenance**,**(R) Reconfiguration**,**(R) Reconfigure System**, and then**(G) Offline Menu**.
2. From the Offline Menu, select **(G) Define Line Groups, Fax Groups**.
3. Select **(G) Current Group=** and enter a **number** (1-24) for the line group to which you want to assign a fax group.
4. Select **(C) Fax Group connections for current line group**. The system displays Line Group and Module (For example: Line group X, Module Y, where X is the line group that you selected in step 3, and Y is the first number of the first module that has voice ports in line group X.)
5. Enter the **fax group number** of the fax group to be connected with the lines of the current line group on the specified module. You can assign a fax group to more than one line group.
6. Repeat this procedure for each line group that you want to associate with fax groups.
7. Exit to the NuPoint Voice Configuration Offline Menu.
8. Activate the inactive configuration to make the changes take effect.
9. Assign the fax feature bits to the FCOS and LCOS that control the behavior of mailboxes that will be fax-enabled.

26.88.8 Set Limits for NuPoint Fax

To set up limits to govern the fax feature:

1. From the Main Menu, select **(S) System Maintenance**,**(R) Reconfiguration**, and then**(L) Limits COS**.
2. Select **(C) Choose Limits COS to Modify** and enter the number of the LCOS you want to modify.
3. Select **(N) Name Selected LCOS** and enter a descriptive name (1-15 characters) OR press Enter to accept the displayed name.

To set CNG Tone Detection Length for Walkaway Fax

1. Select **(P) Set NuPoint Fax Limits for Selected LCOS**.
2. Select **(C) Pre-greet Silence Interval to Improve Walkaway CNG Detection =**. This parameter should be 0 unless extremely noisy lines affect the CNG detection ability. Enter '.' to set the value to zero.

To set Fax Delivery Limits

1. Still in the NuPoint Fax Limits menu, select **(A) Maximum Number of Digits for Telephone Number** and enter the maximum number of digits (1-25) allowed in the fax phone number for fax delivery. Include access digits and area code requirements.

2. Select **(D) Fax Delivery Retry Frequency** and enter the number of retry attempts (0-255) the server will make to deliver a fax.
3. Select **(E) Fax Delivery Retry Interval** and enter the number of minutes between fax delivery retries.

To set Fax Storage Limits

1. Still in the NuPoint Fax Limits menu, select **(B) NuPoint Fax Message Count** and enter the maximum number of faxes (1-72) allowed or enter 0 to allow an unlimited number of faxes to be stored.
2. Exit to the Limits Class of Service menu and select **(D) Set Mailbox & Message Age Limits for selected LCOS**.
3. Select **(A) Played Fax Message Retention** and enter the number of hours (0-8760) a played fax message is kept if not deleted by the user.
4. Select **(B) Unplayed Fax Message Retention** and enter the number of hours (0-8760) an unplayed fax message is kept.
5. Select **(C) Urgent Fax Message Retention** and enter the number of hours (0-8760) an urgent fax message is kept.
6. Select **(D) Fax Receipt Retention** and enter the number of hours (0-8760) a fax receipt is kept if not deleted by the user.
7. Exit to System Configuration menu to save your changes.

26.88.9 Configure a Mailbox for NuPoint Fax

To configure a new or existing mailbox for Fax Mail, Fax Publishing, Guaranteed Fax, or Fax Broadcast:

1. From the Main Menu, select **(M) Mailbox maintenance**.
2. Select **(C) Create new mailboxes** OR **(M) Modify Mailboxes** and enter the number of the mailbox to create/modify. (When you select (M), the word "New" precedes each prompt in the following instructions.)
3. Press **Enter** until you see the **Features Class of Service** prompt. Assign a fax-customized FCOS by entering the number of the FCOS (1-640) that includes fax feature bits. Press **Enter**.
4. At the **Limits Class of Service** prompt, enter the number of the LCOS that includes the applicable fax limits.
5. If you have NP Net, at the **Network Class of Service** prompt, enter the number of the NCOS that includes the applicable fax limits.
6. At the **Restrictions Class of Service** prompt, and then enter the number of the RCOS that includes the applicable fax restrictions.
7. For Guaranteed Fax, you need to set up message delivery to the target fax machine. If this mailbox isn't used for Guaranteed Fax, skip to the next numbered step.
8. Press **Enter** until you see the **Message waiting type #1** and then enter **5** for Pager.
9. At the Pager Access Type prompt, enter the letter of the index to be used for delivery to a fax machine. Valid choices are:

    - **I** Internal outdial index
    - **B** Billed outdial index
    - **U** Non-billed outdial index
    - **N** Undefined index
10. At the **Pager number** prompt, enter the phone number of the target fax machine.

11. At the Post-pager number prompt, enter any overflow from the pager number that did not fit in the Page number field; OR leave blank.
12. Skip the **Pager frequency** and **interval** prompts as these items are controlled by LCOS settings.
13. At the **Message delivery** prompt, enter Y to activate.
14. Press **Enter** until you see the **Pager start time** prompt, and then enter the**time**at which fax delivery is to start. Enter the time in hours and minutes followed by “am” or “pm,” for example 6:00pm. To have fax delivery enabled for all times, set both Pager start time and Pager stop time to the same value, such as 12:00am.
15. At the **Pager stop time** prompt, Enter the **time** at which fax delivery is to stop.
16. Press **Enter** until you see the **Fax retrieval pager access type** prompt, and then enter the letter of the index (I, B, U, or N) to be used for fax retrieval, OR enter a pager system number from 0 to 15.
17. At the **Default telephone number for fax retrieval** prompt, enter the default **number** (1-16 characters) of the fax phone the fax message is to be delivered to. This field can contain any additional characters necessary for outdialing.
18. At the **Call placement pager access type prompt**, enter the letter of the index (I, B, U, or N) to be used for fax retrieval, OR enter a pager system number from 0 to 15. **Note**: This entry is required to send fax from the Web View interface.
19. At the **Time zone offset** prompt, enter the **number** of hours difference between the time zone of the mailbox owner and the local time zone of the NuPoint Unified Messaging server. Valid values are from -23 to +23. This number must match the offset of one of the time zones set in the Time Zone Configuration Menu.
20. Press **Enter** to skip through each of the remaining mailbox configuration prompts. After the last prompt, the system displays the mailbox configuration, then prompts for the next mailbox number.

At this point, the parameter settings are saved and you can continue with mailbox configuration or exit.

26.89 Introduction

The server keeps records of fax traffic, both at the system and mailbox level. Mailbox owners can be billed for faxes sent and received, either in terms of the number of faxes, or the total number of pages.

You can set NuPoint Fax billing rates for the following types of usage:

- Number of received fax messages
- Number of sent fax messages
- Retrieval of non-billed fax messages
- Retrieval of billed fax messages
- Undelivered fax messages
- Number of fax pages received
- Number of non-billed fax pages received
- Number of billed fax pages received
- Fax disk usage

These different usages can be combined in many ways to provide users with defined billing levels. This section describes each usage type. For instructions to produce billing reports, see Run a Billing Report. Fax statistics reports are also available to monitor the use of fax groups and fax storage.

NuPoint Unified Messaging servers offer two other methods of billing mailbox owners for fax usage:

- Fax transactions are recorded in Call Detail Recorder records, which can be downloaded to a computerized billing system for interpretation and billing.

  OR

- The server can place fax calls using mailbox owners' long distance carriers and calling card numbers. This can eliminate the need for any further billing, because there is no toll incurred by the server.

26.89.1 Billing Parameters

The Billing Menu, reached from the Reports Menu, identifies several categories of system usage that you can configure for billing. The categories of Messages Received and Disk Usage contain fax fields:

Messages Received

Messages Received contains fields both for faxes received and faxes sent. You can bill fax messages either on the number of messages or the number of pages. Additionally, you can bill retrieved fax messages in two categories: those for which the call was placed using the mailbox owner's calling card (billed messages), or those that were dialed without using a calling card (non-billed messages). You can also place a rate on undelivered fax messages, which incur storage space while on the system.

For each of the fax fields in Messages Received Billing, you can set two rates: one for instances below a certain boundary (for example, the first ten faxes received each billing period), and another for each instance above the boundary (all faxes received after the first ten). You can also set the boundary between low and high usage.

Fax Received Messages

This billing parameter allows you to bill mailbox owners based on the number of faxes that they receive during a billing period.

Fax Sent Messages

This billing parameter allows you to bill mailbox owners based on the number of faxes that they make or give during a billing period. If a mailbox owner sends/gives a fax to a distribution list, each member of the distribution list counts as one fax message sent.

Fax Retrieval Non-Billed Messages

This parameter bills mailbox owners for each successful outgoing fax call that the server makes using a non-billed access code. These calls may be local or long distance, depending on the configuration of access codes and the mailbox LCOS. Faxes that callers retrieve during a NuPoint Voice session are not counted in this billing parameter.

Fax Retrieval Billed Messages

This parameter bills mailbox owners for each successful outgoing fax call that the server makes using a billed access code. These fax calls are made using the mailbox owner's long-distance carrier and calling card, thus the server does not incur any toll charges for the calls. Faxes that callers retrieve during a NuPoint Voice session are not counted in this billing parameter.

Fax Undelivered Messages

You can use this billing parameter to charge for fax messages that are received into a mailbox, but never delivered to a fax machine. These messages are eventually purged from the system due to age.

Fax Pages Received Messages

This billing parameter allows you to charge mailbox owners based on the number of fax pages received, regardless of the total number of faxes. If you are trying to serve a lot of customers with few fax ports, it may work better to bill your customers for fax pages rather than total faxes (see “Fax Received Messages,” above), since a single fax that contains many pages can occupy a fax port for several minutes.

Fax Pages Sent Messages

This billing parameter allows you to charge mailbox owners based on the number of fax pages sent, regardless of the total number of faxes. If you are trying to serve a lot of customers with few fax ports, it may work better to bill your customers for fax pages rather than total faxes (see “Fax Sent Messages,” above), since a single fax that contains many pages can occupy a fax port for several minutes.

Fax Pages Retrieval Non-Billed Messages

This parameter bills mailbox owners for each page of successful outgoing fax calls that the server makes using a non-billed access code. These calls may be local or long distance, depending on the configuration of access codes and the mailbox LCOS. Faxes that callers retrieve during a NuPoint Voice session are not counted in this billing parameter.

Fax Pages Retrieval Billed Messages

This parameter bills mailbox owners for each page of successful outgoing fax calls that the server makes using a billed access code. These fax calls are made using the mailbox owner’s long-distance carrier and calling card, thus the server does not incur any toll charges for the calls. Faxes that callers retrieve during a NuPoint Voice session are not counted in this billing parameter.

Disk Usage

Disk Usage billing allows you to charge mailbox owners for the amount of storage used by their mailbox during a billing period. Fax messages, like voice messages, occupy space on the system’s hard disks. You can bill at different rates for voice messages and fax messages, if desired.

Fax Disk Use Rates

Simply stated, this billing parameter sets a cost for fax storage on the system’s hard disk. Storage used during a billing period is the result of the size of each message times the length of time that the mailbox owner has it in his or her mailbox.

Because the density (amount of information) of a fax page varies, fax disk usage is not measured in units of pages or total faxes. Instead, fax disk usage is measured in units of comparable voice storage. In other words, if a fax message stored on the system’s hard disk takes up as much space as a two-minute message, it would be billed the same as a two-minute message. If a mailbox owner kept that fax message for five days before discarding it, the total usage would equal ten minutes of storage.

The average double-spaced fax page (8.5" x 11") requires the same amount of storage as about 12 seconds of voice recording. A very dense fax page can use the equivalent storage space as 40 or more seconds of voice recording.

As with the Messages Received parameters, you can set a low usage rate, high usage rate, and boundary for Fax Disk Use. The boundary is in units of equivalent voice storage minutes.

26.89.2 Set Billing Rates for Fax

You can set billing rates for fax usage by number of messages received and/or by disk usage.

- Follow this procedure to set billing rates for Fax messages received.
- Follow this procedure to set billing rates for Fax disk usage.

26.89.3 Fax Statistics

The NuPoint Unified Messaging server can produce individual mailbox and system-wide statistics on fax usage.

Mailbox Statistics

The Mailbox Dump (from the Mailbox Maintenance menu of the **Text Console**) report for individual mailboxes contains many pieces of information relating to NuPoint Fax. In addition to identifying the mailbox configuration, including COS assigned to the mailbox, the report shows:

- Whether the mailbox has a fax cover page or greeting
- The number of fax messages and pages received
- The number of fax messages and pages sent
- The number of fax messages and pages delivered (downloaded) by the user to a fax machine
- The number of undelivered faxes
- The disk space used by faxes in the mailbox

System Statistics

The Mailbox Statistics report (reached from the Statistics Menu of the **Text Console**) contains information about the total amount of disk space used for fax storage. Within the Speech Statistics section of the Total Speech and Account Breakdown report are numbers for:

- The number of fax greetings and messages on the system, and the total number of frames and blocks that each occupies. The report also shows the percentage of storage blocks filled by each type of fax.
- A summary of the number of storage blocks used by both fax messages and greetings combined.

26.89.4 About the **Fax Group Usage Report**

This **Text console** report provides several pieces of information regarding fax group usage that you can use to monitor your system configuration. The reporting period can be any portion of the most recent seven days, and any hour or range of hours during those days. You can choose either a full report, which gives the statistics in 15-minute increments, or a summary report, which you can use to scan for possible problem areas.

Below is a sample Fax Group Usage Report followed by an explanation of how to read the report.

FAX GROUP USAGE 15min REPORT

Mon Jan 30, 20xx 7:50 am

01/30/XX 8hr --- minutes interval ---

Fax Group 1

DAY=01 HOUR=08 00-14 15-29 30-44 45-59 TOTAL BUSY

Transactions 1 8 22 21 52

Total Use 123 984 2706 2583 6396

No Resource Count 0 0 1 0 1

ATB Seconds 0 0 10 2 12 1 %

ATB Count 0 0 1 1 2

HIGHEST ATB_SEC: 10 sec at 8 hr

LOWEST ATB_SEC: 0 sec at 8 hr

Reading the Fax Group Usage Report

The report heading shows the date and time that the report was run.

The first line of the report shows the date and time interval during which the data was gathered.

- **Fax Group *n*** The following information concerns this fax group.
- **DAY=01 HOUR=08** The data displayed immediately below refers to traffic on day 1 (Monday) between the hours of 8:00 am and 9:00 am. 00-14 indicates that data in that column was gathered during the first fifteen minuets of the hour; 15-29 refers to the second 15 minutes of the hour, and so on.
- **Total** The combined data for the four 15-minute intervals. If this column contains a hyphen, it means that the data for that hour has not yet been gathered. For example, if the report is run at 3:30 p.m., and the report interval is for hours 12-15 (noon to 3 p.m.) the entries for the hour 15 (3 to 4 p.m.) show hyphens.
- **Transactions** The total number of fax receptions/transmissions that the fax group processed during the time period. Note that this does not reflect the number of fax pages nor the number of faxes; a single outgoing fax call (a transaction) could send several faxes from one mailbox.
- If a fax transaction spans two reporting periods, the Total Use fields show the time used in each period. The Transactions field counts the fax in the period in which the transaction started.
- **Total Use** The number of seconds that the channels in the fax group were involved in fax transactions during the time period.
- **No Resource Count** The number of times that all fax channels in the fax group were in use and another voice port requested a fax channel. This indicates that the fax group is too small to service all requests and some requests are being rejected.
- **ATB Seconds** The total number of seconds that all fax channels in the fax group were in use simultaneously.
- **Busy** The percentage of the hour that all fax channels were busy and the potential for request rejection existed.
- **ATB Count** The number of times that all fax channels in the fax group were in use simultaneously.

- **HIGHEST ATB_SEC:** This statistic identifies the busiest hour(s) for the fax group during the entire reporting period, and the number of seconds that all channels were busy during that hour.
- **LOWEST ATB_SEC:** This statistic identifies the hour(s) that had the least amount of time when all channels were busy.

Below is a sample Total Fax Group ATB Summary Report.

TOTAL FAX GROUP ATB SUMMARY REPORT

Mon Jan 30, 1995 4:24 pm

01/23/95 8hr-17hr day1-day5

GROUP TRANSACTIONS TOT SEC NO RES ATB CNT ATB SEC BUSY

----- ------------ ------- ------ ------- ------- ----

1 345 60030 1 2 12 1 %

The fields in the Fax Summary Report are identical to the fields in the Fax Group Usage Report. The data reported is the summary for the entire reporting period. You can use the report to monitor fax group usage, and to look for possible trouble spots. You can then decide whether you need to run the more detailed Fax Group Usage Report.

26.89.5 Run a Fax Group Usage Report

To run a Fax group usage report:

- Follow the instructions to Run a Line Group Usage Report, selecting a line group that has Fax groups

26.89.6 Run a Fax Group Usage Report

To enter the parameters for a fax group usage report (both standard and summary forms) and produce the report:

1. From the Main Menu, select **(R) Reports**, **(S) Statistics** and then **(F) Fax Group Usage**.
2. Select **(A) Beginning Group** and enter a**fax group number**between 1 and 24.
3. Select **(B) Ending Group** and enter a**fax group number**between 1 and 24. To report only one group, enter the same group number you entered in the Beginning Group field.
4. Select **(C) Beginning Hour** and enter the **number**, in military time, of the first hour of the time period for the report. The default is 8:00 a.m. (8). The range is 0 to 23 hours. 0 (zero) is midnight, 12 is noon, and 23 is 11:00 p.m.
5. Select **(D) Ending Hour** and enter the **number**, in military time, of the last hour of the time period for the report. Default is 5:00pm (17).
6. Select **(E) Beginning Day** and enter the **number** of the first day of the period for the report. (Sunday =0, Monday = 1, Tuesday = 2, etc.) Default is Monday (1)
7. Select **(F) Ending Day** and enter the **number** of the last day of the period for the report. The default is Friday (5).

8. Select **(G) Summary** and then enter **Y** to run a summary report or **N** to run a standard report with details at 15-minute intervals.
9. Select **(R) Run Report** and then select an output routing for the report:

   - **C** to send the report to the console without pausing (CTL + S to stop scrolling; CTL + Q to restart)
   - **P** to send the report to the console, pausing as the screen fills
   - **F** to send the report to a file on the server
   - **A** to append the report to an existing file on the server

26.89.7 Troubleshooting

This topic provides instructions for troubleshooting NuPoint Fax. If you are unable to resolve a problem after following the guidelines below, contact your distributor or technical support.

Configuration Problems

The majority of reported problems with NuPoint Fax are caused by configuration errors. Before testing for bad hardware, check the following areas of your NuPoint Voice configuration:

- Run a System Configuration Report and verify that each line group that is used for fax transactions has fax resources assigned to it.
- Run a Fax Group Usage Report and make sure that there is little or no blockage. If there are not enough fax resources (channels) assigned to a line group, fax calls may fail.
- Examine LCOS settings to make sure that limits are set appropriately for NuPoint Fax users. See the Fax Planning section for more information on LCOS settings.
- Examine FCOS settings to ensure that the correct features are enabled for NuPoint Fax application mailboxes and users. See the Fax Planning section for more information on FCOS settings.
- Check the configuration of any mailboxes that are reporting problems and make sure that they are assigned to classes of service that support NuPoint Fax.

Hardware Problems

If the NuPoint Voice configuration seems to be okay, the problem may be in the sending/receiving fax machine. Follow these guidelines to help isolate the problem.

- If users are reporting a problem with a specific fax machine, use a different fax machine and attempt to send and/or receive a fax using the mailbox that is having the problem.
- If you hear the prompt:

  Fax message complete

  or

  Your fax sent

the problem is probably with the receiving fax machine. Test the fax machine according to the manufacturer's instructions.

- If you hear the following prompt

  I'm sorry, I did not get your fax message

  or

  I'm sorry, I could not deliver your fax message

  - Check error logs for errors involving fax.
  - Examine fax LEDs for transmit/receive status.

Note:
Although Fax is a software-only feature, the numbering scheme of "slot:channel" is maintained for backward compatibility purposes. All fax channels reside in slot 5 (5:0 to 5:5).

Printing Problems

If users are unable to print fax messages, check to make sure that FCOS bit 110 - Make/Give to Telephone Number is enabled in their mailbox.

26.90 Description

NP Forms is an optional voice forms feature for NuPoint Voice systems that allows callers to leave messages in a way that simulates written information on paper forms. This feature requires installation of the Miscellaneous Options blade. Applications include:

- Order entry
- Questionnaires
- Routine requests for information
- Overflow for busy ACD (Automatic Call Distributor) groups.

Callers accessing an NP Forms application are automatically moved through a series of prerecorded questions. The system waits for the caller to record an answer before moving on to the next question. System users can then log into a single mailbox and listen to the sequence of answers.

A sample NP Forms session for ordering forms might go as follows:

NP Form:	*You have reached the city government forms service. Please answer the following questions to have forms mailed to you:* *Please state the name or the type of form.*
Caller:	I need the application for a small business license.
NP Form:	Please state your full name and spell your last name after the tone.
Caller:	Eric Meissner. M-E-I-S-S-N-E-R.
NP Form:	Please state your mailing address, including zip code, after the tone.
Caller:	4210 Monterey Road, San Francisco, California, 91010
NP Form:	Please state a phone number where you can be rea ched during business hours. Include the area code.
Caller:	Area code 415, 555-1234
NP Form:	Thank you for calling. Good-bye.

26.90.1 Inside an NP Forms Application

A typical NP Forms application uses three types of NuPoint Voice mailboxes:

- A rotational mailbox that plays an initial greeting and routes the call to one of several template mailboxes
- Template mailboxes with distribution lists that contain Greeting Only mailboxes and that collect the recorded answers to the questions
- Greeting Only mailboxes that contain the "questions" that callers will hear

The NP Form application mentioned above would have a structure similar to that shown here:

Note that the figure above is simplified to show only a single Template mailbox. In actual operation, an NP Forms application needs enough Template mailboxes to hold all caller responses (see NP Forms Limitations).

Distribution list 01 in the Rotational mailbox must contain all of the Template mailboxes. The first Template mailbox must have a distribution list 01 that contains the Greeting Only mailboxes for the MESA Form. The Rotational mailbox will pass control of each call to the first Template mailbox until that mailbox is full. It then

passes calls to the second template mailbox, and so forth. Figure 1-2 shows this aspect of the sample NP Forms application.

Distribution list 01 in the Rotational mailbox must contain all of the Template mailboxes. The first Template mailbox must have a distribution list 01 that contains the Greeting Only mailboxes for the NP Form. The Rotational mailbox will pass control of each call to the first Template mailbox until that mailbox is full. It then passes calls to the second template mailbox, and so forth. The figure below shows this aspect of the sample NP Forms application.

26.90.2 Playback and Transcription

The Rotational mailbox serves as a single point of entry for retrieving all caller responses stored in any of the Template mailboxes. A transcriber can listen to caller responses by logging in to the NP Forms Rotational mailbox, which retrieves the stored responses from *all* Template mailboxes in its distribution list 01.

After login, the system prompts the transcriber to select either Unplayed or Saved messages. The number of messages reflects the number of callers that responded to any of the questions. When playing back the messages, the system separates responses to each question with a “bloop” sound. Transcribers can save and replay the messages, and can pause, skip forward, and skip backward during playback.

The system plays back responses in chronological order. Thus, it plays back all responses stored in the first Template mailbox before playing the responses from other Template mailboxes. More than one person can call into the Rotational mailbox at the same time to transcribe messages.

NP Forms is compatible with the autoplay feature (FCOS bit 52). With this feature enabled, a transcriber can listen to all responses without having to press the P key on the telephone to advance through the messages. (Transcribers must still press K or D to keep or discard the messages.)

Note:
To retrieve NP Forms messages, a transcriber calls the Rotational mailbox, *not* the template mailboxes.

26.90.3 NP Forms Mailbox Interaction

The numbered steps below illustrate the sequence and interaction of the mailboxes in an NP Forms call:

1. A caller dials a DID number or extension number that corresponds to the Rotational mailbox
2. The system plays the greeting/instructions recorded in the Rotational mailbox.
3. The Rotational mailbox transfers control of the call to one of the Template mailboxes.
4. The system plays the greeting in the first Greeting Only mailbox defined in distribution list 01 of the Template mailbox.
5. The system records the caller’s response.
6. The system repeats steps 4 and 5 for each Greeting Only mailbox in distribution list 01 of the Template mailbox.

7. After recording the last caller response, the system plays a standard good-bye message or presents the caller with further options, depending on the FCOS settings of the Template mailbox.
8. At the end of the call, the system deposits all of the responses into the Template mailbox as a single message.

26.90.4 Tree Mailboxes and NP Forms

Tree mailboxes allow callers to press DTMF keys to choose from several options, and can be used either before or after an NP Forms application.

When a Tree mailbox precedes an NP Forms Rotational mailbox, callers can select alternatives to filling out the NP Form, such as transferring to a live attendant or leaving a message in another mailbox. By setting the Rotational mailbox as the first mailbox in distribution list 01 and including feature bit 120 (Default to First Child of Tree Mailbox) in the Tree mailbox FCOS, callers with rotary dial phones are automatically transferred to the NP Form where they are prompted with the first question.

If the last mailbox in distribution list 01 of the Template mailbox is a Tree mailbox, callers can select additional options after completing an NP Form. (The Template mailbox must contains FCOS bit 139.) The Template mailbox plays the greeting of the Tree mailbox, then allows callers to select from the choices listed in the greeting. This way callers can return to a "higher menu" or hold/transfer for live assistance. Again, if the FCOS for the Tree mailbox contains bit 120, callers with rotary phones can be automatically transferred to a specific extension or mailbox.

26.90.5 NP Forms FCOS Configuration

The NuPoint Voice software includes a pre-defined FCOS for use with NP Forms, and pre-defined FCOS for Rotational and Tree mailboxes. There are also several individual FCOS bits that allow some flexibility in configuring NP Forms.

NP Forms Default FCOS

- Default **FCOS 16** contains all of the feature bits necessary for a **Template** mailbox. Optionally, you can add bit **139** to allow callers to access other options after completing an NP Form.
- Default **FCOS 17** is predefined for a standard **Rotational** mailbox. Add feature bit **149** for Rotational mailboxes that are used in NP Forms.
- Default **FCOS 06** contains all of the feature bits necessary for the **Greeting Only** mailboxes that play the questions to NP Forms callers.
- Default **FCOS 15** is predefined to support **Tree** mailboxes. As an option, you can add feature bit **120** so that callers with rotary phones are automatically moved to the first Template (child) mailbox.

NP Forms FCOS Bits

The FCOS bits that are useful in NP Forms applications are:

- **135 Defines template mailbox -** A mailbox with this feature plays the greetings stored in its child mailboxes, sequentially, and records a response after each greeting.
- **136 Don’t say "End of Message" -**When set to On for a Template mailbox, the system does not say "End of message" after each message is played or recorded.
- **138 Don’t say "Message complete" -** When set to On for a Template mailbox, the system does not say "Recording complete" after each message is recorded.

- **139 Template: assume last greet mailbox FCOS -**When set to On for a Template mailbox, the Template mailbox assumes the FCOS values of the last mailbox in distribution list 01 after playing the greeting, and call flow is altered accordingly. For example, if the last mailbox is a tree or chain mailbox, the caller can continue to interact with the system after completing the NP Form.
- When bit 139 is set to Off for a Template mailbox, callers always hear, "Thank you for calling, good-bye," after completing the NP Form.
- **149 Log into template through rotational mailbox -** When set to On for a Rotational mailbox, a transcriber can call into the Rotational mailbox and automatically pick up the messages from all Template (child) mailboxes.

NP Forms Limitations

An NP Forms application can generate a lot of responses from callers, and these responses must be transcribed and taken off of the system or they will fill up the available voice storage. The NP Forms application has some built-in limits to reduce the chances of this happening.

- Each NP Forms application can have a maximum of 190 Template mailboxes.
- There can be no more than 200 questions (Greeting Only mailboxes) in distribution list 01 of the first Template mailbox. The other Template mailboxes in the NP Form do not need a copy of the distribution list; the system uses the distribution list in the first Template mailbox.
- Each Template mailbox can store a maximum of 200 responses. Since most NP Forms consist of several questions, each caller leaves several responses. If an NP Form has four questions, a single Template mailbox can store responses from 50 callers (200 = 4*50).
- NP Forms Rotational mailboxes automatically rotate on full. You cannot assign the Index or Period type of rotation.
- The system deposits caller responses in the first Template mailbox until it is full, then it rotates to the second Template mailbox, and so on. It cycles through all of the Template mailboxes before again putting responses in the first Template mailbox.

If all Template mailboxes in an NP Forms application are full, callers hear, "I'm sorry, I cannot deliver your message now. Please try again later."

26.90.6 Configure an NP Forms Template Mailbox

This procedure describes how to configure an NP Forms Template mailbox and the Greeting Only mailboxes that will contain the questions for the NP Form.

1. Complete a Rotational Mailbox Diagram for each Rotational Mailbox, and a Mailbox Worksheet for all Template and Greeting Only mailboxes.
2. Create or modify the required template mailboxes and apply default **FCOS 16** for **Template** mailboxes.
3. Create or modify the Greeting Only mailbox that will play the first question to callers and apply default **FCOS 6** for Greeting-only mailboxes.
4. Configure all remaining child mailboxes in the same manner.

To create Distribution List 01 for the Template mailbox:

1. Create distribution list 01 with the following parameters:

   - Mailbox number of the Template mailbox
   - Distribution List Number 01
   - Sorted list
   - Add as members the mailbox numbers of all Greeting Only mailboxes

26.90.7 Create an NP Forms Application

26.90.8 Configure a Rotational Mailbox for NP Forms

This procedure describes how to configure a rotational mailbox for use with NP Forms, including setting index-type rotation and adding the template mailboxes to distribution list 01.

1. Complete a Rotational Mailbox Diagram , and a Mailbox Worksheet for each mailbox.
2. From the Main menu, select **(M) Mailbox maintenance**.
3. Create the mailbox by selecting **(C) Create new mailboxes** or **(M) Modify mailboxes** and enter the **number** of the mailbox to create/modify. To leave a parameter unchanged, press Enter to move to the next prompt.
4. Set all applicable parameters the same as for Create a Standard Mailbox, except for the Features Class of Service parameter, where you will enter the default FCOS 17, or the number of a customized FCOS that includes all the applicable bits for a Rotational mailbox.
5. After responding to the last mailbox parameter, the system displays the mailbox configuration, then prompts for the next mailbox number to modify or create. At this point, the parameter settings for the template mailbox are saved. Press**Enter**at the Mailbox to create? prompt to return to the Mailbox maintenance menu.

To create Distribution List 01 for the Template mailbox:

1. Select **(L) List Maintenance** and then **(C) Create, Modify, or Show Distribution Lists**.
2. At the **Mailbox:** prompt, enter the number of the Rotational mailbox from step 3.
3. At the **Distribution List** prompt, enter **01**.
4. At the **(S)orted or (U)nsorted list?** prompt, enter **S**.
5. If you want, you can check the list to make sure the member is not already on it by entering **Y** to the **Check for duplicate before add (y/n)?**prompt.
6. At the **(A)dd, (D)elete,or (S)how list ?** prompt, enter **A** to add a member.
7. At the **Member**: prompt, add the mailbox **numbers** of the Template mailboxes in one of the following formats:

   - A single mailbox number, for example 3788
   - A continuous range of mailbox numbers, for example 3001-3788
   - A series of mailbox numbers, for example 3781,3782,3786,3788
   - You can mix formats of mailbox number entries, so you can specify all the mailbox numbers necessary in one attempt. For example, this entry is valid: 208,222-308,333,334,661
8. The system confirms each addition. When finished, press Enter at the **(A)dd** prompt.

9. At the **Save Changes to Distribution List?** prompt, press **Y**. The system reports the current members, reflecting members just added or deleted, and your changes are saved.

26.90.9 Worksheet Index

- FCOS Worksheet
- Mailbox Individual Worksheet
- NP Forms Diagram
- Rotational Mailbox Diagram
- Tree Mailbox Diagram

26.90.10 FCOS Worksheet

FCOS Worksheet

Features Class of Service Menu

FCOS

FCOS to modify

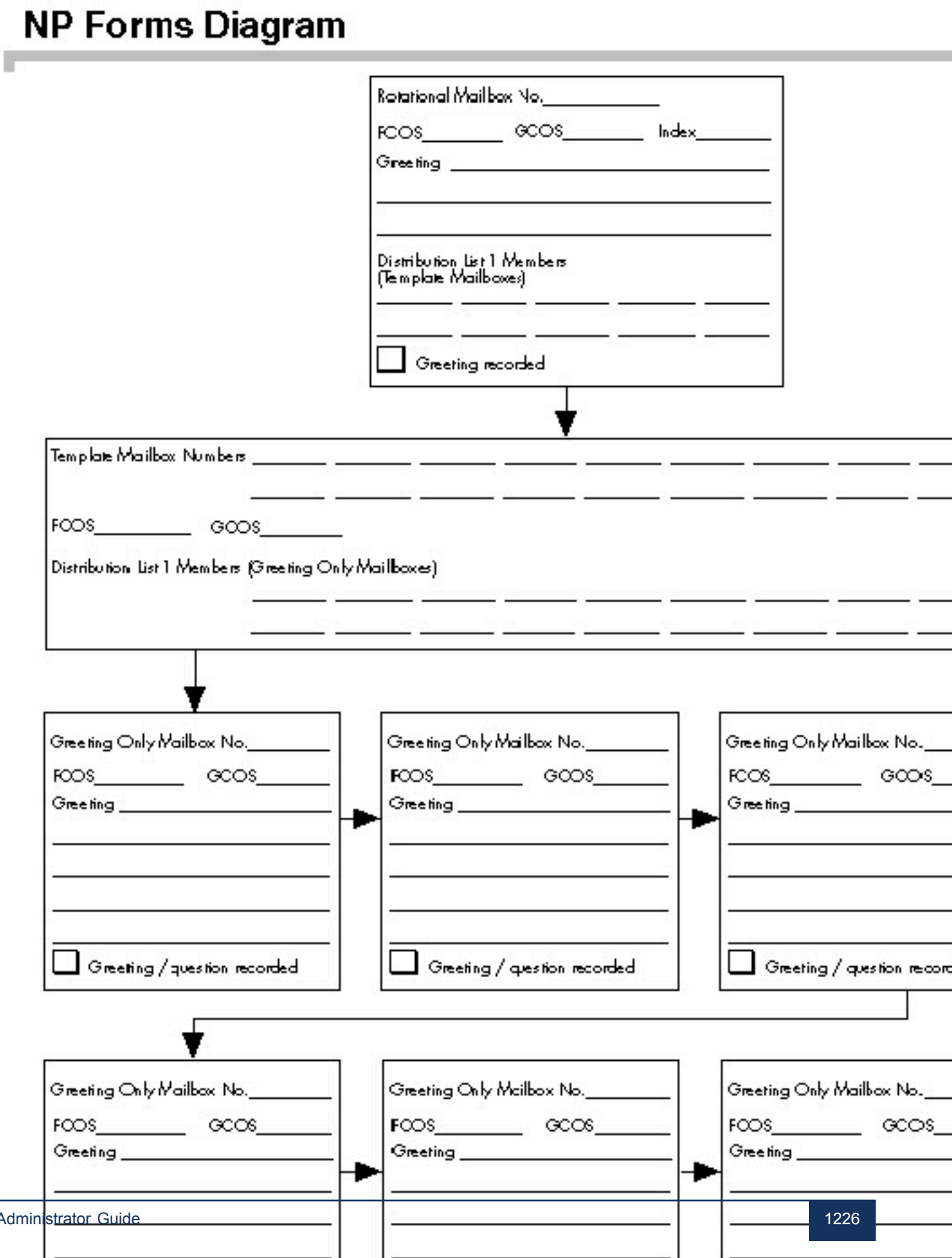
FCOS name

FCOS to copy

FCOS Features

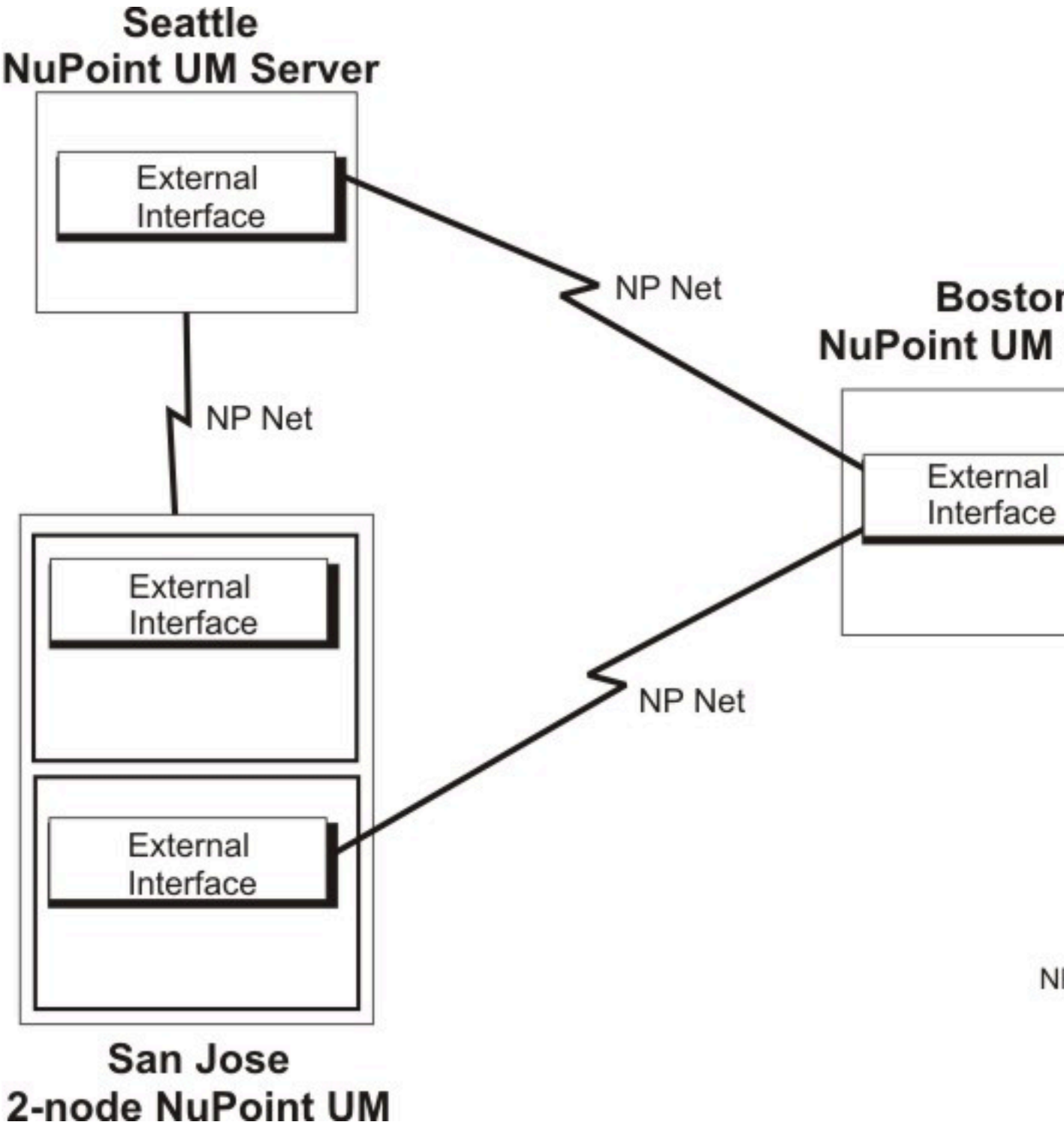
1 Greeting	060 062 063 064 065 161 162 224
2 Login	001 016 066 069 081 101 102 103 104 105 106 107 108 109 132 151 152 156 165 218 219 225
3 Logout	003 009 170 220
4 Attendant Call	002 098
5 Outside Caller	004 002 005 017 041 051 092 098 111 112 113 114 115 116 117 118 119 137 176 203 221
6 Prompts	051 082 083 097 098 098 131 133 136 138 140 146 157 159 176 202 208 Language (1) 010 011 012 013 014 099 150 233 Interface (1) 209 210
7 Receive Msgs	039 040 041 042 043 044 045 046 047 088 111 112 113 114 115 116 117 118 119 127 173 175 179 185 190 198 199 223
8 Play Msgs	060 006 007 039 046 047 048 049 052 057 058 059 075 076 089 144 145 147 153 204 215 216
9 Answer Msgs	029 019 030 031 038 147 158
10 Keep/Discard Msgs	053 054 055 056 145
11 Make Msgs	020 021 022 023 032 034 061 087 092 096 110 126 157 158 171 172 188 191
12 Give Msgs	024 086 018 025 026 027 028 033 035 061 084 085 110 126 157 158 192
13 Msg Address.	018 019 021 023 025 027 030 031 087 095
14 User Options	070 015 071 072 073 074 077 078 093 094 095 124 125 127 130 142 143 148 180 195 196 201
15 User Dist. Lists	032 033 036 044 074 134 222
16 Master Dist. Lists	034 035
17 Check In/ Out	008 090 091
18 Super User	021 122 068 120 123 141 147 152 174 178 186 187 189 229 234
19 Msg Wait Ind.	079 080 134 182 183 205 228 234
20 NuPoint Fax	090 191 192 193 194 195 196 197 198 199 200 203 206 207 230
21 Paging	077 124 168 169 171 172 173 181 188 208 209 210 211 212 213 219
22 E-mail	054 170 184 205 217 220 221 224 225
23 Network/ NP Forms	135 139 149

26.90.11 NP Forms Diagram



26.91 Introduction

NP Net is an optional networking feature for NuPoint Unified Messaging servers. It allows you to connect NuPoint UM systems together to form a digital network. With NP Net, mailbox owners can make voice messages for mailboxes on remote servers in the same manner as they make messages to local mailboxes. For example, a user can log into a NuPoint UM Voice mailbox, make a message for several recipients, some local and some remote, and send that message. Users can also answer messages and forward (give) messages to users on remote nodes. The figure below shows a simple NP Net network.



NP Net transmits messages in digital form, as opposed to actually playing messages over the phone lines to remote systems. Digital transmission increases throughput.

NP Net provides the user with **NP Net TCP/IP** networking. NP Net TCP/IP supports TCP/IP over Ethernet.

The building blocks of an NP Net network are the servers. Each server functions as a **node** on the network. NP Net is scalable so that it can work on all NuPoint UM server models, providing lower-cost, lower throughput networking on smaller servers and higher throughput messaging on larger servers.

26.91.1 Configuration Task List

The configuration steps for NP Net involve the following tasks:

1. Configure TCP/IP to define node characteristics.

The following configuration must be done from the **Text console**:

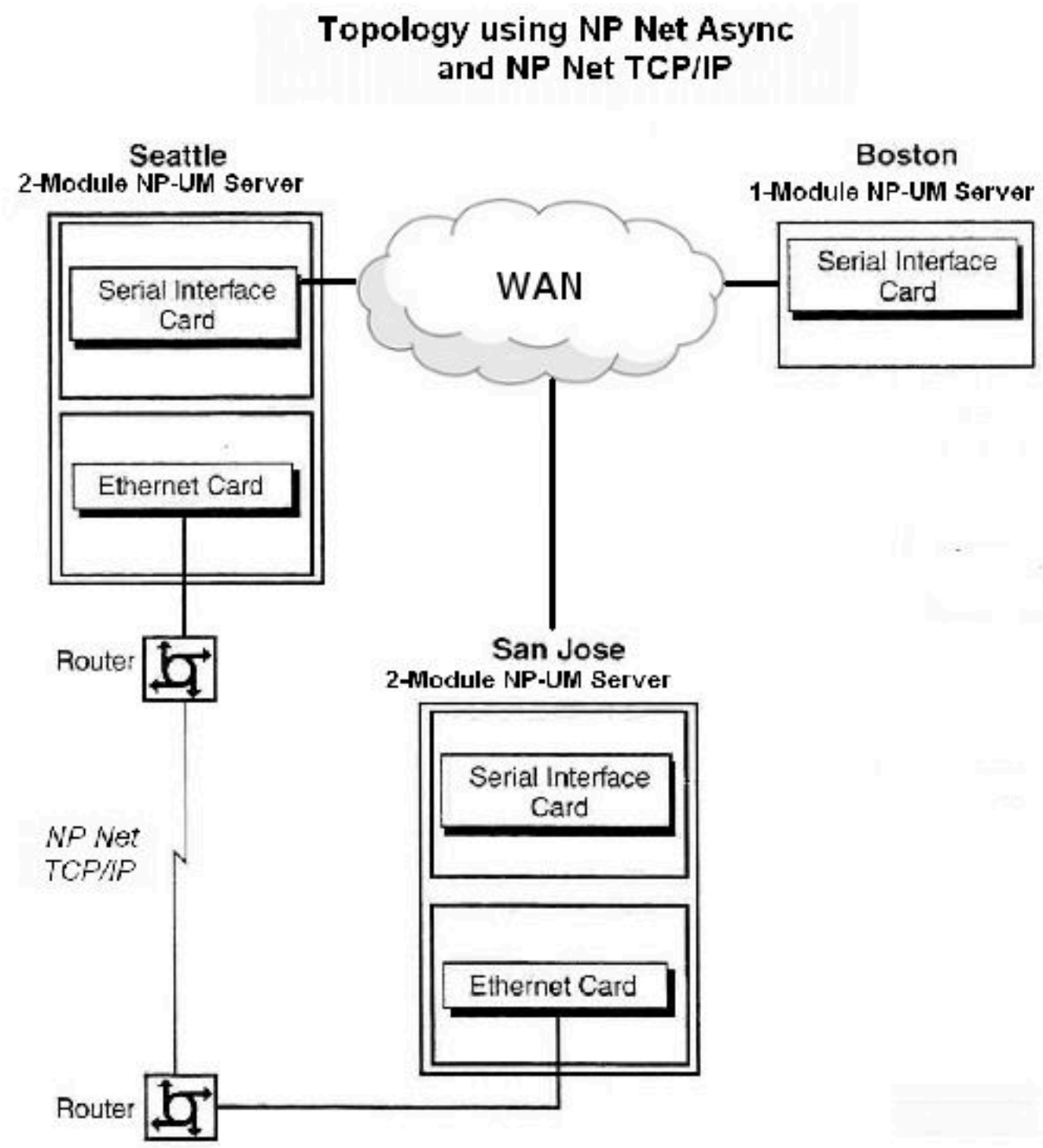
1. Configure the Network Node Table to identify the protocol and 'address' of each node on the network.
2. Modify the Dial Plan to allow network addressing.
3. Program the Digits Translation Table to determine the correct node and mailbox number.
4. Configure Network Queuing to control thresholds for sending messages.
5. Define a Network Class of Service to provide network privileges for users.
6. Apply the Network Class of Service to user mailboxes.

26.91.2 NP Net TCP/IP Overview

NP Net TCP/IP connects the servers together using Ethernet. NP Net TCP/IP can use an existing private network, or it can send messages over a public network. The high bandwidth of Ethernet connections allows for a large volume of network traffic, providing users with network service that is almost indistinguishable from local messaging.

In order to use NP Net TCP/IP, a server also must have the **Unified TCP/IP Interface** optional feature installed. This optional feature provides a single point of configuration for all TCP/IP applications on these servers.

NP Net TCP/IP Topology



26.91.3 NP Net - Terms and Concepts

These concepts are discussed in more detail in later sections.

Network Dialing Plan

The NuPoint Voice dialing plan has characters to support network mailboxes. If an **N** or **P** precedes a number in a dialing plan position, it means that all mailboxes represented by that position are network mailboxes and will be processed by the NP Net software. See Configuring Network Addressing for more information about the network dialing plan.

Digits Translation Table

The Digits Translation Table determines which messages go to which node. All network messages are compared to this table before being sent to the appropriate node. See Configuring the Network Node Table for more information about the digits translation table.

Network Queues

Network messages are stored in local network queues until they are transmitted to remote nodes. Separate queues are kept for urgent and batch (non-urgent) messages to each remote node. Messages are queued until a message threshold is reached and a message delivery time window is open. The local node then initiates a connection with the appropriate remote node. See Configuring the Network Queues for more information about network queues.

Network Node Table

To initiate a connection to a remote node, the local NP Net node must have all of the following information:

- the node number of the remote node
- the string that must be outdialed to reach that particular node, or the IP address of the node
- whether access to the remote node is enabled or disabled

As described previously, NP Net uses the Digits Translation Table to find the node number of the destination node. The Network Node Table matches the node number of each remote node with its corresponding hardware type, outdial string (access code), and access status. See Configuring the Network Node Table for more information on the Network Node Table.

Network Class of Service

Network Classes of Service (NCOS) are used to control user privileges such as making or answering messages across the network. See Configuring the Network Class of Service for more information on Network Class of Service.

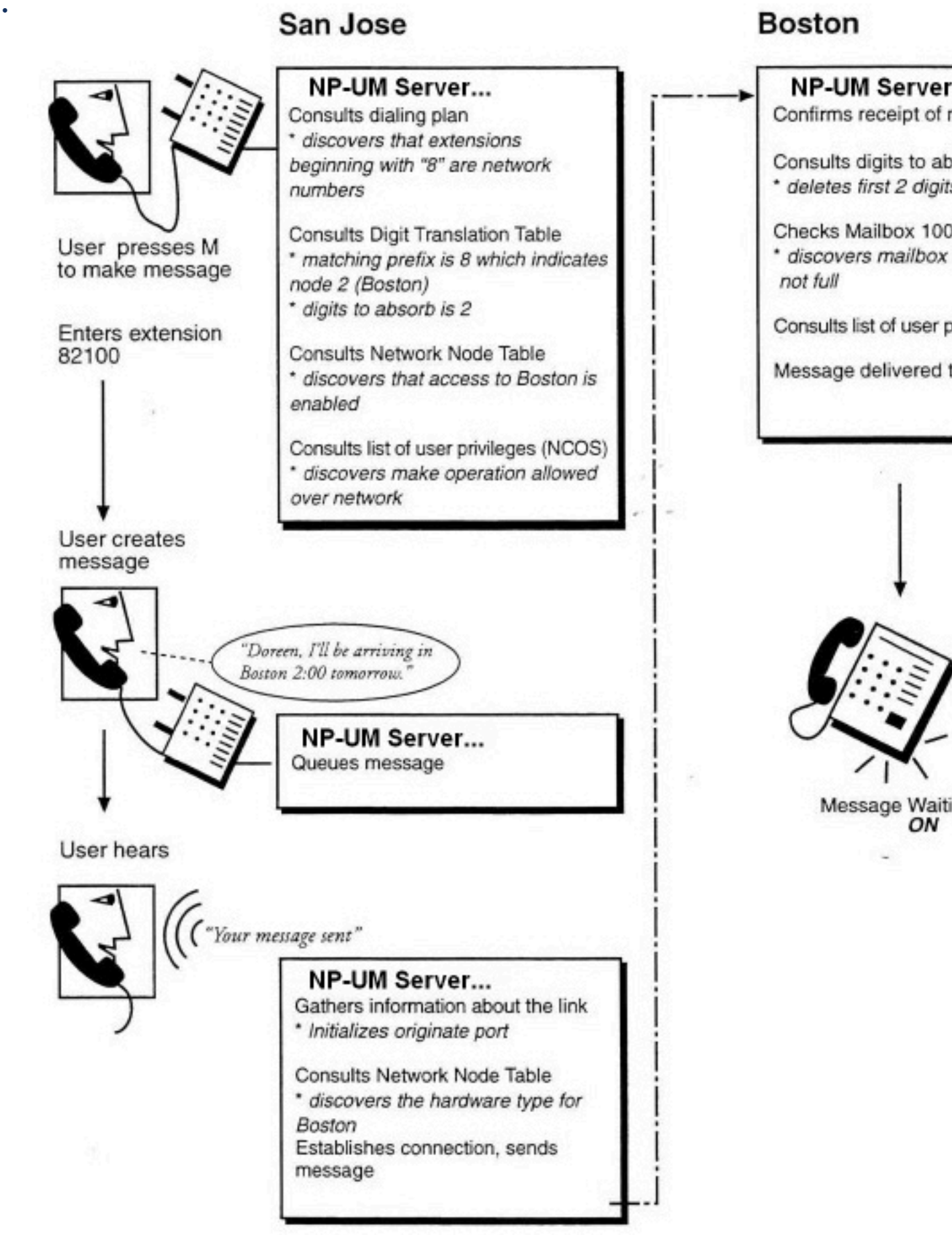
26.91.4 Message Flow Through an NP Net Network

This section describes how a voice message flows through the NP Net network. From the sender's point of view, if Name Broadcast mailboxes are used, there is no difference between sending a message to a local mailbox and sending one to a remote mailbox. (Name Broadcast mailboxes provide name confirmation across the network.) When a user receives a message from a remote mailbox, he or she hears "Remote message from [name]" where [name] is the name of the remote mailbox owner.

The diagram below is an overview of a message traveling from one node to another (San Jose to Boston). In this example, the dialing plan is configured such that mailbox numbers beginning with 8 are network numbers and that node 2 is Boston. In the discussion of the various NP Net functions in the following sections, the inner workings of the network are discussed in more detail.

The following paragraphs explain some of the processing shown in the diagram in more detail.

1. The user addresses a message to a destination mailbox, records it, and presses X to send the message, just as if it were being sent to a mailbox on the same system.
2. The NuPoint Voice software compares the leading digit of the destination mailbox with the dialing plan, where it finds an N or a P, indicating that the destination is a network mailbox.
3. The NuPoint Voice software then checks the Network Classes of Service (NCOS) assigned to the sender's mailbox to see if the operation is permitted.
4. The leading digits of the mailbox number are compared with the prefixes stored in the Digits Translation Table, where the number of the destination node is found.
5. The NuPoint Voice software checks the Network Node Table to be sure that the destination node is listed, and that access is enabled.
6. The message is put into the message queue that is waiting to be sent to that node.
7. The NP Net software checks the queue every thirty seconds to see if one of the queue thresholds has been reached, at which point it checks the Network Node Table for the hardware type, which provides the call setup instruction.
8. The connection is made, and messages are sent to the destination (remote) node.
9. The remote node uses the "digits to absorb" value to convert the mailbox number in the message header to a valid local mailbox by deleting the specified number of leading digits.
10. The remote node checks the size of the message to be sure that it does not exceed the node's network message limit. The remote node also checks the message size against the available space in the user's mailbox.
11. The remote node compares the Group Class of Service (GCOS) of the sending and receiving mailboxes, if the sender's Network Class of Service contains a feature that dictates this check. If the Gross match, or if they have even one group in common, the message is sent to the appropriate mailbox.
12. The receiving node converts the message timestamp (the message creation time) to local time and announces the converted time when the recipient plays the message. A receipt, which says that the recipient has not played the message, is sent back to the sender. If the sender keeps the receipt, NP Net will issue a receipt update during the first communications session established between the nodes after the recipient has played the message. The receipt update announces the time that the message was played, converted to the sender's local time.
13. If the recipient decides to answer the message, or if there is a receipt, the node number and sender’s mailbox number attached to the original message identify the destination mailbox on the originating node for return messages. Answers and receipts are not processed through the Digits Translation Table.


San Jose
Boston
NP-UM Server...
Consults dialing plan
* discovers that extensions beginning with "8" are network numbers
Consults Digit Translation Table
* matching prefix is 8 which indicates node 2 (Boston)
* digits to absorb is 2
Consults Network Node Table
* discovers that access to Boston is enabled
Consults list of user privileges (NCOS)
* discovers make operation allowed over network
NP-UM Server
Confirms receipt of
Consults digits to ab
* deletes first 2 digit
Checks Mailbox 100
* discovers mailbox not full
Consults list of user p
Message delivered
User presses M to make message
Enters extension 82100
User creates message
"Doreen, I'll be arriving in Boston 2:00 tomorrow."
NP-UM Server...
Queues message
Message Waiti
ON
User hears
"Your message sent"
NP-UM Server...
Gathers information about the link
* Initializes originate port
Consults Network Node Table
* discovers the hardware type for Boston
Establishes connection, sends message

26.91.5 Overview of NP Net Installation and Configuration Tasks

The table below shows the tasks required to install and configure NP Net TCP/IP. Use this table as a road map to guide you during installation and configuration.

For this task...	Reference information is here:
Install the NPUM Voicemail Networking software blade to enable NP NetTCP/IP	Installing an Optional Feature
Configure NP Net TCP/IP	About NP Net TCP/IP
Configure the Network Node Table	Configuring the Network Node Table
Configure the dialing plan	Creating a Network Dialing Plan
Configure the Digits Translation Table	The Digits Translation Table
Configure the network queues	Configure Network Queues
Configure the network class of service	Configuring the Network Class of Service
Enable network messaging for user mailboxes	Configuring Network Mailboxes

26.92 About NP Net TCP/IP

This section explains NP Net TCP/IP concepts and describes how to configure NP Net TCP/IP.

NP Net TCP/IP connects these servers together using TCP/IP over Ethernet or an appropriate wide-area network. NP Net TCP/IP can use an existing private network, or it can send messages over a public network. The high bandwidth of Ethernet connections allows for a large volume of network traffic.

NP Net TCP/IP requires an Ethernet card and the NPUM Voicemail Networking software blade. If you have not already done so, install the hardware and software. The rest of the information in this section assumes that you have completed those prerequisite steps.

NP Net TCP/IP Configuration

NP Net TCP/IP uses certain information that is configured in the TCP/IP Interface optional feature. You must be familiar with this information and you must have configured the TCP/IP interface before starting to configure NP Net TCP/IP. This information is:

- Module Number and Slot Number where the Ethernet card is installed
- The Operation Mode of the card, either primary or secondary
- Whether the card is enabled or disable the Ethernet Card
- Ethernet Card Configuration (either Ethernet 1 or Ethernet 3)
- Domain Name
- Node Name
- Node IP Address
- Subnet Mask
- Physical Network Number
- Broadcast Address

- Gateway IP Address

When you configure NP Net TCP/IP, as described in the Procedures section of this section, you define the following parameters:

- The **module number** that contains the Ethernet card to use for NP Net TCP/IP, and the number of the Ethernet card in that module. You can only configure NP Net TCP/IP on one module of a multi-module server.
- The **System Node Name**, which is used by NP Net in reports.
- The **System Local Node Number**, which is used by NP Net to do message routing (see Configuring the Network Node Table for information on configuring the Network Node Table).
- System **Network Message Limit** in number of minutes
- The number of **Send and Receive Circuits** (virtual circuits) to be used by NP Net. The number of circuits determines the throughput. You can configure a node with more of one type of circuit than the other, if needed.

26.92.1 Configuring TCP/IP

Before you begin, ensure that the NPUM Voicemail Networking software blade is installed.

To Configure NP Net TCP/IP

To configure NP Net TCP/IP parameters:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **NP Net TCP/IP**. The NP Net TCP/IP configuration screen displays.
4. Configure the following parameters:

Parameter	Description	Value
Host Number to Configure	Select the module number on which to configure NP Net TCP/IP.	1 - 4
Ethernet Card Configuration	Enter the number of an enabled Ethernet card in the module.	1 - 2
System Node Name	Enter the name of the node being used for TCP/IP	Max. 15 characters
System Network Message Limit	Enter the maximum number of minutes for a network message.	1 - 99

Parameter	Description	Value
Receive Circuits	Enter the number of receive circuits to be used by NP Net.	2 - 9
Send Circuits	Enter the number of send circuits to be used by NP Net.	2 - 9
System Local Node Number	Enter the number of the local node.	1 - 8191

5. Click **Save**.
6. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.92.2 Configuring TCP/IP

Before you begin, ensure that the NPUM Voicemail Networking software blade is installed.

Configure NP Net TCP/IP

This procedure describes how to configure the low-level NP Net TCP/IP parameters.

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, **(G) Offline Menu** and then **(N) NP Net TCP/IP Menu**.
2. Select **(H) Host Number to configure** and enter the **module number** on which to configure NP Net TCP/IP. The module must contain an Ethernet card.
3. Select **(I) Ethernet Card Configuration** and enter the **number** (1-2) of an enabled Ethernet card in the module. You can only configure NP Net TCP/IP on one module of a multi-module NP-UM system.
4. Select **(N) System Node Name** and enter the **name** (1-15 characters) of the node.
5. Select **(M) System Network message limit**and set the maximum**number of minutes**(1-99) for a network message. The local node will reject messages that exceed this limit.
6. Select **(R) Receive Circuits** and enter the **number** (2-9) of receive circuits to be used by NP Net. The number of circuits determines the throughput.
7. Select **(S) Send Circuits** and enter the **number** (2-9) of send circuits to be used by NP Net. You can configure a node with more of one type of circuit than the other, if needed.
8. Select **(T) System Local Node Number** and enter the **number** (1 - 8191) of the local node used by NP Net for message routing.

   - Note: The default system local node number is 1. Assign a different number (2, 3, etc.) to reduce the chance of conflicts with other systems.
9. Exit to the NuPoint Voice Configuration Main Menu to save your changes.
10. When you configure NP Net TCP/IP for the first time, you must **reboot** before you activate the configuration.

26.93 Network Node Table - Introduction

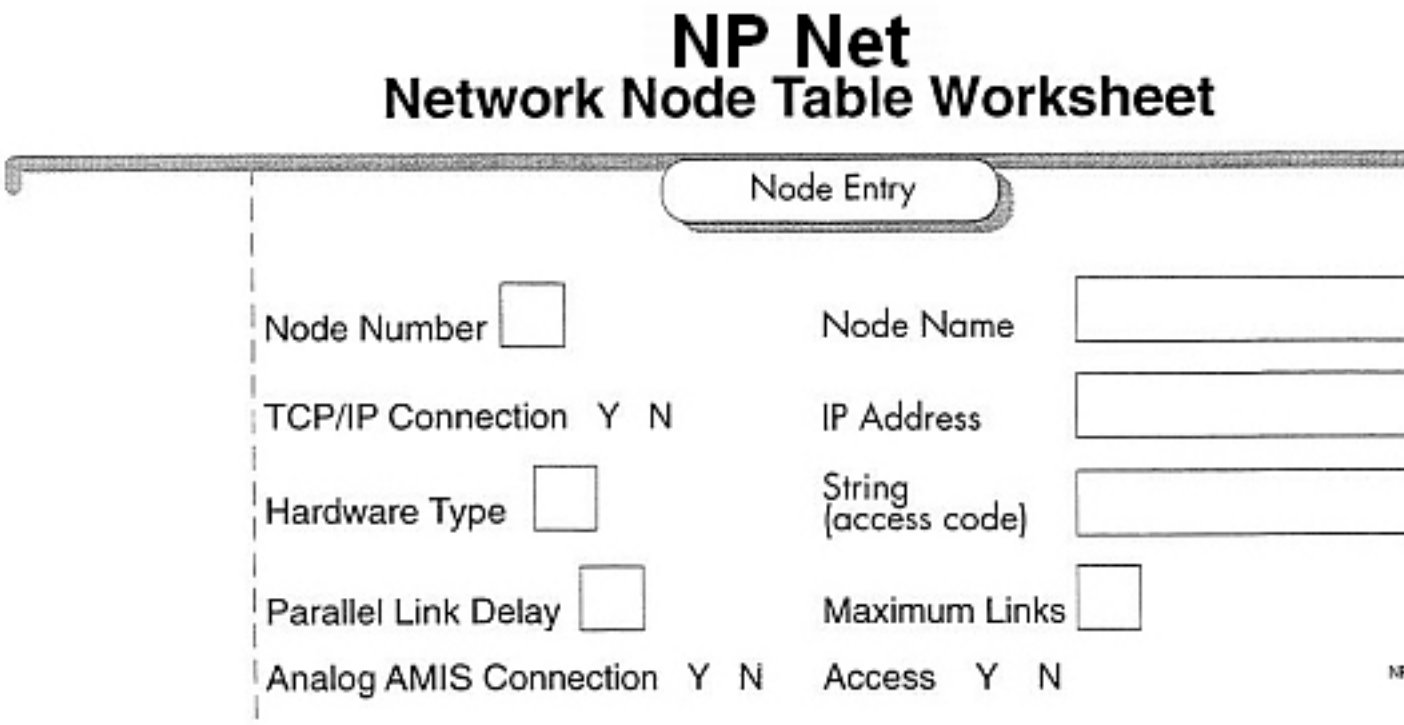
Note: Network Node Table programming must be done using the **Text Console**.

The Network Node Table stores information that is essential for the local node to communicate with other nodes on the network. The table contains one entry for each node on the network, and that entry contains information such as the remote node number and its phone number or IP address. This section provides detailed information about the fields in the Network Node Table and how they are used by NP Net TCP/IP.

It is very important that you plan out your NP Net network before configuring the Network Node Table on each node. You must know the node number and phone number or IP address of each remote node, plus other information, before you can create an entry for the node. Be sure to completely fill in a section of a Network Node Table Configuration Worksheet for each remote node and one for the local node before starting to create entries in the table. (You should create an entry for the local node in the table as a reference, but set it to have access disabled.)

26.93.1 Network Node Table Configuration Worksheet

You configure the Network Node Table using the Network Node Access Table Maintenance Menu, which is a submenu of the Network Maintenance Menu. The fields in the Network Node Table Configuration Worksheet correspond to the information you must enter when you create a new node entry. The fields are described below the sample worksheet. Blank worksheets for you to copy and use are here.



Worksheet Definitions

Node Number: The number of the node for this entry. Each NP Net node on the network must be represented by a unique number. You can use numbers from 1 to 8191, but the maximum number of nodes is 1500.

Node Name: A descriptive name for the node (e.g. New York, Chicago) of up to 13 alphanumeric characters, including capitals and spaces. The node name is not required; NP Net software recognizes nodes by their numbers.

TCP/IP Connection: Circle Y for all remote nodes that the local node accesses using NP Net TCP/IP.

IP Address: The IP address of the remote node, if it uses NP Net TCP/IP.

Hardware Type: For NP Net TCP/IP nodes, the hardware type is always ETHERNET.

Access: Circle Y (accessed enabled) for all nodes except the local node. If necessary, you can set access to N to suspend access to a node without deleting the node from the Network Node Table.

When users try to make messages to a disabled node, they are informed that the destination is "not a valid remote mailbox number." When you disable access to a node that already has messages queued, the NP Net software holds the messages until the Message Waiting Threshold is reached, and then sends receipts to all senders, informing them that their messages could not be delivered. Once receipts are sent, the messages are purged from the queue.

Parallel Link Delay: (Requires the Parallel Links optional feature) Specify the number of minutes that an existing connection must be open before another link is established. Set this to 0 to have the originating node create a new connection as soon as the previous one succeeds.

Maximum Links: (Requires the Parallel Links optional feature) Specify the maximum number of links to be used to communicate to the remote node.

26.93.2 Create or Modify a Network Node Table Entry

Use this procedure to create a new entry in the Network Node Table for NP Net TCP/IP.

1. Fill out a Network Node Access Table worksheet.
2. From the Main Menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, and then **(T) Network Node Table**.
3. Select **(C) Create new node entry** or **(M) Modify a node entry** and enter the node **number** (1 to 8191) for which you want to create/modify an entry. Press Enter to retain the current setting of any parameter.
4. At the **Select Protocol [TAV]?** prompt, do one of the following:
5. select **T** if the node will be accessed using **TCP/IP**
6. select **A** if the node will be accessed with an analog (**AMIS**) connection
7. select **V** if the node will be accessed using **VPIM** (for nodes that do not accept proprietary TCP/IP)

To configure **TCP/IP** connections:

- At the **Node name** prompt, enter the **name** (1-12 numeric characters, including spaces) of the new node.

- At the **IP Address** prompt, enter the **IP address** of the new node.
- At the **Select Encoding Type** prompt, enter **H** for **G.711** or enter **N** for **NMS**
- At the **Access (Y/n)** prompt, specify whether access to the node should be on (**Y**) or off (**n**).

To configure **AMIS** connections:

- At the **Node name** prompt, enter the **name** (1-12 numeric characters, including spaces) of the new node.
- At the **String?** prompt, enter the string (up to 16 alphanumeric characters) required to access this node. (This is usually a phone number, for example, 6135922122).
- At the **Access (Y/n)** prompt, specify whether access to the node should be on (**Y**) or off (**n**).

To configure **VPIM** connections:

- At the **Domain Name** prompt, enter the domain name of the new node (for example, mitel.com).
- At the **Select Encoding Type** prompt, enter **G** for **G.721**, **H** for **G.711,** or enter **N** for **NMS**
- At the **Select Prefix to Use** prompt, enter **D** to use the default prefix, **N** to use no prefix, or **A** to use an alternate prefix, and then specify the alternate prefix.
- At the **Access (Y/n)** prompt, specify whether access to the node should be on (**Y**) or off (**n**).

If you have installed the Parallel Links optional feature, you are prompted to configure it now.

1. At the **Parallel link delay** prompt, set the **number of minutes** that the existing connection or connections must be open before a parallel connection is established. If you enter 0, a new link is created as soon as the previous link succeeds.
2. At the **Maximum parallel links** prompt, set the maximum **number** (1-8) of parallel links that the node can establish with another node. Do not exceed the number of physical links that both nodes can support.

NP Net displays a message that the entry for the node has been created. You can repeat the steps above to create more node entries, or press **Enter** to return to the Network Node Access main menu. Select **(L) List the node table** to view all nodes.

- **Node Number**: The number of the node for this entry. Each NP Net node on the network must be represented by a unique number. You can use numbers from 1 to 8191, but the maximum number of nodes is 99.
- **Protocol**: NP Net on Release 8.5 or later supports only one protocol for communication with the remote nodes. This protocol is TCP/IP Connection. Select “Y” for all remote nodes that the local node accesses using NP Net TCP/IP.

> **Note**:
> The other two protocols “Basic NP Net” and "Analog AMIS Connection” are not used in communication with remote nodes.

- **Node Name**: A descriptive name for the node (e.g. New York, Chicago) of up to 12 alphanumeric characters, including capitals and spaces. The node name is optional (but highly recommended to help clarify the location where your system will be connecting) since NP Net software recognizes nodes by their numbers.

- **IP Address**: The IP address of the remote node, if it uses NP Net TCP/IP.
- **Node (Encoding) Type**: The encoding type indicates whether the node is configured to receive/send messages in G.711 format or NMS format.

Note:
This option is only applicable for Release 8.5 and later systems and you need to specify the G.711 format in this field.

- **Access**: Select “Y” (accessed enabled) for all nodes except the local node. If necessary, you can set access to "N" to suspend access to a node without deleting the node from the Network Node Table.

Note:
When users try to make messages to a disabled node, they are informed that the destination is “not a valid remote mailbox number." When you disable access to a node that already has messages queued, the NP Net software holds the messages until the Message Waiting Threshold is reached, and then sends receipts to all senders, informing them that their messages could not be delivered. Once receipts are sent, the messages are purged from the queue.

26.93.3 Delete a Network Node Table Entry

Use this procedure to delete nodes from the Network Node Table.

1. From the Main menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, *and then* ***(T) Network Node Table***.
2. Select **(D) Delete node entry** and enter the **number or a range of numbers** of the node or nodes to delete.
3. At the **Delete (Y/N)** prompt, press **Y** to confirm the deletion or **N** to cancel the deletion.
4. Press **Enter** to return to the Network Node Access Table menu.

26.93.4 View the Network Node Table

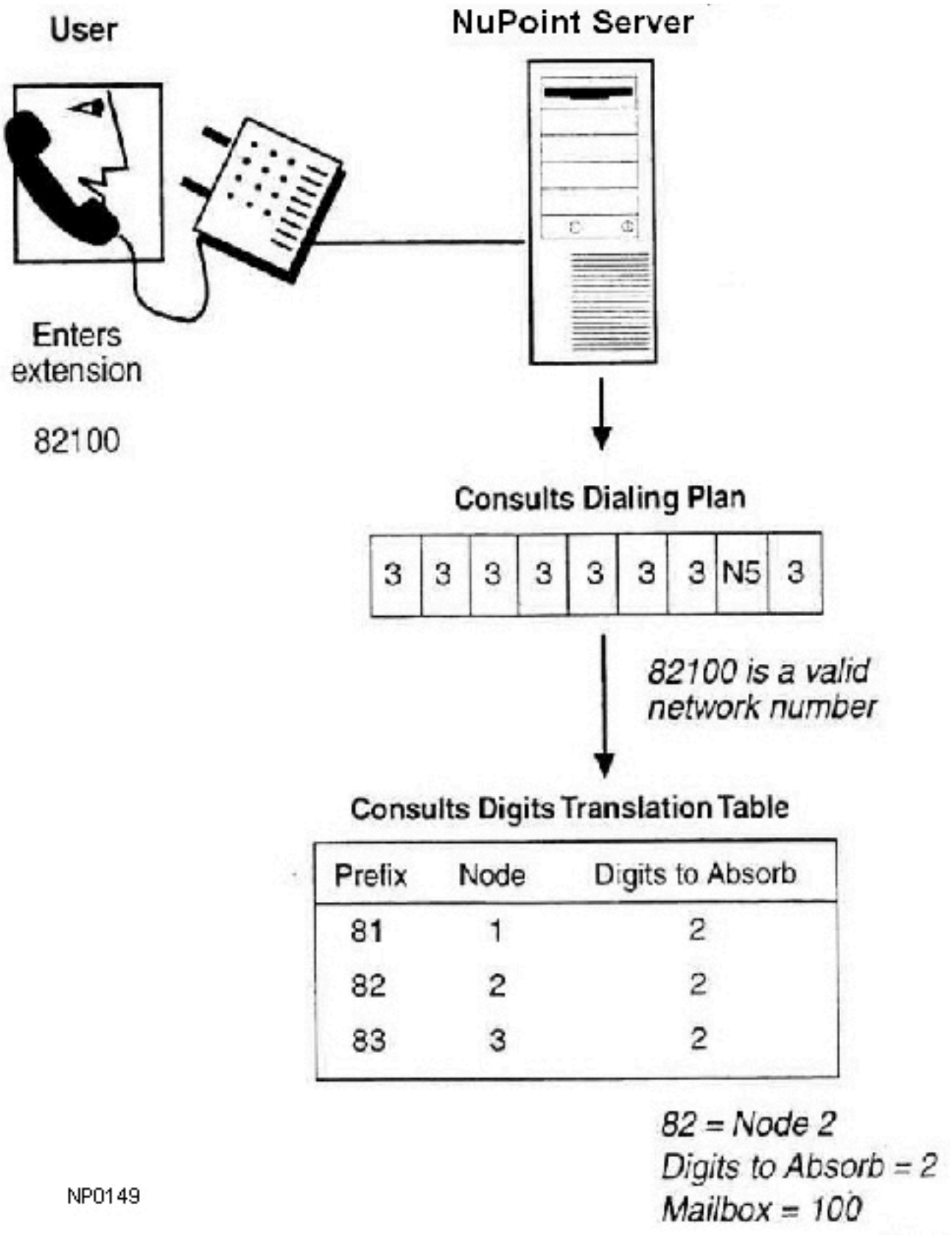
To view Network Node information:

1. From the Main Menu, select **(S) System Maintenance**, **(W)Network Menu**, **(M) Network Maintenance**, and then **(T)Network Node Table**.
2. To inquire about a single node, select **(I) Inquire about a node entry** and then enter the **number** of the node for which you want information.
3. To view the entire network node table, select **(L) List the node table**.
4. Press **Enter** to return to the Network Node Table menu.

26.94 Configuring Network Addressing - Overview

When a user addresses a message, the NuPoint Voice software must be able to identify the address as either a local mailbox or a remote mailbox. If it is a remote mailbox, the NuPoint Voice software must be able to identify the correct remote node and the correct mailbox on that node.

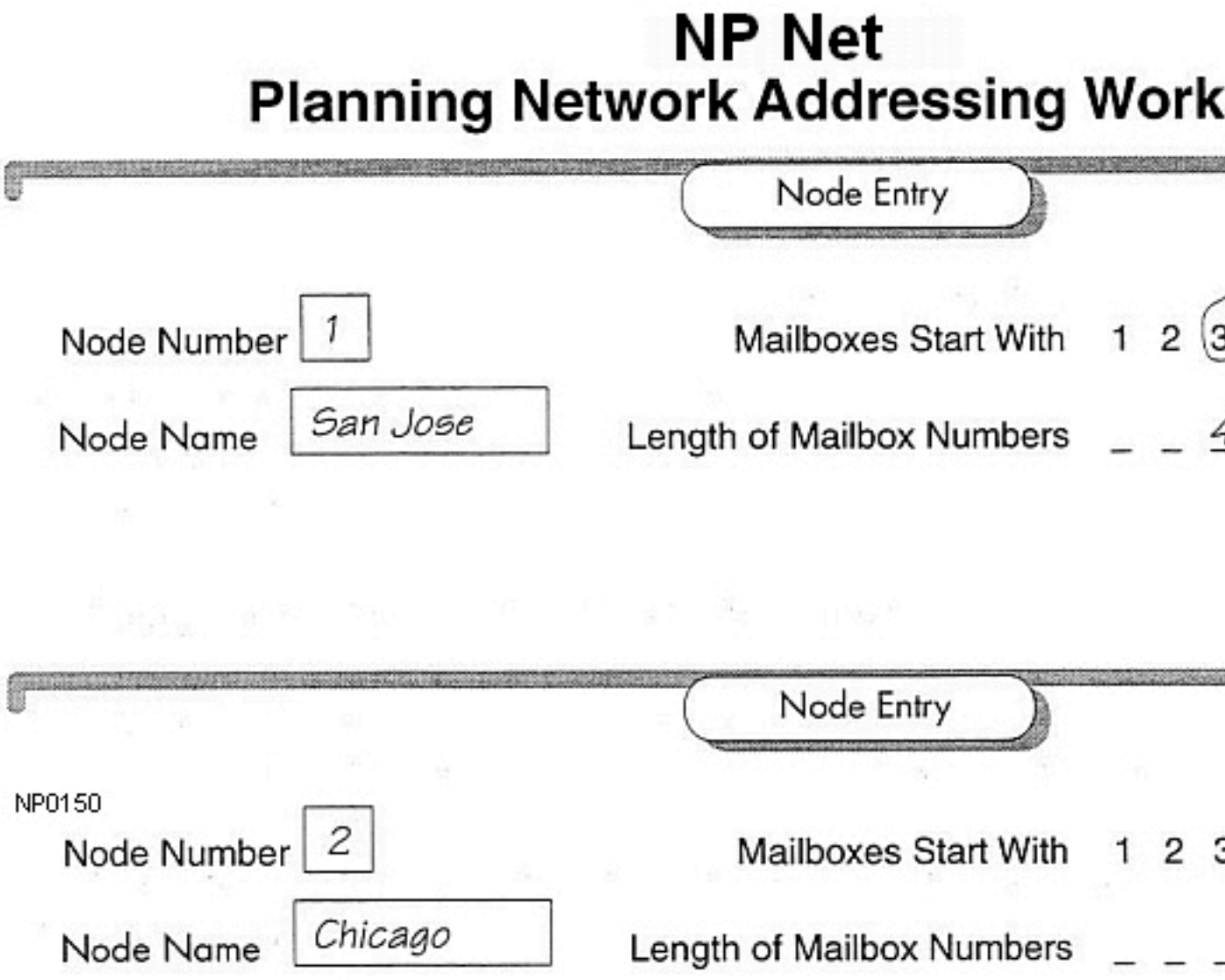
The Dialing Plan identifies the message address as either a local mailbox or a remote mailbox. The Digits Translation Table determines the correct node of the remote mailbox and how to derive the mailbox number from the address entered. The diagram below shows how these two filters work together:


User
NuPoint Server
Enters extension
82100
Consults Dialing Plan
3 3 3 3 3 3 3 N5 3
82100 is a valid network number
Consults Digits Translation Table
Prefix Node Digits to Absorb
81 1 2
82 2 2
83 3 2
82 = Node 2
Digits to Absorb = 2
Mailbox = 100
NP0149

26.94.1 Planning Network Addressing

Your NP Net network will be much easier to maintain and expand if you carefully plan network addressing in advance. You must consider any existing switch extension numbering and NuPoint Voice dialing plans, and then create dialing plans on all nodes that allow easy access to all other nodes.

Use the Planning Network Addressing Worksheet to gather the information that you need to create a network addressing scheme that meets your needs. Study the sample worksheet and descriptions below, and then copy the blank worksheet and fill in the information for your network. Be sure to include an entry for your local node.



Worksheet Definitions

Node Number: The number of the node for this entry. Each NP Net node on the network must be represented by a unique number. You can use numbers from 1 to 8191, but the maximum number of nodes is 1500.

Node Name: The name or location of the node.

Mailboxes Start With: Circle the numbers that are used at the node as the first digit in user mailboxes. For example, if mailboxes at a node are in the 3000 and 4000 range, circle 3 and 4.

Length of Mailbox Numbers: For each number that you circled, write in the number of digits in mailboxes that start with that number. If mailboxes have variable lengths, write V.

26.94.2 The Digits Translation Table

Note:
Digits Translation Table programming must be performed using the **Text Console.**

The Digits Translation Table is the "sorting machine" or "routing table" for network messages. When a user addresses a message to a remote mailbox, NP Net compares the mailbox address to the prefixes listed in the Digits Translation Table. The Digits Translation Table tells where the message is going, and how many digits the remote node must delete ("absorb") to find the destination mailbox.

The following excerpt from a Digits Translation Table indicates that any mailbox addresses that begin with 21 or 22 are to be routed to node 2 (Chicago), and any addresses that begin with 23 are to be routed to node 8 (Dallas). In addition, the remote nodes must strip off two digits (the prefix) to find the destination mailbox number.

Node Node Digits To

Prefix Number Name Absorb

21 2 Chicago 2

22 2 Chicago 2

23 8 Dallas 2

It is recommended that the table be the same in each node. You can enter your local node number in this table. If some nodes are not allowed to communicate with certain remote nodes, then use the GCOS feature to properly segregate those communities of interest.

Note:
Digits Translation Table programming must be done using the Text Console.

Node Prefixes

All network messages are routed by the node prefixes in the Digits Translation Table. Node prefixes are the leading digits of network mailbox numbers that are unique to a node. In the sample Digits Translation Table above, the prefix 23 uniquely identifies node 8; only network addresses at node 8 begin with the digits 23.

The length of an individual prefix depends on whether you are using access codes (see below) and whether mailboxes on two or more nodes share the first, second, third, fourth, etc. digits. Each prefix consists of a number of shared leading digits, plus one digit that is found only in the mailboxes of a single node.

Example:

The San Jose node has the following dialing plan:

4,N4,N4,N4,4,4,4,4,4

This means that the remote mailbox numbers that San Jose can access begin with 2, 3, or 4, and consist of four digits.

The Chicago node (Node 2) uses mailbox numbers 2000 to 2999, and 3000 to 3250

The New York node (Node 4) uses mailbox numbers 3260 to 3999, and 4000 to 4499

The Dallas node (Node 6) uses mailboxes 4500 to 4999

Because none of the nodes have overlapping mailbox numbers, the digits to absorb count is 0 for all prefixes. The San Jose Digits Translation Table would look like this:

Node Node Digits To

Prefix Number Name Absorb

2 2 Chicago 0

30 2 Chicago 0

31 2 Chicago 0

320 2 Chicago 0

321 2 Chicago 0

322 2 Chicago 0

323 2 Chicago 0

324 2 Chicago 0

325 2 Chicago 0

326 4 New York 0

327 4 New York 0

328 4 New York 0

329 4 New York 0

33 4 New York 0

34 4 New York 0

35 4 New York 0

36 4 New York 0

37 4 New York 0

38 4 New York 0

39 4 New York 0

40 4 New York 0

41 4 New York 0

42 4 New York 0

43 4 New York 0

44 4 New York 0

45 6 Dallas 0

46 6 Dallas 0

47 6 Dallas 0

48 6 Dallas 0

49 6 Dallas 0

If a message is made for remote mailbox 3267, NP Net checks the table, sees that prefix 326 matches this mailbox, adds a flag to the message that tells the remote node to absorb no leading digits from the incoming mailbox number, then adds the message to the queue for node 4.

Note the variation in the number of digits needed to make a prefix unique to a node. Chicago is the only node using mailboxes that begin with 2, so that prefix only needs to be one digit. Chicago and New York both uses mailboxes in the 3200 series, so these prefixes must be taken out to the third digit to be unique.

Another thing that is noteworthy about this dialing plan is that no remote mailbox numbers overlap, either with each other or with local San Jose mailboxes. New York, Chicago, and Dallas could use mailbox numbers that begin with 1, 5, 6, 7, 8, and 9, but users on the San Jose system cannot send messages to these mailboxes through NP Net. The San Jose dialing plan will need to be configured differently in order to enable messages to those mailboxes. The Digits To Absorb feature can be used to add this flexibility to the dialing plan.

Digits To Absorb

You assign a Digits To Absorb number to each prefix in the Digits Translation Table. The number of digits can be from 0 to 10. After NP Net matches the destination mailbox number to a prefix, it attaches the corresponding Digits To Absorb count to the message. The remote node deletes the specified number of leading digits to convert the network mailbox number to a local mailbox number. You must configure each node to send Digits To Absorb counts that allow remote nodes to translate network mailbox numbers to valid local mailbox numbers.

Digits to Absorb and Local Mailboxes

If local mailbox numbers match a dialing plan position that contains an N, then there must be a prefix entry in the Digits Translation Table that has the local node number.

If every node on the network uses the same dialing plan, all mailboxes must be the same length. For example, if every node on a network uses the dialing plan *N7,N7,N7,N7,N7,N7,N7,N7,N7*, users on every node are permitted to make messages for local or remote mailboxes that have 7 digit numbers only. Since NP Net does not absorb digits from local mailboxes, all local mailboxes on every system must be 7 digits; therefore, no digit absorption is possible throughout the network. The following section shows a way to formulate a network-wide dialing plan to avoid this limitation.

Using the Digits to Absorb Feature to Create "Access Codes"

The digits to absorb feature can simplify Digit Translation Table configuration by allowing each node administrator to formulate "access codes" for the other nodes on the system. A user enters the access code for the node before entering the mailbox number of the recipient when making a message for a remote mailbox. For example, if the access code for Boston is 82 and the mailbox you want to reach is 100, you would enter 82100.

You can implement this feature with the either N or the P character in the dialing plan. With the N implementation, users will enter just the access code and mailbox. With the P implementation, users will enter a "network" access code digit, identifying that a network message is being made, then a "node" access code, identifying the destination node, then the destination mailbox number.

The access codes are prefixes in the Digits Translation Table; the associated digits to absorb count tells the remote node to delete the access code to obtain the local mailbox number. Problems with mailbox number overlap between remote nodes are avoided, since the "real" mailbox number (the local mailbox number on the remote node) is obtained after the message is sent.

Using the Digits to Absorb Feature to Create Same-Length Mailbox Numbers

If you want users to always enter the same number of digits for all network addresses, you can use the Node Prefixes and the Digits to Absorb feature in the Digits Translation Table to "pad out" the mailbox numbers for nodes that use shorter extensions. For example, if node 2 uses 3-digit extensions and node 6 uses 4-digit extensions, you can create prefixes for node 2 that are one digit longer than the prefixes for node 6. You also set the Digits to Absorb count for node 2 to be one digit greater than the Digits to Absorb for node 6. The sample Digits Translation Table below shows this kind of configuration.

Node Node Digits To

Prefix Number Name Absorb

211 2 Chicago 3

22 6 Dallas 2

26.94.3 Creating a Network Dialing Plan

When you initially configure NP Net software on your server, you must set the dialing plans so that users can send network messages. You must set the dialing plan of every line group (NuPoint Voice, NP Receptionist, and so on) from which users will be allowed to send network messages. If any line group has more than one application, such as NP Receptionist and an integration, remember to change all of the dialing plans. Do not change PBX dialing plans for Enhanced SMDI line groups.

If the dialing plan for a particular application is not changed, a user who calls in on the line group dedicated to that application will be unable to make messages for remote mailboxes. For example, Message Delivery uses the dialing plan specified for the Pager Application. When Message Delivery calls a user at a pre-programmed telephone number because there is an unplayed message in the mailbox, the user enters the mailbox passcode and is logged into the mailbox.

If the Pager Application dialing plan is not changed to match the Network Dialing Plan, the user will be unable to make messages to remote mailboxes. To communicate with remote mailboxes, the user must call the standard NuPoint Voice number, where he or she will log in under the NuPoint Voice application.

When you configure the dialing plans for NP Net messaging, you must choose to use a network prefix digit, direct network addressing digits, or a star-prefix dialing plan.

Using a Network Prefix Digit

A network prefix dialing plan uses one number to indicate that the mailbox address that follows is a network address. For example, if 9 is the network prefix digit, users must press 9 and then the network mailbox address to send network messages.

You specify a network prefix digit in the dialing plan with the letter P, followed by the number of allowable digits in a network mailbox address (*including* the prefix digit). For example, if 9 is the network prefix digit and network mailbox addresses have 6 digits, the dialing plan might look like:

0,0,0,4,4,4,0,0,P7

Notice that the P is in the 9s position, and it allows for seven digits: the network prefix digit plus a six-digit network mailbox address. The system strips off the prefix digit before comparing the mailbox address to the Digits Translation Table. In other words, if a user addresses a message to 9234567, the system compares 234567 against the Digit Translation Table.

In this example, if the sender attempts to address a message by pressing 9 and five digits (or any number other than six), the system says that the address is not valid. Local mailbox numbers cannot begin with the same digit as the prefix digit.

The P character can make dialing plans very flexible, especially when adding NP Net to a server that has an established mailbox dialing plan. For example, if both the local node and remote nodes have mailboxes that begin with 6 and 7, the administrator can tell users to press 9 plus the mailbox number to make a message for a remote mailbox. The 6 and 7 positions in the dialing plan can still be used by local mailboxes, and the previously unused dialing plan position 9 is reserved for remote mailboxes. The system handles the mailbox 678123 differently than 9678123.

Using Variable-Length Network Addresses

It is not uncommon for different nodes on a network to have mailboxes that do not have the same number of digits. For example, node 1 may have 4-digit mailboxes and node 2 may have 5-digit mailboxes. There are two ways to accommodate this situation in network addressing.

If you want users to always enter the same number of digits for all network addresses, you can use the Digits to Absorb feature in the Digits Translation Table to "pad out" the shorter mailbox numbers. See Digits Translation Table for more information on this technique.

The other alternative is to use the P and V characters together in the dialing plan. (The V character indicates a variable-length mailbox number; see About Dialing Plans for more information on the V character.) This combination allows users to address messages by entering a network prefix digit followed by the minimum number of digits required to uniquely identify a remote node and mailbox. For example, if node 3 uses 5-digit mailbox numbers and node 4 uses 4-digit mailbox numbers, the following dialing plan on node 1 would allow addressing to mailboxes on both nodes:

0,0,0,4,4,4,0,0,PV

If the prefixes in the Digits Translation Table matched the node numbers, then a user could address a message to mailbox 44564 on node 3 by entering 9344564, and to mailbox 3445 on node 4 by entering 943445.

Addressing by Area Code and Phone Number

You can also use the P character to allow addressing messages by area code and phone number. This type of dialing plan is useful when users have DID or Centrex-type service and callers are used to reaching them by dialing 7 or 10 digits (without going through an operator). It can alleviate conflicts between telephone/mailbox numbers on different nodes that share the same telephone number prefix (the first three digits of a seven digit telephone number).

For example, two nodes may have telephone numbers that begin with 257. A dialing plan with P11 in the 1s position would allow users to address network messages by entering 1 + the area code + the mailbox number, just as though they were dialing long-distance calls. The P in the dialing plan means that the 1 is dropped. The Digits Translation Table is configured to match the area codes and route messages to the correct remote nodes. When a message reaches a remote node, the three area code digits are deleted, and the message is delivered to the local seven digit mailbox number.

Using Direct Network Addressing Digits

If you do not want to use a prefix digit for network addressing, or if you want to use fully integrated local and remote mailbox numbers, you can use direct network addressing digits. The N character in a dialing plan position indicates that mailbox addresses that begin with that digit are network mailboxes, and should be processed by the NP Net software. The N is always followed by the number of valid digits in the network mailbox address. For example, the following dialing plan indicates that addresses that start with 7 or 8 are 6-digit network addresses.

0,0,0,4,4,4,N6,N6,0

In this example, when a message is addressed to a mailbox number that begins with 7 or 8, the NP Net software finds the destination node by comparing the leading digits of the mailbox number with the prefixes stored in the Digits Translation Table. Those prefixes would start with 7 or 8; the first digit is not stripped off when you use the N character.

Note that local mailbox numbers can also begin with 7 or 8, but they must have 6 digits, and the Digits Translation Table must contain prefixes that match the local mailboxes with the local node number. If the node number in the table matches the local node number, the message is sent immediately to the local mailbox (local messages sent through a network dialing plan are not queued). Senders do not need a Network Class of Service to send local messages, even though the dialing plan position indicates a network mailbox destination. Billing and statistics are the same as for local messages sent through a conventional dialing plan.

You can use this strategy is to create a same-length dialing plan for every node on the network, such as *N7,N7,N7,N7,N7,N7,N7,N7,N7,N7*. This means that every time a message is made for a mailbox, the address is checked against the Digits Translation Table to find the destination node. The main advantage of this type of dialing plan is that a user enters the same number of digits to reach a mailbox on any node.

Creating a Uniform Network Dialing Plan

You can use a uniform dialing plan if the mailbox numbers on each node have unique ranges (for example, mailbox numbers on node 2 are in the range of 3000 to 3500 and no other nodes have mailbox numbers in that range). The advantage of a uniform dialing plan is that users can simply dial the mailbox number to access remote mailboxes. The disadvantage is that you must take local mailboxes into account in the Digits Translation Table. Mailbox number distribution takes careful planning, since local mailbox numbers cannot conflict with mailbox numbers on any remote node. You can resolve conflicts by adding *access codes* to remote mailbox numbers, then using the digits to absorb feature to tell the receiving system to delete the access code to find the true mailbox number. The digits to absorb feature is described earlier in this section.

Using a Star Prefix Dialing Plan

NuPoint Unified Messaging servers that do not have any open positions in the dialing plan may need to use a star prefix dialing plan for network addressing. The star prefix dialing plan provides the functionality of both the N and P characters, although the functions have different names. If the P function were assigned to the 9 position in a star prefix dialing plan, a user would press 9* and then the network mailbox address to send a network message.

See About Dialing Plans for more information about star prefix dialing plans.

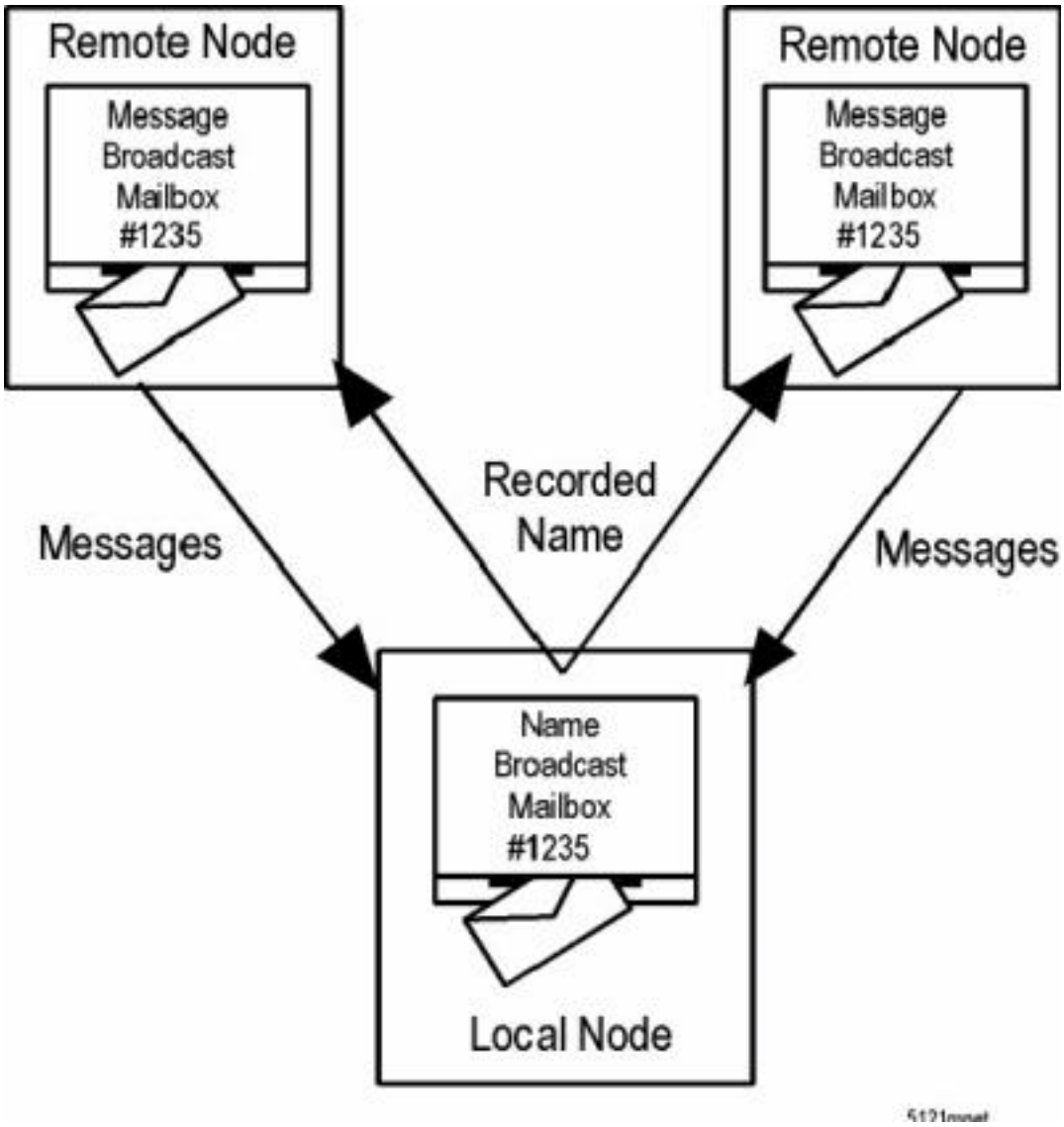
26.94.4 Using Broadcast Mailboxes for Transparent Network Messaging

Transparent network messaging means that there is no difference to the user between sending a message to a remote mailbox and sending a message to a local mailbox. The user does not enter a network prefix when addressing a message, and the user hears the name confirmation of the mailbox owner.

You can use broadcast mailboxes to achieve this transparency. A message broadcast mailbox automatically sends any messages that it receives to the mailboxes in its first distribution list. A name broadcast mailbox automatically sends the owner's recorded name to the mailboxes in its distribution list number 9, to be used as the recorded name for those mailboxes. You enable these features in the FCOS of the broadcast mailboxes. See Types of Mailboxes for more information about broadcast mailboxes.

For complete network transparency, every user on every node must have a mailbox on every node. A user's mailbox on the local node has name broadcast enabled, so that the user's recorded name is broadcast to that user's mailboxes on all other nodes. The user's mailboxes on remote nodes all have

message broadcast enabled, so that all messages made for that user are broadcast to the local node. The diagram below shows this type of configuration:



Users always address messages to mailboxes on their local node. Because the recipient mailbox is local, the sender hears the mailbox name confirmation. If the mailbox is configured as a broadcast mailbox for a user on a remote node, the mailbox forwards the message over the network to the local node of the recipient.

Note: Broadcast mailboxes put an extra burden on system administrators. You must still configure the Digits Translation Table to provide the routing required for network messages. In addition, mailbox adds, moves and changes must be coordinated across the network, and the distribution lists in the broadcast mailboxes must be kept current. See Configuring Network Mailboxes for information about adding remote mailbox addresses to distribution lists.

26.94.5 Network Addressing Examples

The following examples illustrate various ways of configuring network addressing to meet the needs of different networks.

Example 1: Adding Simple Access Codes

A network consists of four nodes: San Jose (Node 1), Chicago (Node 2), New York (Node 4) and Dallas (Node 6). Before the NP Net optional feature was installed, the San Jose node had three digit local mailboxes that began with digits 3 through 8. If the administrator wants to retain this structure, she can use dialing plan position 9 for remote mailboxes. The following changes makes this possible:

- The old San Jose dialing plan of *0,0,3,3,3,3,3,3,0* is changed to *0,0,3,3,3,3,3,3,N5*.
- The access codes for all remote nodes begin with 9
- Each prefix has a digits to absorb count of 2
- The Digits Translation Table for San Jose looks like this:

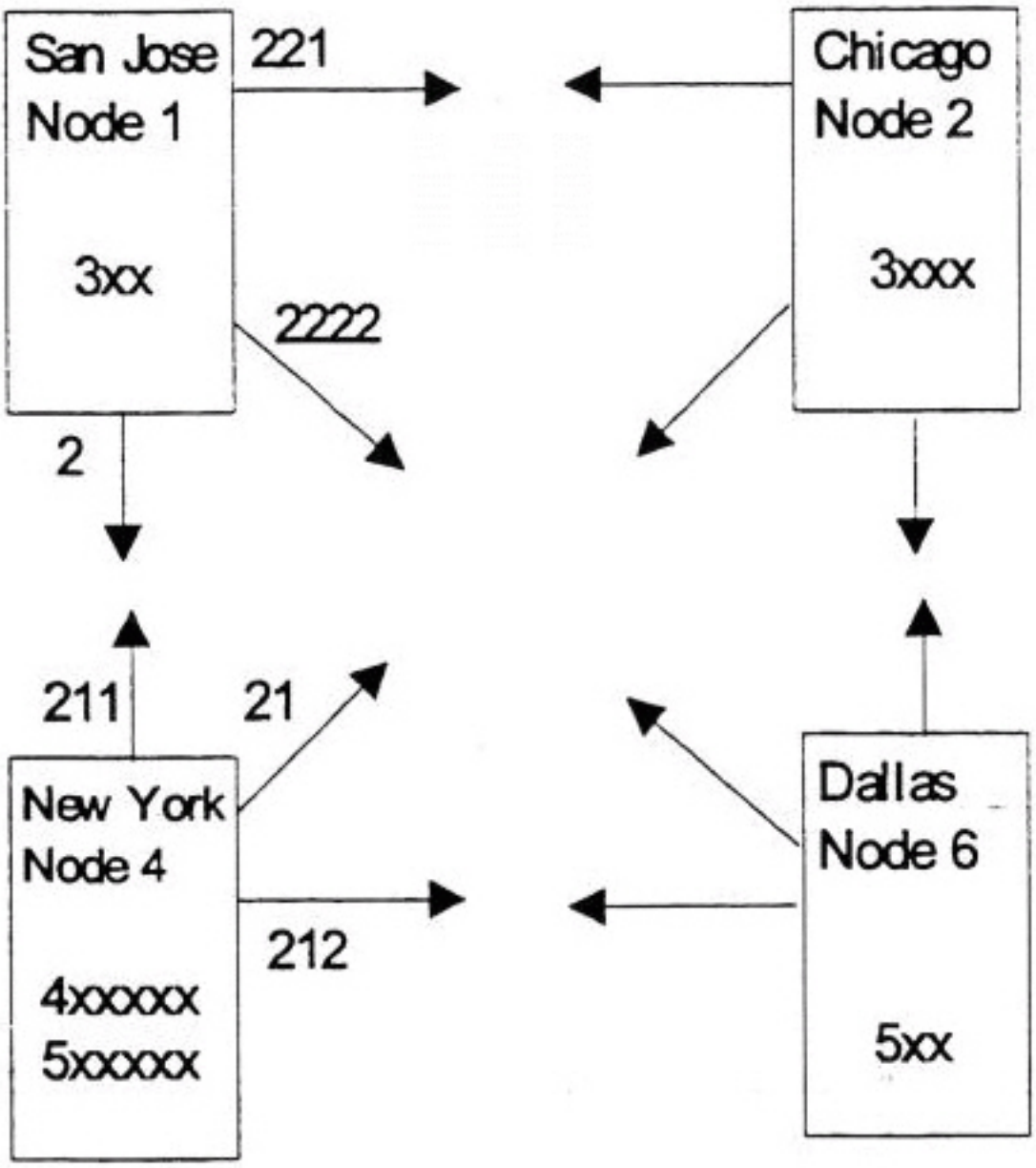
Node Number	Node Name	Digits to Absorb
Prefix		
92	2 Chicago	2
94	4 New York	2
96	6 Dallas	2

The access code length depends on how many number combinations are needed to cover all the nodes on the system, but the codes should not be so long that it is a chore for users to send remote messages. In the example above, the access codes can be up to 8 digits, since mailbox numbers can be up to 11 digits, but it is unreasonable to expect system users to remember 8 digit access codes and 3 digit mailbox numbers. A very large network would require more positions for remote nodes to make this scheme workable.

This method is useful for NuPoint Unified Messaging servers like the one in the example, where NP Net software is installed on an established system that has a pool of users who have memorized many mailbox numbers and do not want them to change. It is also practical for NuPoint Unified Messaging servers on which both NP Net and NP Receptionist are installed. Mailbox numbers can match NP Receptionist extension numbers without regard to the extension/mailbox structures of other nodes.

Example 2: Access Codes and Variable Length Remote Mailbox Numbers

Suppose one has the network shown below. The Chicago node (Node 2) has four digit mailboxes that start with 3, the New York node (Node 4) has six digit mailboxes starting with 4 or 5, and the Dallas node (Node 6) has three digit mailboxes that start with 5. Optimally, all these mailboxes must be served by the same dialing plan position. The access codes for all remote nodes can still begin with 9, as that digit is not part of any existing dialing scheme. Let’s analyze each node individually:



San Jose

Users on the San Jose node would like to enter the same number of digits to send messages to mailboxes on any of these three remote nodes, even though the destination mailbox numbers have different lengths. A digits absorbed count for each prefix is suddenly very useful. Since New York remote mailboxes already have six digits, the administrator decides that users will only need to enter a one digit access code (i.e. 9) to reach New York. The digits to absorb count for the New York node is 1. The prefixes listed for New York in the Digits Translation Table must include at least the first digit of all possible valid mailbox numbers on the node, to make all mailboxes accessible, and to make all prefixes unique. The dialing plan in San Jose is changed to 0,0,3,0,0,0,0,0,N7 to accommodate the New York node. Local mailboxes are unaffected by the change.

To access the four-digit mailboxes on the Chicago node, the Digits Translation Table must have three digit prefixes (access codes) to conform with the seven-digit network dialing plan (three digit access code plus a four digit extension equals seven digits). The digits to absorb count is also 3 for all Chicago prefixes.

The Dallas node uses three-digit mailboxes, so it needs a four digit access code to conform with the dialing plan. The digits to absorb count is 4 for all Dallas prefixes.

San Jose Digit Translation Table

Node Node Digits To

Prefix Number Name Absorb

221 2 Chicago 3

2222 6 Dallas 4

24 4 New York 1

25 4 New York 1

New York, Chicago, and Dallas

The administrators for the New York, Chicago, and Dallas nodes all decide that users on their servers will address network messages with a prefix digit, a node access code, and variable length mailbox numbers. This simplifies their system planning and maintenance.

All three sites use 9 as the network prefix digit, so the dialing plan for New York is

0,0,0,6,6,0,0,0,PV

The Digit Translation Tables for all three nodes look follow the same pattern. The table for New York is shown below.

Node Node Digits To

Prefix Number Name Absorb

1 1 San Jose 1

2 2 Chicago 1

6 6 Dallas 1

When a user in New York wants to address a message to mailbox 325 in San Jose, he enters 91325. The New York node recognizes the address as a network address and strips off the 9 because of the P character in the dialing plan. It then compares the remaining digits with the prefixes in the Digits Translation Table and finds that the message is for San Jose. When the San Jose node receives the message, it strips off one digit and delivers the message to mailbox 325.

26.94.6 Create New Prefix/Node Pairs

Use this procedure to create a new entry in the Digits Translation Table. Each entry associates a dialed prefix with a node, and sets the number of digits for the remote node to absorb from the network mailbox number.

1. From the Main Menu, select **(S) System Maintenance**, **(W)Network Menu**, **(M) Network Maintenance**, and then **(D)Digits Translation**.
2. Select **(C) Create new prefix/node pairs** and enter the **number** (1-8191) of the new entry.
3. At the **Absorb digits** prompt, enter the **number** (0-12) of digits to absorb from the network mailbox number.
4. At the **Prefix** prompt, enter a dialed prefix **number** (1 to 99,999,999,999) that indicates a message for the node in step 2.
5. Repeat step 4 to associate additional prefixes with the node, or press **Enter** to stop entering prefixes.
6. Repeat steps 2 through 5 to create entries for additional nodes. Press **Enter** when you have finished creating entries for all nodes.

26.94.7 Delete Prefix/Node Pairs

This procedure describes how to delete prefix/node pairs from the Digits Translation Table.

1. *F*rom the Main Menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, *and then* ***(T)Network Node Table****.*
2. *Select* ***(D) Delete prefix/node pairs*** *and enter a valid prefix* ***number*** *(or range of numbers separated by hyphen) to delete.*
3. *You are prompted to confirm the deletion. For single prefixes, enter* ***Y*** *to delete. For ranges of prefixes, type the word* ***delete*** *when prompted to confirm.*

26.94.8 View the Digits Translation Table

To see an online display of information about prefix/node pairs in the Digits Translation Table:

1. From the Main Menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, and then **(D) Digit Translation** Menu.
2. To view a single entry or range: select **(I) Inquire about prefix/node pairs** and enter a valid prefix number of hyphen-separated range of numbers to display.
3. To view the entire digits translation table: select **(L) List the dta table**. The server displays the report.

Sample Report:

```
>>>
www.mitel-amc.com <<<
```

PREFIX/NODE PAIR REPORT

Wed Jan 13 13:54:46 20xx

Prefix Node Absorb Cnt

700 700 3

801 801 3

802 802 3

803 803 3

804 804 3

5 Prefixes found

26.94.9 Modify the Node Number for a Prefix

Use this procedure to change the node number and number of digits to absorb associated with a prefix in the Digits Translation Table.

1. From the Main Menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, and then **(D) Digit Translation** Menu.
2. Select **(M) Modify the node number for a prefix** and enter a valid prefix **number** or hyphen-separated range of numbers.
3. At the **New node number:** prompt, enter a valid node number.
4. At the **Absorb cnt:** prompt, enter the number of digits (0-12) to absorb. The system displays the prefix to modify and prompts you to confirm.
5. Press **Y** to confirm modification or **N** to leave unchanged.

26.94.10 Configuring the Network Queues - Overview

Note:
Network Queue programming must be performed using the **Text Console.**

You can control when a local NP Net node originates connections with remote nodes by configuring the network queues. You can set the different parameters that control when a queue is ready to send, such as time of day and number of messages waiting in a queue. You can also set the number of times that the local node tries to connect to a remote node once it determines that it is time to send the messages.

You can use the network queue parameters to help control toll charges with dial-up NP Net connections. If all of your connections are TCP/IP, you probably want to set the queues to send messages immediately.

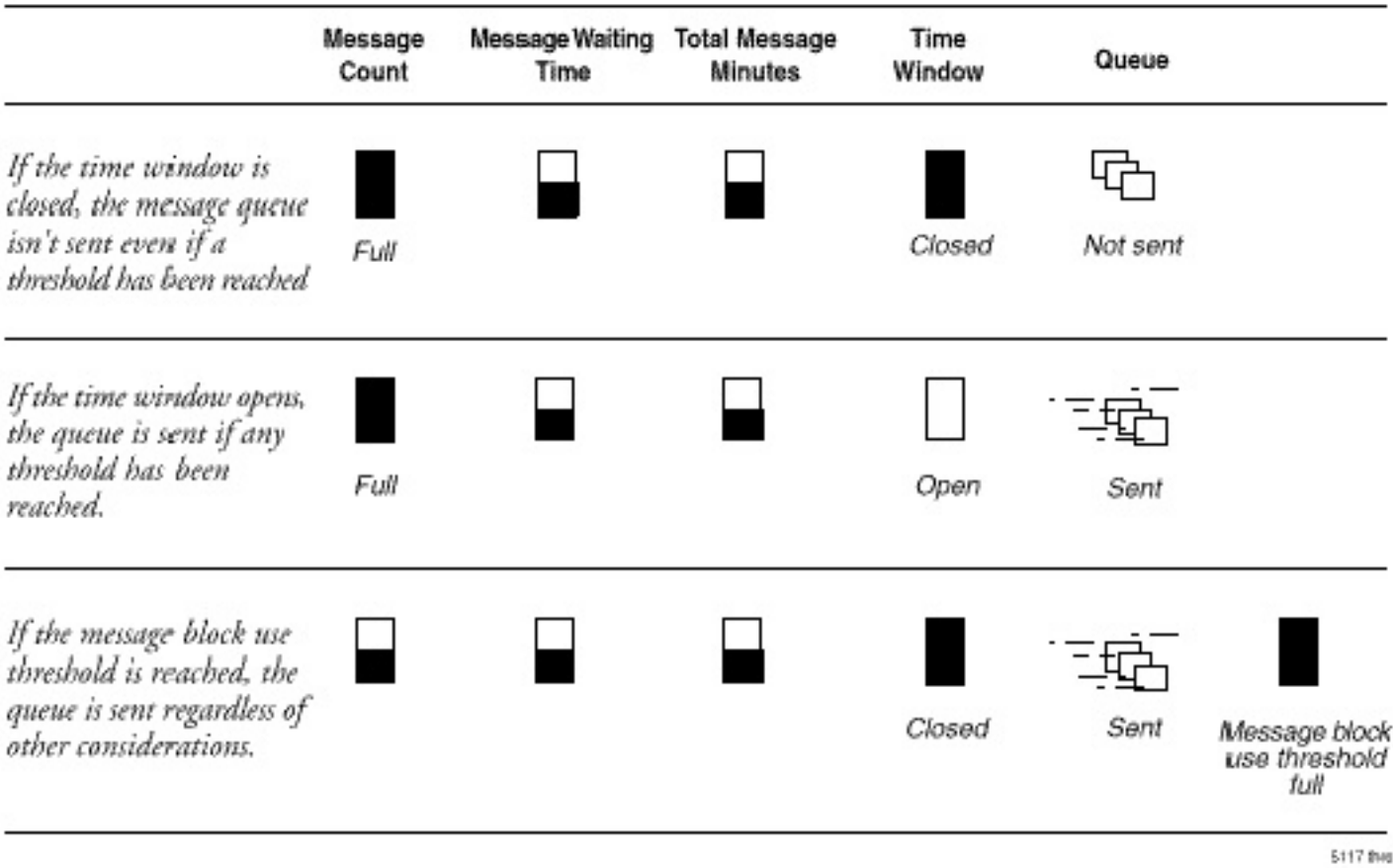
There are some basic functions of NP Net queues that you should understand before configuring the queue parameters:

- Messages addressed to remote nodes are stored in separate queues; there is an urgent message queue and a batch message queue for each node.
- The queues are checked every 30 seconds to find out if it is ready to send.

- The parameters that you set for queues apply to all nodes, but each queue is monitored separately. When the urgent queue for remote node 2 is full, the local node originates a connection to that node; it does not originate connections to any other nodes until their queues are full.
- Each node only originates connections when it needs to *send* messages, however, once a connection is established between two nodes, any messages queued for the originating node on the answering node are also sent, so messages go both ways. (If a node makes a connection to send only urgent messages, the answering node is only allowed to send messages from its urgent queue.)

After you have set the queue parameters, you should closely monitor the network queue statistics to ensure that the thresholds are set at realistic values. The cost of sending a network queue must be balanced against the need to receive messages in a timely manner and the need to clear network queue storage space. The storage aspect is particularly important when controlling costs; network message delivery that is triggered by reaching the message block use threshold will probably occur when tariffs are highest, since most messages are recorded during normal business hours.

The figure below shows the hierarchy of the various thresholds. The Time Window overrides the Message Count, Message Waiting Time, and Total Message Minutes parameters, but the Time Window is overridden by the Message Blocks Used threshold.



26.94.11 Network Queues Worksheet

The Network Queues Worksheet is designed to help you plan and record the settings of the network queues. The fields on the worksheet match the information that you must supply when configuring the

queues. Study the sample worksheet and the definitions that follow, and then copy the blank worksheet and fill it in.

NP Net
Network Queues

Network Queue Limits

Message Block Use Threshold (80-100%): 90

Maximum Call Setup Tries: 4

Call Setup Retry Interval (minutes): 10

Network Queue Time Windows

Always Open? Weekdays Weekends

Weekday Start Time (hour:min am/pm): Batch _____

Weekday Stop Time (hour:min am/pm): Batch _____

Weekend Start Time (hour:min am/pm): Batch 9:00

Weekend Stop Time (hour:min am/pm): Batch 4:00

Network Queue Thresholds

Message Count Threshold: Batch 10 Urgent 2

Message Waiting Threshold: Batch 10 Urgent

Total Message Minutes Threshold: Batch 9 Urge

Worksheet Definitions: Network Queue Thresholds

Network queue thresholds allow you to control when messages are sent to another node. Cost is an important consideration when setting these parameters; the first minute of a call is tariffed higher, so it is more economical to send a group of messages than to send each message separately

You can set different network queue thresholds and time windows for urgent and batch messages. (All messages not specifically marked urgent by the sender are considered batch.) With this two-tiered system, routine messages are sent at a time when the call is more economical, while more important messages are delivered promptly. (It is recommended that you set realistic batch limits or restrict the assignment of Network Classes of Service that allow the user to send urgent messages over the network to prevent users from marking all remote messages urgent.) The batch queues and remote queues of each remote node are monitored individually by NP Net.

Message Count Threshold: The number of messages, names, greetings, and receipt updates that must be waiting in a queue for a certain node before that queue becomes ready to send. This threshold is appropriate for sites where users tend to make frequent, short messages. The default message count threshold for batch messages is 5; for urgent messages, it is 0.

Message Waiting Threshold: The length of time, in minutes, that the oldest message will be kept waiting in the queue before the queue becomes ready to send. If the queue has a very restrictive time window (for example, if batch messages can be sent only between 12:00 am and 5:00 am), set this threshold to a low value to ensure that all network queues are ready to send when the window opens. The default message waiting threshold for batch messages is 10 minutes; for urgent messages, the default is 0 minutes (no waiting).

Total Message Minutes: The number of minutes of speech that must be waiting in a queue for a certain node before that queue becomes ready to send. This threshold is appropriate for systems where system storage tends to be high, but it is not triggered efficiently by frequent, short messages. If the node tends to process a high volume of short messages, the message count threshold is a better choice. The default Total Message Minutes threshold for batch messages is 5 minutes of speech; for urgent messages, the default is 0 minutes of speech.

Worksheet Definitions: Network Queue Time Windows (Start/Stop Times)

The start and stop times create a limited time period during which messages can be sent to remote nodes. This time window overrides all message thresholds; queues that are ready to send will not trigger a call unless the window is open. Conversely, when the time window opens, queues that have not yet met any of the thresholds will not be sent. The time window and thresholds must be carefully set, to ensure that messages do not remain queued for an unacceptable period of time.

You set separate time windows for batch and urgent messages. Within these categories, you set time windows for weekdays and weekends. In the default configuration, network queue time windows for batch and urgent messages are always open.

Always Open: Circle Weekdays or Weekends for either urgent or batch queues if you do not want message sending to be restricted by time of day.

Weekday Start Time: Write in the time of day that you want the local node to start sending messages on weekdays, provided that at least one of the network queue thresholds has been met.

Weekday Stop Time: Write in the time of day that you want the local node to stop sending messages on weekdays.

Weekend Start Time: Write in the time of day that you want the local node to start sending messages on weekends, provided that at least one of the network queue thresholds has been met.

Weekend Stop Time: Write in the time of day that you want the local node to stop sending messages on weekends.

Worksheet Definitions: Network Queue Limits

Network queue limits control network queue storage and determine how often, and at what interval, a node should attempt to send a network queue to another node before the queue is considered "undeliverable."

Message Block Use Threshold: The percentage of total queue storage that must be full to trigger an automatic connection. The Message Block Use Threshold is a "safety valve" that forces the node to empty queues when total network queue storage is almost full.

When the message block use threshold is reached, the system checks the network queues for the node with the greatest number of messages waiting and marks that queue as ready to send. The queue is sent immediately; the message block use threshold overrides all other thresholds, including network queue time windows. The system will continue to send queues until message storage falls below the threshold.

You can set the message block use threshold at any value between 80% and 100%. The default threshold is 80%.

Maximum Call Setup Tries: The maximum number of calls that an originating node will make to try to establish a connection with another node. The default value is 50.

Call Setup Retry Interval: The time, in minutes, between attempts to establish a connection. The default interval is 10 minutes.

An originate link executes the originate actions of the hardware type up to three times in immediate succession when attempting to call another node. These three calls constitute one try; that is, the call setup tries counter is increased only after all three attempts have failed.

When a first attempt at originating a call fails (the node may be busy communicating with another node on the system, for example), the node waits the amount of time specified by the call setup retry interval before repeating the originating actions. This sequence will continue until communications are established or the maximum call setup tries threshold has been reached.

If all attempts to communicate with the destination node fail, all users who sent messages to that node are notified that these messages could not be delivered.

26.94.12 Configure Network Queues

To configure the network queue parameters, including message thresholds, time windows, and queue limits:

1. From the Main Menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance,** and then **(Q) Modify Network Queueing**. Proceed to step 7.
2. Select **(T) Message Thresholds** and then select either **(B) Batch queue** or **(U) Urgent queue**.
3. To reset all threshold values to their default values, select **(W) Set to Default Values** and then enter **Y** to confirm. Otherwise, proceed to step 4.

4. Select **(M) Message Count Threshold** and enter the **number**of messages and receipt updates in a queue that, when reached, causes the queue to be sent.
5. Select**(S) Message Waiting Threshold (minutes)** and enter the **number**of minutes that a message waits before being sent.
6. Select**(T) Total Message Minutes** and enter the **number**of minutes that the total messages add up to before the queue is sent.
7. Exit from the Network Queueing menu. Repeat steps 2 through 7 for the other queue (batch or urgent).

Set Queue Time Windows

1. Exit to the Modify Network Menu and select **(S) Start/Stop Times**.
2. Select the queue to modify: either **(B) Batch queue** or **(U) Urgent queue**
3. If you do not want any time limits on when the local node can originate NP Net connections, follow these steps. Otherwise, proceed to step 11.

    - Select **(U) Always Open Weekday Window**. The system displays the parameters of this option and prompts for confirmation.
    - Enter**Y**to set the window to always open;**N**to leave the times unchanged.
    - If you do not want any time limits on when the local node can originate NP Net connections on the **weekends**, select **(V) Always Open Weekend Window**. The system displays the parameters of this option and prompts for confirmation.
    - Enter**Y**to set the window to always open;**N**to leave the times unchanged.
4. To set time limits, select **(A) Weekday Start Time** and enter the **time**that NP Net starts sending the network queue on weekdays. The time must between 01 00 am or pm and 12 00 am or pm in the format**hh mm am**or**hh mm pm**.
5. Select**(D) Weekday Stop Time** and enter the **time**that NP Net starts sending the network queue on weekdays. The time must between 01 00 am or pm and 12 00 am or pm in the format**hh mm am**or**hh mm pm**.
6. Select**(E) Weekend Start Time** and enter the **time**that NP Net starts sending the network queue on weekends.
7. Select **(I) Weekend Stop Time** and enter the **time** that NP Net stops sending the network queue on weekends.
8. Exit from the Start/Stop Times menu.
9. Repeat steps 9 through 15 for the other queue type (batch or urgent).

Set Network Limits

1. Exit to the Modify Network Queue menu and select **(L) Limits**.
2. To set parameters to their default values, select **(W) Set to Default Values** and then enter **Y** to confirm. Otherwise, proceed to step 19.
3. Select **(T) Message Block Use Threshold**and enter the**number**that indicates a percentage of buffers used for messages. When this percentage is reached, NP Net will send the queue with the greatest number of message. NP Net continues to send queues until the message storage falls below the threshold. This number can be from 80 to 100.
4. Select **(U) Maximum Call Setup Tries** and enter the **number** that indicates the number of times NP Net will try to send a network queue. Each try consists of three call setup attempts.

5. Select **(V) Call Setup Retry Interval** and enter the **number** of minutes between attempts to set up a connection to a remote node.
6. Exit the Modify Network Queue menu.

26.94.13 Managing NCOS

Network classes of services (NCOS) are similar to FCOS, except that every network bit controls one of the twelve network options (see NCOS Fields Description). You can have a maximum of 64 NCOS on the system.

You can

- List NCOS
- Add an NCOS
- Edit an NCOS
- Delete an NCOS
- See a list of NCOS Fields Description

Listing NCOS

To display a list of all NCOS in the system

- In the navigation tree, click Class of Service and then click Network COS.

Add an NCOS

1. In the navigation tree, click Class of Service and then click Network COS. The Network COS list is displayed.
2. Click Add. The Add NCOS form is displayed.
3. Do one of the following:

   - Copy an existing NCOS by selecting one from the list and clicking the **Copy from** button. The parameters of that NCOS will be copied into your new NCOS, which you can then edit as required. The Next Available NCOS number is automatically applied.

     OR
   - Chose to manually select all limits for the new NCOS
4. In the **Number** field, enter a **number** (1-64) for this NCOS, or click **Next Available** to automatically assign the next number.
5. In the **Name** field, enter a **name** (up to 15 alphanumeric characters) for this NCOS.
6. Select the check box beside each network bit that you want to enable for the NCOS. (Clear a check box to disable the selection.) For a list of network bits, see NCOS Fields Description.
7. To save the NCOS and return to the Network COS list, click Save

Edit an NCOS

Best practices dictate that you always keep your default NCOS intact. If you need to modify an NCOS, we suggest that you copy the default NCOS into a new NCOS (see "Add an NCOS" above) and modify

it there. After you save the new NCOS, you need to assign it to the appropriate mailboxes. This way, if you have problems/conflicts with the new COS, you can always restore the default until you have finished troubleshooting.

Delete an NCOS

Deleting an NCOS that is in use by mailboxes will cause all of those mailboxes to be assigned the default (1) NCOS. A warning message is displayed to allow you to cancel the operation. If you are deleting the default NCOS, the mailboxes assigned to it will be assigned to the next available NCOS. You cannot delete the last remaining NCOS in the system; therefore, you cannot select all NCOS for deletion.

To delete one or multiple NCOS

1. In the Network COS list, select one or multiple NCOS, and then click Delete. The system will prompt you to confirm the deletion.
2. To confirm the deletion, click Yesfor a single deletion or Yes to allfor a range.

   OR

   To reject the deletion, click No.

NCOS Fields Description

Field	Description	Values
Number	*Required field. Determines the number of the new NCOS. You can manually enter a number from 1-64 as long as it is not already assigned to an NCOS. You can also click the Next Available button to have the system assign the next available number to the NCOS.	Enter a number in the range of 1-64. The number must not be already used for an existing NCOS. Or click the "Use next available number" link.
Name	*Required field. This is the name of the NCOS. (**Note**: You can create unnamed NCOS using the Text console but they are not supported in the Web console. If you encounter an unnamed NCOS, use the Text console to name it.)	Maximum 15 alphanumeric characte rs.

Field	Description	Values
(Network options)	There are twelve network options on the system. They are listed here. Yo u select any combination of the opti ons to enable them for this NCOS. Mailboxes that are assigned this N COS will have the selected network options enabled. Clear an option to d isable it.	Select any combination of the following twelve network options: • Enable GCOS check across network • Allow user to make network messages • Allow user to make urgent network messages • Allow user to give network messages • Allow user to give urgent network messages • Allow user to answer network messages • Allow user to answer urgent network messages • Automatic receipt on network messages • Set "Remote message" when playing network messages • Allow user to make fax messages over the network • Allow user to give fax messages over the network • Allow user to answer fax messages over the network

26.94.14 Configure a Network Class of Service

To create or modify an NCOS by adding and deleting network messaging features:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(N) Network COS**.
2. Select **(C) Current NCOS** and enter the **number**(1-64) of the NCOS that you want to create or modify.
3. Select**(N) Name NCOS**and enter a descriptive **name**for the NCOS, possibly one that describes the NCOS user group.
4. If you want to view the networking features that you can add to an NCOS, press **(H) Help NCOS**.
5. Select **(A) Add features**.
6. At the **Feature to add** prompt, enter the **numbers**(1-12) of the NCOS features that you want to add. You can enter an individual feature number, a comma-separated list, or a range, such as 2-4.
7. If you want, you can view the NCOS to verify your work. Press **(R) Report NCOS** and enter the number of the NCOS you created. The system displays the NCOS information.
8. If necessary, make further changes to the NCOS by adding or deleting features. When you are finished, exit to the System Configuration Menu to save your work.

26.95 Configuring Network Mailboxes

This section describes NP Net mailbox maintenance: creating network mailboxes, adding network mailboxes to distribution lists, and working with broadcast mailboxes over the network. The information here is an addition to the mailbox information in the Mailboxes section.

Creating Network Mailboxes

There is very little difference between a regular mailbox and a network mailbox. A regular mailbox becomes a network mailbox when you associate it with a network class of service (NCOS) that allows messaging across the network. Network Class of Service is described in Configuring the Network Class of Service.

Unless you specify otherwise, all mailboxes are assigned NCOS 1. To make administration easier, you should configure NCOS 1 to match the needs of the largest group of network users.

If you enabled GCOS checking across the network (NCOS feature 001), you must pay special attention to the GCOS that you assign to each mailbox so that the mailbox owner can communicate with the appropriate people.

Modifying Existing Mailboxes for Networking

When you add NP Net software to a NuPoint Unified Messaging server that is already processing calls, the default NCOS that was assigned to all mailboxes becomes effective. To change mailbox NCOS assignments on one mailbox or on a range of mailboxes.

Adding Network Mailboxes to Distribution Lists

If you maintain any distribution lists from the console, such as system-level distribution lists, you can add remote mailboxes to those lists. You add remote mailboxes from the console using the same letters as the dialing plan: N and P. When adding members to a distribution list, enter N and a remote mailbox number (just like a user would enter the number when addressing a message), or P and a prefix and mailbox number.

Any remote mailbox entries that you put in distribution lists must match the dialing plan and Node Access Table configuration.

Broadcasting over the Network

A Broadcast mailbox (mailboxes with FCOS bit **122**) functions differently when broadcasting to remote mailboxes:

- FCOS bit **123**, which directs the system to announce the broadcast mailbox number/name to the recipient, rather than the sender's mailbox number/name, does not work when the message is sent to a remote node.
- Messages made for a broadcast mailbox are automatically sent to every member of distribution list 01 of that mailbox. Local and remote mailboxes can be included in this distribution list. Distribution lists are limited to 200 members, and each local or remote mailbox in the list counts toward that limit.
- The same system will not perform a "double broadcast," that is, if one of the child mailboxes is also a broadcast mailbox, the message will *not* be sent to the mailboxes in its distribution list 01.

- If a remote broadcast mailbox is included in distribution list 01 of the local broadcast mailbox, the message *will* be broadcast to the remote mailbox's distribution list 01, since each broadcast is done by a different system.

Message Queues and the Mailbox Message Count

The mailbox Limits Class of Service limits the number of messages that can be stored in a mailbox. The maximum number of messages allowed is **200** (note that attachments to a message count toward this total). Network messages that are queued but have not been sent count toward this limit, and so do message receipts. You must take these additional demands on mailbox message storage into account when programming network queue configurations and when assigning Limits Classes of Service to network mailboxes.

26.95.1 Network Billing

This section describes the mailbox billing counters and the parts of the standard billing report that reflect NP Net usage. Refer to the Software Configuration section for instruction to adjust billing rates and run the billing report.

Network Message Counters

Network message counters tally the number of messages sent by a mailbox to remote nodes. Different counters measure the total number of network messages sent, the number of nodes to which a message is sent, number of remote recipients to which a message is sent, and the number of network messages received by the mailbox during the billing period. Separate totals are kept for urgent and batch messages that meet each of these criteria.

Network messages sent

This counter keeps track of the total number of batch messages recorded for remote mailboxes during the billing period. A "Give + comments" message is counted as one message, as is an original message that has an answer or answers attached.

Messages are billed on a "per message" basis, *not* a "per recipient" basis; when a batch message is made to a distribution list, or by using the "make multiple" feature, it counts as one network message sent.

Network urgent messages sent

This counter keeps track of the total number of urgent messages sent to remote nodes by the mailbox during the billing period. A "Give + comments" message is counted as one message, as is an original message that has an answer or answers attached.

Messages are billed on a "per message" basis, *not* a "per recipient" basis; when an urgent message is made to a distribution list, or by using the "make multiple" feature, it counts as one urgent network message sent.

Number of network nodes sent to

The Make Multiple and Broadcast features permit users to send a single message to more than one node. This counter allows the administrator to charge separately for each node to which a batch message is sent, since each destination node requires a separate transmission. The number of recipient mailboxes on each node does not matter. For example, a single message that is broadcast to five mailboxes on three different nodes increments this counter by 3.

A "Give + comments" message is equivalent to the single message in the previous paragraph, as is a "Give + message with an answer or answers attached."

Number of network nodes sent urgent to

The Make Multiple and Broadcast features enable users to send a single message to more than one node. This counter allows the administrator to charge separately for each node to which an urgent message is sent, since each destination node requires a separate transmission. The number of recipient mailboxes on each node does not matter. For example, a single message that is marked urgent, then sent to five mailboxes on three different nodes increments this counter by three.

Number of network recipients sent to

The Make Multiple and Broadcast features permit users to send a single message to more than one remote mailbox. This counter allows the administrator to charge separately for each remote mailbox to which a batch message is sent. The number of nodes is irrelevant. For example, a single batch message sent to five mailboxes on three different nodes, increments this counter by 5.

Number of network recipients sent urgent to

The Make Multiple and Broadcast features enable users to send a single message to more than one remote mailbox. This counter allows the administrator to charge separately for each. For example, a single message that is marked urgent, and then sent to five mailboxes on three different nodes increments this counter by 5.

Network messages received

This counter keeps track of the number of batch messages received from remote nodes by the mailbox during the billing period. A "Give + comments" message is counted as one message, as is an original message that has an answer or answers attached.

Network urgent messages received

This counter keeps track of the number of urgent messages received from remote nodes by the mailbox during the billing period. A "Give + comments" message is counted as one message, as is a original message that has an answer or answers attached.

Network Message Length Counters

Message length counters keep track of the total amount of recorded speech that fits certain criteria. Every mailbox has these counters, and all counters are incremented in tenths of a minute.

Among the reasons why an administrator would set rates based on message lengths are (1) messages use up disk storage when they wait in the queue, and (2) the longer the message, the longer the transmit time. While the cost of transmitting a single two minute message may not be significantly higher than the cost of transmitting a single one minute message, the cost differences can be substantial when they are multiplied over many messages.

There are separate message length counters for Batch and Urgent messages. Batch messages usually stay in the queue longer than urgent messages, but urgent messages may be transmitted during time periods when transmission charges are highest. Take these factors into account when setting rates.

Message length for network messages sent

The counter tallies the total amount of recorded speech in all batch messages sent to remote nodes by the mailbox during the current billing period.

Message length for network messages sent urgent

The counter tallies the total amount of recorded speech in all urgent messages sent to remote nodes by the mailbox during the current billing period.

Message length for network messages received

This counter totals the amount of recorded speech in all batch messages received from remote nodes during the current billing period.

Message length for urgent network messages received

This counter totals the amount of recorded speech in all urgent messages received from remote nodes during the current billing period.

Message length for number of network nodes sent

NP Net multiplies the amount of recorded speech in each batch message by the number of remote nodes to which the mailbox sends the message. The results are recorded by this counter.

Message length for number of network nodes sent urgent

NP Net multiplies the amount of recorded speech in each urgent message by the number of remote nodes to which the mailbox sends the message. The results are recorded by this counter. The number of recipients on each node does not count here.

Message length for number of remote recipients sent

NP Net multiplies the amount of recorded speech in each batch message by the number of remote mailboxes to which the mailbox sends the message. The results are recorded by this counter. The number of different remote nodes is irrelevant here; two messages for the same remote node are equivalent to one message for two different remote nodes.

Message length for number of remote recipients sent urgent

NP Net multiplies the amount of recorded speech in each urgent message by the number of remote mailboxes to which the mailbox sends the message. The results are recorded by this counter. The number of different remote nodes is irrelevant here; two messages for the same remote node are equivalent to one message for two different remote nodes.

Network Billing Report Entries

The billing report includes the charges accrued by network messaging. When no charges have accumulated for a counter, the entry does not appear on the billing report.

MAILBOX: 402 ID: A.G. Bell

GROUP: GCOS 1 FCOS 1: UNLIMITED base rate

$ 5.00

$ .40 40 user messages received

$ 2.30 23 caller messages received

$ .00 0 call placements sent

$ .00 0 future deliveries sent

$ 2.60 13 urgent messages sent

$ .00 0 tas messages received

$ 1.20 24 number of receipts requested

$ 4.10 41 greetings played

$ 3.50 72 times logged in

$ 9.60 9.6 user connect time

$ 1.70 3.4 caller connect time

$ .00 0 call placement time

$ 1.80 .09 disk usage

$ 5.40 18 messages sent to nodes

$ 6.00 6 urgent messages sent to nodes

$ 3.21 32.1 .1 minutes sent network urgent

$ 5.84 116.8 .1 minutes sent over network

$ 1.40 14 messages received from nodes

$ .50 1 urgent messages received

$ 2.36 94.5 .1 minutes rcvd over network

$ 1.26 6.3 .1 minutes rcvd network urgent

Total Charges = $ 58.17

26.95.2 NP Net Reports

The **Text Console** of NuPoint UM servers can provide reports on all aspects of NP Net configuration for NP Net TCP/IP.

When you complete NP Net programming for the first time, or when you update the configuration, print the reports showing the configuration. Confirm the changes and communicate them to the customer, then leave a copy on site for technicians servicing NP Net in the future.

The available reports are:

- Digits Translation Report
- Node Access Table Report
- Network Queues
- TCP Network Status

Each time that you request one of these reports you are given the option to view these reports on the system console or your terminal connection, send them to a specific serial port, or put the information in a file.

The Digits Translation Report

This report displays each node prefix and associated node number that has been programmed into the Digits Translation Table. The Digits Translation report has the following format:

```
 >>>
Denver NuPoint Voice <<<

PREFIX/NODE PAIR REPORT

Wed Mar 10 11:35:48 20XX

Prefix Node Absorb Cnt

700 700 3

801 801 3

802 802 3

803 803 3

804 804 3

805 805 3

807 807 3

7 Prefixes found
```

The Node Access Table Report

The Network Node Table stores the access string and hardware type of each remote node on the system. This information enables the originate link of the local node to establish communications with the other nodes on the system.

The Node Table Report shows the node number, node name, access code (string), hardware type and access status (enabled or disabled) for every node that was entered into the Network Node Table.

```
>>> Denver NuPoint Voice <<<

NODE ACCESS TABLE REPORT

Wed Mar 10 11:32:36 20XX

NODE NAME PROTO STRING HARDWARE ACCESS ENCODING

700 davebell TCP 10.37.52.130 0 = ETHERNET Y NMS

801 grace TCP 10.39.37.110 0 = ETHERNET Y G.711

802 luna TCP 10.39.37.69 0 = ETHERNET Y G.711

803 ibm3250 TCP 10.39.37.4 0 = ETHERNET N G.711

804 toronto TCP 10.39.37.100 0 = ETHERNET Y NMS

805 mango TCP 10.39.37.68 0 = ETHERNET Y G.711

806 mstclust TCP 10.39.37.145 0 = ETHERNET Y G.711

807 Thomas TCP 10.39.37.121 0 = ETHERNET Y G.711

8 Nodes found

/usr/vm/log/tmp_ShL.0A1 (END)
```

Network Queue Parameters Report

The Network Queue Menu, accessed from the reports menu, has two entries, Report Queue Parameters and Dump. "Dump" is a utility that is used only by service personnel. The Queue Parameters report shows the current network queue configuration. The report for the default configuration is as follows:

Batch Urgent

Weekday start time (hh:mm) 12:00 am 12:00 am

Weekday stop time (hh:mm) Never Never

Weekend start time (hh:mm) 12:00 am 12:00 am

Weekend stop time (hh:mm) Never Never

Message count threshold 1 0

Waiting time threshold (minutes) 5 0

Total message minutes threshold 0 0

Limits

Message blk use threshold (percent) 80

Max call setup tries 50

Call retry interval (minutes) 10

Max age for a message in queue No Limit

Press any key to continue....

Network Queue Dump

This real-time dump report is valuable when debugging NP Net delivery problems. It lists all current messages in the network queue. Each remote node is displayed separately, and batch and urgent deliveries are separated.

BATCH QUEUE:

URGENT QUEUE:

QUEUE SUMMARY:

Total Nodes: 0 Total Msgs: 0 Total Frames: 0

Press any key to continue....

26.95.3 Network Statistics Reports

Two statistics reports give comprehensive pictures of network usage. These reports are available from the Network Usage Report Menu, which is a sub-menu of the Statistics Menu (*not* the Network Reports menu).

The Network Usage Report

The Network Usage Report gives 15 minute "snapshots" of network message activity for a specified reporting period. This reporting period can be any hour, or range of hours, from the current day or the previous 6 days.

>>> Denver NuPoint Voice <<<

NETWORK USAGE 15min REPORT

Mon Dec 4, 20xx 7:58 pm

12/04/XX 8hr-17hr --- minutes interval ---

MESSAGE DAY=01 HOUR=08 00-14 15-29 30-44 45-59 AVERAGE

BATCH IN QUEUE 0 0 0 0 0

URG IN QUEUE 0 0 0 0 0

BATCH MAX LENGTH 0 0 0 0 -

URG MAX LENGTH 0 0 0 0 -

BATCH LATENCY H:M:S 0:00:00 0:00:00 0:00:00 0:00:00 -

URG LATENCY 0:00:00 0:00:00 0:00:00 0:00:00 -

BATCH DELIVERED 0 0 0 0 0

URG DELIVERED 0 0 0 0 0

TOTAL UNDELIVERED 0 0 0 0 0

BATCH RECEIVED 0 0 0 0 0

URG RECEIVED 0 0 0 0 0

Reading the Network Usage Report

The report heading shows the node name, the report name, the date and the time that the report was run.

The first line of the report shows the date and time interval during which the data were gathered.

A hyphen (-) in any column means the system was not processing messages during the report period (there was a power failure, or the system was taken offline for maintenance, for example). A zero in any column means the system was operable, but there was no activity.

MESSAGE DAY = 03, **HOUR =** 11 indicates that the data displayed immediately below were gathered on Wednesday, during the hour between 11 and 12 am. 00-14 indicates that data in that column were gathered during the first fifteen minutes of the hour; 15-29 refers to the second 15 minutes of the hour, etc.

AVERAGE is the average value of the four 15-minute samples. If a hyphen appears, in place of a numerical value, it means that the data have not yet been gathered. For example, if the report is run at 3:30 pm, and the report interval is for hours 12-15 (noon to 3 pm) of the same day, the entries for hour 15 (3 to 4 pm) will all be hyphens.

BATCH IN QUEUE is the total number of batch (non-urgent) messages and receipt updates present in the network queue during the time period.

URG IN QUEUE is the total number of urgent messages in the network queue during the time period.

BATCH MAX LENGTH is the total number of minutes of recorded speech in the network batch queue during the time period.

URG MAX LENGTH is the total number of minutes of recorded speech in the urgent network queue during the time period.

BATCH LATENCY is the maximum number of seconds that a message remained in the batch network queue during the time period.

URG LATENCY is the maximum number of seconds that a message remained in the urgent network queue during the time period.

BATCH DELIVERED is the total number of batch messages that were delivered to their destination nodes during the time period. (Receipt updates do not count here.)

URG DELIVERED is the total number of urgent messages that were delivered to their destination nodes during the time period.

TOTAL UNDELIVERED is the total number of messages (batch and urgent) that were rejected by their destination nodes during the time period. (Receipt updates do not count here.)

The Network Usage Summary Report

The Network Usage Summary Report gives peak (maximum) and total statistics for network message activity during a specified reporting period. This reporting period can be any hour, or range of hours, from the current day or from the previous 6 days.

```
                        >>>
Denver NuPoint Voice <<<

                        NETWORK
USAGE SUMMARY REPORT


                              Mon
```

```
Dec 4, 20XX  8:08 pm

12/04/XX  8hr-17hr


Day
1       <------------PEAKS----------><------------TOTALS---------->

NETWORKING:   IN
QUEUE   MINUTES   LATENCY
DELIVERED   UNDELIV  RECEIVED

BATCH:               0         0   0:00:00         0         0         0

URGENT:              0         0   0:00:00         0         -
```

0

Reading the Network Usage Summary Report

The report heading shows the node name, the report name, the date and the time that the report was run.

Each section is preceded by the date and time during which the data were gathered.

PEAKS - Statistics are for maximum activity during the reporting period. Although separate statistics are kept for batch and urgent message queues, these statistics are not broken down by destination node; that is, urgent queue statistics refer to urgent messages accumulated for every node on the network.

A hyphen (-) in any column means the system was not processing messages during the report period (there was a power failure, or the system was taken offline for maintenance, for example). A zero in any column means the system was operable, but there was no activity.

BATCH IN QUEUE is the maximum number of batch (non-urgent) messages and receipt updates present in the network queue at any time during the time period.

URGENT IN QUEUE is the maximum number of messages, marked urgent by the sender, that were present in the network queue at any time during the time period.

BATCH MINUTES is the maximum number of minutes of recorded speech from batch messages and receipt updates present in the network queue during the time period.

URGENT MINUTES is the maximum number of minutes of recorded speech from urgent messages present in the network queue during the time period.

BATCH LATENCY is the maximum number of seconds that a single message remained in the batch network queue during the time period.

URGENT LATENCY is the maximum number of seconds that a single urgent message remained in the network queue during the time period.

TOTALS - Data is a summary of activity during the reporting period

BATCH DELIVERED is the total number of batch messages that were delivered to their destination nodes during the time period. (Receipt updates do not count here.)

URGENT DELIVERED is the total number of urgent messages that were delivered to their destination nodes during the time period.

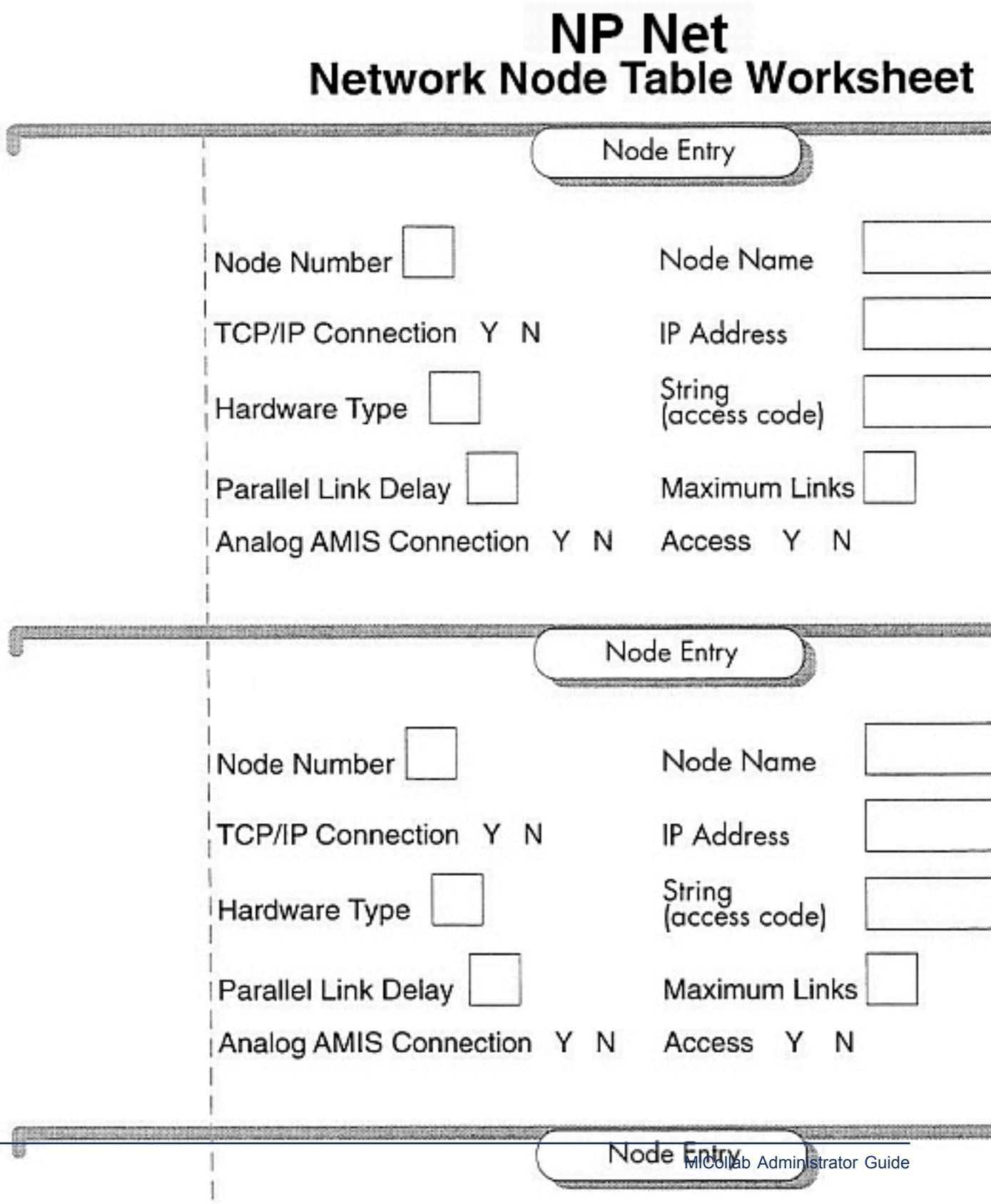
BATCH UNDELIVERED is the total number of batch messages that were rejected by their destination nodes during the time period. (Urgent messages are always delivered.)

BATCH RECEIVED is the total number of batch messages that were received from other nodes during the time period. (Receipt updates do not count here.)

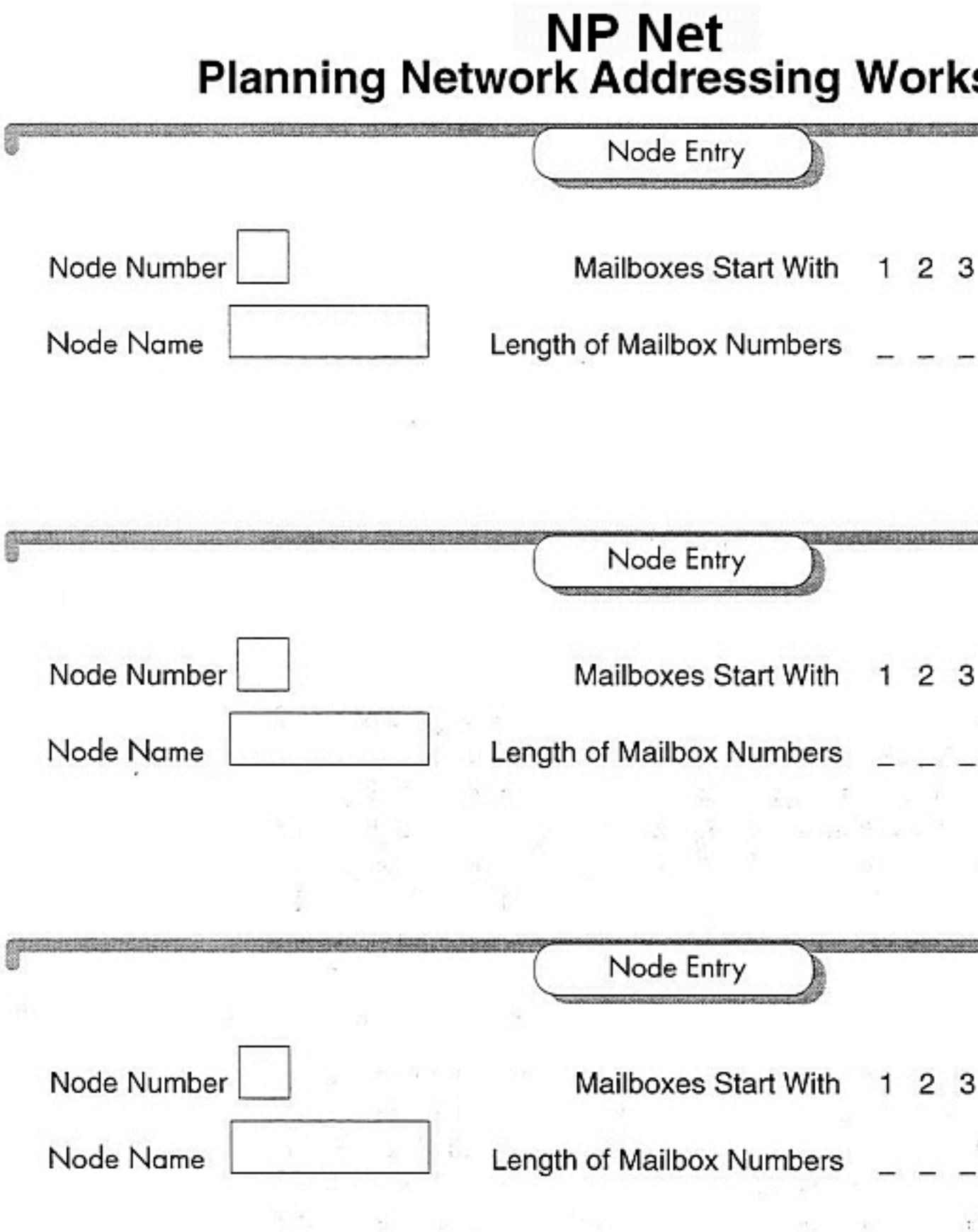
URGENT RECEIVED is the total number of urgent messages that were received from other nodes during the time period.

26.95.4 Worksheets - NP Net

Network Node Table Worksheet



26.95.5 Network Addressing Planning Worksheet



26.95.6 Network Queues Worksheet

The Network Queues Worksheet is designed to help you plan and record the settings of the network queues. The fields on the worksheet match the information that you must supply when configuring the queues. Study the sample worksheet and the definitions that follow, and then copy the blank worksheet and fill it in.

NP Net
Network Queues

Network Queue Limits

Message Block Use Threshold (80-100%): 90

Maximum Call Setup Tries: 4

Call Setup Retry Interval (minutes): 10

Network Queue Time Windows

Always Open? Weekdays Weekends

Weekday Start Time (hour:min am/pm): Batch _____

Weekday Stop Time (hour:min am/pm): Batch _____

Weekend Start Time (hour:min am/pm): Batch 9:00

Weekend Stop Time (hour:min am/pm): Batch 4:00

Network Queue Thresholds

Message Count Threshold: Batch 10 Urgent 2

Message Waiting Threshold: Batch 10 Urgent

Total Message Minutes Threshold: Batch 9 Urge

Worksheet Definitions: Network Queue Thresholds

Network queue thresholds allow you to control when messages are sent to another node. Cost is an important consideration when setting these parameters; the first minute of a call is tariffed higher, so it is more economical to send a group of messages than to send each message separately

You can set different network queue thresholds and time windows for urgent and batch messages. (All messages not specifically marked urgent by the sender are considered batch.) With this two-tiered system, routine messages are sent at a time when the call is more economical, while more important messages are delivered promptly. (It is recommended that you set realistic batch limits or restrict the assignment of Network Classes of Service that allow the user to send urgent messages over the network to prevent users from marking all remote messages urgent.) The batch queues and remote queues of each remote node are monitored individually by NP Net.

Message Count Threshold: The number of messages, names, greetings, and receipt updates that must be waiting in a queue for a certain node before that queue becomes ready to send. This threshold is appropriate for sites where users tend to make frequent, short messages. The default message count threshold for batch messages is 5; for urgent messages, it is 0.

Message Waiting Threshold: The length of time, in minutes, that the oldest message will be kept waiting in the queue before the queue becomes ready to send. If the queue has a very restrictive time window (for example, if batch messages can be sent only between 12:00 am and 5:00 am), set this threshold to a low value to ensure that all network queues are ready to send when the window opens. The default message waiting threshold for batch messages is 10 minutes; for urgent messages, the default is 0 minutes (no waiting).

Total Message Minutes: The number of minutes of speech that must be waiting in a queue for a certain node before that queue becomes ready to send. This threshold is appropriate for systems where system storage tends to be high, but it is not triggered efficiently by frequent, short messages. If the node tends to process a high volume of short messages, the message count threshold is a better choice. The default Total Message Minutes threshold for batch messages is 5 minutes of speech; for urgent messages, the default is 0 minutes of speech.

Worksheet Definitions: Network Queue Time Windows (Start/Stop Times)

The start and stop times create a limited time period during which messages can be sent to remote nodes. This time window overrides all message thresholds; queues that are ready to send will not trigger a call unless the window is open. Conversely, when the time window opens, queues that have not yet met any of the thresholds will not be sent. The time window and thresholds must be carefully set, to ensure that messages do not remain queued for an unacceptable period of time.

You set separate time windows for batch and urgent messages. Within these categories, you set time windows for weekdays and weekends. In the default configuration, network queue time windows for batch and urgent messages are always open.

Always Open: Circle Weekdays or Weekends for either urgent or batch queues if you do not want message sending to be restricted by time of day.

Weekday Start Time: Write in the time of day that you want the local node to start sending messages on weekdays, provided that at least one of the network queue thresholds has been met.

Weekday Stop Time: Write in the time of day that you want the local node to stop sending messages on weekdays.

Weekend Start Time: Write in the time of day that you want the local node to start sending messages on weekends, provided that at least one of the network queue thresholds has been met.

Weekend Stop Time: Write in the time of day that you want the local node to stop sending messages on weekends.

Worksheet Definitions: Network Queue Limits

Network queue limits control network queue storage and determine how often, and at what interval, a node should attempt to send a network queue to another node before the queue is considered "undeliverable."

Message Block Use Threshold: The percentage of total queue storage that must be full to trigger an automatic connection. The Message Block Use Threshold is a "safety valve" that forces the node to empty queues when total network queue storage is almost full.

When the message block use threshold is reached, the system checks the network queues for the node with the greatest number of messages waiting and marks that queue as ready to send. The queue is sent immediately; the message block use threshold overrides all other thresholds, including network queue time windows. The system will continue to send queues until message storage falls below the threshold.

You can set the message block use threshold at any value between 80% and 100%. The default threshold is 80%.

Maximum Call Setup Tries: The maximum number of calls that an originating node will make to try to establish a connection with another node. The default value is 50.

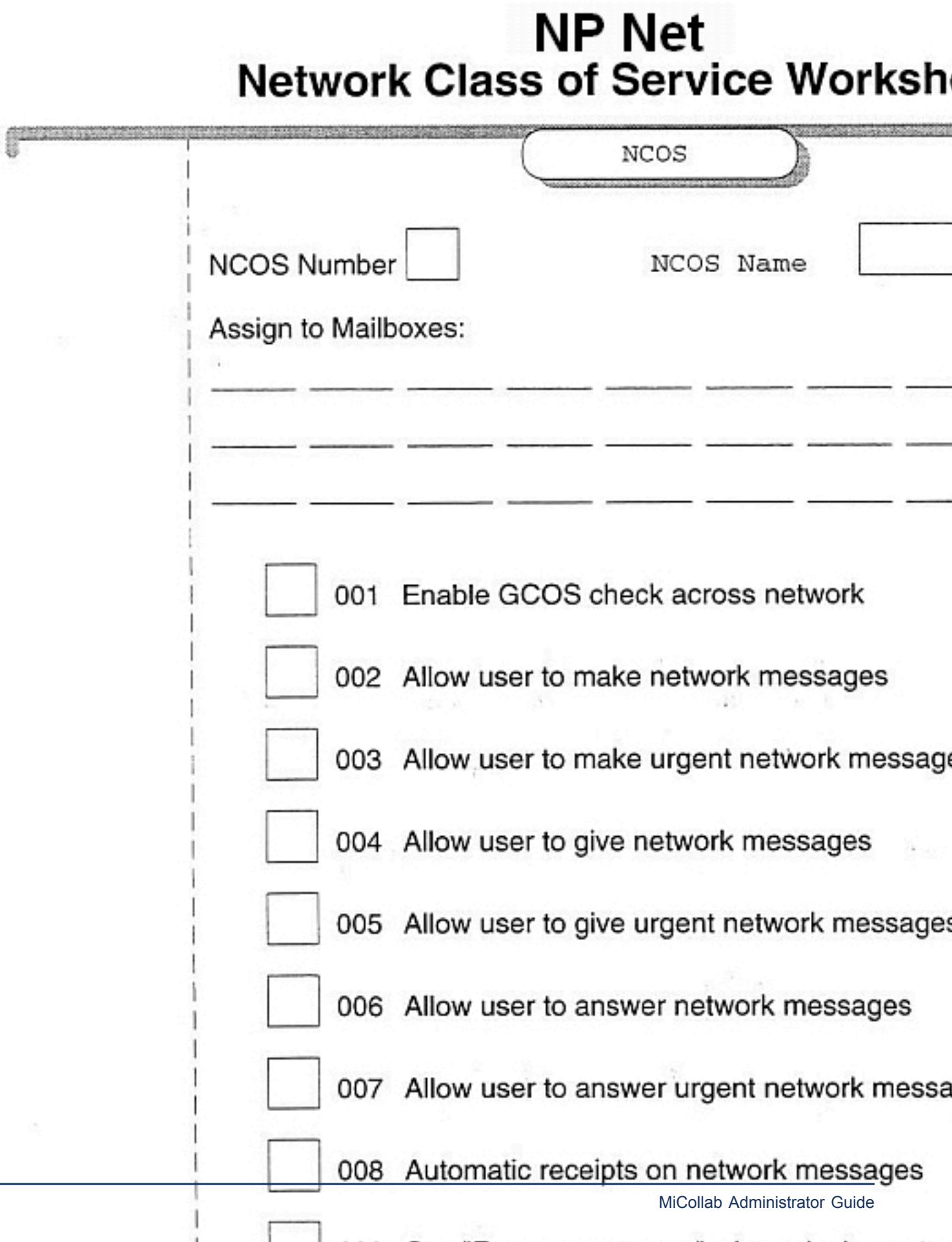
Call Setup Retry Interval: The time, in minutes, between attempts to establish a connection. The default interval is 10 minutes.

An originate link executes the originate actions of the hardware type up to three times in immediate succession when attempting to call another node. These three calls constitute one try; that is, the call setup tries counter is increased only after all three attempts have failed.

When a first attempt at originating a call fails (the node may be busy communicating with another node on the system, for example), the node waits the amount of time specified by the call setup retry interval before repeating the originating actions. This sequence will continue until communications are established or the maximum call setup tries threshold has been reached.

If all attempts to communicate with the destination node fail, all users who sent messages to that node are notified that these messages could not be delivered.

26.95.7 Network Class of Service Worksheet



NP Net
Network Class of Service Worksh

NCOS

NCOS Number ☐ NCOS Name ☐

Assign to Mailboxes:

_____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____

☐ 001 Enable GCOS check across network

☐ 002 Allow user to make network messages

☐ 003 Allow user to make urgent network message

☐ 004 Allow user to give network messages

☐ 005 Allow user to give urgent network messages

☐ 006 Allow user to answer network messages

☐ 007 Allow user to answer urgent network messa

☐ 008 Automatic receipts on network messages

26.96 NP OnDemand - Description

Note:
NP OnDemand programming must be done using the **Text Console**.

NP OnDemand is an optional feature that offers carriers and organizations the opportunity to provide their customers or subscribers with temporary mailboxes created at the time there is a need for a caller to leave a message. Mailboxes created on demand can be deleted after an administrator-determined period of time.

Mailboxes on demand inherit the characteristics of a template mailbox that is used as a model. Although an NP OnDemand mailbox could have all the features of a permanent mailbox, the features available to a subscriber are usually limited to playing, keeping, and deleting messages, much like a hotel mailbox.

The following scenario illustrates a typical implementation of NP OnDemand:

Jay makes a telephone call to Celia at her cellular number. When Jay calls, Celia is not able to answer (she's on another call, has her phone turned off, or is out of the service area). Although Celia does not have a regular mailbox with RF Mobilenet, her cellular service, RF Mobilenet has taken a leap ahead of its competition by establishing NP OnDemand as a special benefit to its subscribers. When Celia doesn't answer, Jay hears a greeting that the system administrator has recorded in the template mailbox:

The party you have called is not available. Please leave a message at the tone.

NuPoint Voice instantaneously creates a mailbox for Celia identified by her cellular telephone number, and Jay leaves his message. If he does not terminate the message by hanging up, he hears

Thank you.

NP OnDemand then sets a message waiting indicator for Celia. Whether Celia calls in to NuPoint Voice or she is notified by message delivery, she hears

You have one unplayed message.

Celia then hears the message automatically if message auto-play is a feature assigned to the template mailbox, or she hears

Press P to play the first message.

If Celia receives no other messages during the day, Jay's message and her mailbox are deleted at the nightly purge. If Celia does not retrieve her message within the time limit specified in the LCOS for mailboxes on demand, both accumulated messages and the mailbox are similarly deleted at the next scheduled purge.

26.96.1 NP OnDemand - System Requirements

NP OnDemand makes no special hardware requirements on NuPoint Voice systems.

With respect to NuPoint Voice software:

- NP OnDemand works with all Mitel integrations. The mailbox number is the called number provided by the integration.
- NP OnDemand complements NuPoint Voice features defined by FCOS, and does not in any way alter their operation.
- A mailbox created on demand requires the same account space as a regular mailbox. If a large number of NP OnDemand mailboxes are allowed to persist, a system could run out of account sectors.
- NP OnDemand **cannot** be used with NP Forms or NP Net.

26.96.2 Billing and Statistics

Billing statistics are tabulated for existing mailboxes on demand by a gather, the same as for any regular mailbox. This characteristic of mailboxes on demand and gather with respect to regular billing procedures has two effects that you should be aware of:

- NP OnDemand mailboxes that are active when the gather is run are included in the billing report.
- NP OnDemand mailboxes that have been purged are not included in the billing report.

26.96.3 Configure Call Detail Recorder for NP OnDemand

Note:
Call Detail Recorder is enabled through the **Text Console** only.

Call Detail Recorder features that define an NP OnDemand mailbox are **Call Type 11** (Mailbox Purge) and **Access Type 40**. A CDR record is generated for mailboxes on demand for the following activities:

- Mailbox created, including time and date
- Message received, including time and date; shows the number of unplayed, played, and urgent messages
- Message played, including time and date; shows the number of unplayed, played, and urgent messages
- Mailbox deleted, *n* unplayed messages (could be zero) , including time and date
- Number of minutes a subscriber was logged in to an NP OnDemand mailbox

You must configure CDR in order for call information about NP OnDemand mailbox creation and deletion to appear in CDR reports.

- Enable modules and lines as required by your installation.
- Include **Call Type 11**.

A **Call Type 11** in CDR record field 13 indicates that an NP OnDemand mailbox has been deleted during the scheduled purge.

An **Access Type 40** in CDR field 14 indicates an NP OnDemand access.

26.96.4 NP OnDemand - Configuration Requirements

Switch Configuration

The switch or PBX to which your NuPoint Voice system is connected must be programmed to forward the telephone number or extension for calls that will be handled by NP OnDemand to the NuPoint Voice system rather than treating them as RNA or busy.

Line Groups

NP OnDemand is configured on a line group basis. Define the line groups and assign the lines you want to use for NP OnDemand.

FCOS

Note: Because NP OnDemand is configured on a line-group basis, each line group must have its own template mailbox.

Customize an FCOS for the template mailbox that will be used as the model for mailboxes on demand.

Required FCOS Features

1. **Feature bit 255**: Delete mailbox without unplayed messages. Mailboxes on demand are identified by this feature, which causes those mailboxes without unplayed messages to be deleted at the nightly purge. The FCOS you create for the NP OnDemand template **must** include feature bit 255.
2. **Feature bit 001**: Login to mailbox. Without this feature, users will not be able to log into their NP OnDemand mailboxes and retrieve messages.
3. **Feature bit 218**: Passcode not needed on direct calls. Because NP OnDemand assigns a random passcode when the mailbox is created, users will not be able to retrieve their messages unless this feature is included

Note:
Take care when assigning features to the NP OnDemand template. When an NP OnDemand mailbox is created, it cannot be differentiated from any other mailbox, and it will make available to its owner all features contained in the template.

The table below offers an example of other features that might be included for an NP OnDemand mailbox. The actual features granted to an NP OnDemand mailbox are left to your discretion.

Feature No.	Feature Name
001	Login to mailbox
010	English Language prompts
039	Notification tone when new msg arrives

Feature No.	Feature Name
041	Receive messages from outside callers
047	Notification prompt when new msg arrives
050	Play messages
052	Auto-play unplayed messages
056	Auto-Discard messages
058	Play unplayed messages in FIFO order
088	Receive urgent messages
218	Passcode NOT needed on direct calls
255	Delete mailbox without unplayed messages

LCOS

Create an LCOS to be assigned to mailboxes on demand. In the Message Retention Limit Menu, set desired values for Played Message Retention and Unplayed Message Retention. The default value for Played Message Retention is 672 hours and for Unplayed Message Retention, 336 hours.

A value of zero in the Played Message Retention field causes an NP OnDemand mailbox that had no unplayed messages to be deleted at the next nightly purge. A value of 24 hours in the Unplayed Message Retention field would give the mailbox owner at least one full day to retrieve unplayed messages.

You must set values for length of message retention in order for NP OnDemand to be effective. If the default values for message retention are left unchanged, then an NP OnDemand mailbox is effectively permanent.

Determine the Message Waiting Type

In order for NP OnDemand to be effective, users who are not accustomed to receiving messages must be notified when they have a message waiting. You must therefore decide which message waiting type is appropriate for your application of NP OnDemand.

Same MWI as Regular Mailboxes

If subscribers who will be beneficiaries of mailboxes on demand can be informed about the new service and instructed how to respond to an MWI light or stutter dial tone, then you can use the same message waiting type as you do for your regular NuPoint Voice users.

NP OnDemand also has the capability to dial out to your subscribers and notify them of waiting messages by message delivery.

Notification by Message Delivery

NP OnDemand makes use of the pager function to call a subscriber and tell the subscriber that a message is waiting. To enable this feature when you create the template mailbox:

1. Define either message waiting type #1 or message waiting type #2 as **5**, or Pager.
2. If you already have message delivery enabled on your system, then just enter the appropriate pager access type in the template mailbox.

3. If you do not have message delivery enabled, you must set up a line group for out-dialing and define a pager access type.

> **Note**:
> Leave the pager number field blank. NP OnDemand places the mailbox owner's number in this field.

4. Set message delivery attempts and interval as required.

26.96.5 Create a Template Mailbox

This section describes how to create a template mailbox, then set it up and prepare it for use. General considerations for creating and setting up the template mailbox are discussed first; detailed instructions follow the general considerations.

Template Mailbox Security

In order to ensure security of the template mailbox, Mitel recommends that, once you have created a template mailbox, you change its number to one that is *not* in the dialing plan so that callers cannot leave messages in it or inadvertently log into it. Further, you should assign a nontrivial passcode to the mailbox so that you can log into it to perform maintenance as needed.

Setup and End User Introduction

You can record speech in the template mailbox if you wish; for example:

- A generic greeting that all callers will hear when they reach a person without a mailbox.
- A "name" that the NP OnDemand mailbox owner will hear when the owner logs into the mailbox to retrieve messages.
- From the administrator's mailbox, a welcoming message or invitation to become a regular mailbox owner.

Mitel suggests that, if you wish to record speech in the template mailbox, you use the following procedure:

- Create a template mailbox *in* the dialing plan.
- Record name, greeting, and message as desired.
- Change the mailbox number to one *not* in the dialing plan.

Creating and Setting up the Template Mailbox

1. Create a mailbox named "NP OnDemand Template" within the dialing plan.
2. Assign your custom OnDemand FCOS and LCOS to the NP OnDemand Template mailbox, and assign your selected Message Waiting Type.
3. Log into the NP OnDemand Template Mailbox and record a name (for example, "RF Mobilenet") and a greeting that callers will hear when they leave a message for someone without a regular mailbox.

4. Log into the Administrator's mailbox and record a message to the NP OnDemand Template mailbox. Do not play this message. It will be the first message NP OnDemand mailbox owners hear when they log in to retrieve their messages. (This message might be an introduction of NuPoint Voice or a promotional message urging your subscribers to get their own personalized mailboxes.)

   If someone responds to this message by pressing A, that response will go to the Administrator's mailbox, not to the NP OnDemand Template mailbox.
5. Change the NP OnDemand Template mailbox number to one that it is *not* in the dialing plan.
6. Configure NP OnDemand by modifying the active configuration from the on-line menu:

   - in the Text console Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, **(E) Active Configuration**, and then **(B) NP on Demand Menu**.

   If NP OnDemand is ON for callers, then forwarded calls are treated the same way as they are for a regular mailbox. If NP OnDemand is on for users, then they are treated the same way as the owner of a regular mailbox, except that they are logged in to the NP OnDemand mailbox automatically. When NP OnDemand is on for either callers or users, account space is required.

   If NP OnDemand is OFF for either callers or users, then a call (from whichever category is OFF) is treated as if NP OnDemand were not installed.

Who	ON/OFF	Effect
Callers	ON	On call forward, callers hear the NP OnDemand greeting.
	OFF	On call forward; callers hear the general greeting.
Users	ON	On direct call to the pilot number, users are logged in to NP OnDemand and hear the NP OnDemand greeting.
	OFF	On direct call to the pilot number, users hear the general greeting.

7. Select **(C)** and enter Y to turn on NP OnDemand for callers.
8. Select **(U)** and enter Y to turn on NP OnDemand for users.
9. Select **(M)** and enter the number of the NP OnDemand Template mailbox.
10. Run a Configuration Report (from the Reports menu of the Text Console) to verify that the correct Template Mailbox number has been assigned to NP OnDemand, and that NP OnDemand is installed and turned on for callers and users.

26.97 NP RapidDial - Description

Note:
NP RapidDial must be configured using the **Text console**.

NP RapidDial is an optional feature that allows users to enter an abbreviated phone number to address mailboxes on a NuPoint Unified Messaging system.

NP RapidDial uses a table to map a subscriber group of abbreviated mailbox numbers to the complete mailbox numbers on the NuPoint Unified Messaging system. For example, mailbox numbers in a Subscriber Group might be seven digits long, but NP RapidDial allows you to use only part of each mailbox number to make and send a message or create a distribution list. Members of a Subscriber Group must use a complete phone number to address messages to mailboxes outside of their Subscriber Group.

To install NP RapidDial, follow the instructions for Installing an Optional Feature.

26.97.1 Configuration Requirements NP RapidDial

This section provides the information required to configure the NP RapidDial feature on a NuPoint Unified Messaging system.

After you install NP RapidDial, you must:

- Determine Subscriber Groups
- Configure a variable dialing plan for the Line Group
- Create a Features Class of Service (FCOS) for NP RapidDial
- Create the NP RapidDial Table
- Configure Mailboxes for NP RapidDial

Determine Subscriber Groups

NP RapidDial can only be used to address messages to mailboxes within a Subscriber Group. The NP RapidDial Table defines the groups of subscribers and lists the mailbox numbers in each group.

The NP RapidDial Table separates mailbox numbers into two parts, the prefix and the suffix. The prefix consists of the leading digits in the mailbox number. The suffix consists of the remaining digits in the mailbox number and becomes the NP RapidDial address for the mailbox. For example, the following parameters might appear in the NP RapidDial Table:

Prefix length:	**5**
Suffix length:	**2**

Prefix:	**23422**
Suffix range:	**10-99**

In this example, mailbox numbers in the Subscriber Group use seven-digit numbers that begin with a five-digit prefix of 23422 and end with a two-digit suffix in the range of 10 through 99. With NP RapidDial, members of this Subscriber Group can address messages to another mailbox in this group by entering only the last two digits of the mailbox number.

Configuration Requirements for Prefixes and Suffixes

NP RapidDial mailbox numbers can include up to 11 digits. The prefix can include up to nine digits. In the preceding example, the Subscriber Group supports 90 phone numbers.

Note: When defining a Subscriber Group, make the suffix large enough to identify all phone numbers in the Subscriber Group.

You can add several prefixes and suffixes to a subscriber group, however, ranges of suffix numbers cannot overlap.

Configure a Variable Dialing Plan for the Group

In order for the NP RapidDial feature to function, you must set the line group dialing plan for variable length mailboxes. For information about configuring the dialing plan, refer to Configure a Dialing Plan.

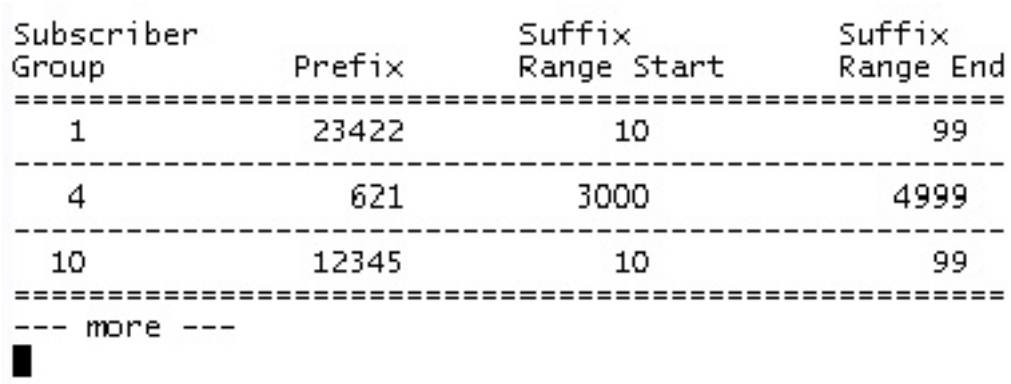
With a variable length dialing plan, the voice mail system uses a timeout to determine when data entry is complete. With NP RapidDial, the user enters as few as two digits or as many as 11 digits. Then, the user either waits for the system to time out or presses the pound (#) key to indicate that data entry is complete.

Create a Features Class of Service (FCOS) for NP RapidDial

To enable NP RapidDial, customize an FCOS that contains feature bit **265** (Enable NP RapidDial Features).

26.97.2 Create the NP RapidDial Table - Overview

The NP RapidDial Table (shown below) maps each NP RapidDial number to its complete mailbox number. This table shows the Subscriber Groups and the mailbox numbers associated with each Subscriber Group. All mailbox users in a Subscriber Group can dial a partial mailbox number to access another mailbox in that group. The same users must dial a complete phone number to reach any mailbox not included in their Subscriber Group.



To create the NP RapidDial table:

1. From the Main menu, select **(M) Mailbox maintenance** and then **(T) NP RapidDial Table Utility Maintenance**.
2. In the RapidDial Table menu, use the configuration menus as described in each of the following sections:
3. **(A) Add new records**
4. **(C) Clear NP RapidDial table**
5. **(D) Delete existing records**
6. **(E) Export NP RapidDial table**
7. **(I) Import NP RapidDial table**
8. **(P) Purge Subscriber Group**
9. **(R) Report all Subscriber Groups**
10. **(V) View Subscriber Group**

26.97.3 (A) Add New Records

To add a new record to the NP RapidDial Table, select **A** from the NP RapidDial Table menu. After you create or modify the NP RapidDial Table, save a copy of the table with the Export NP RapidDial table menu option.

The following table shows you how to add a new Subscriber Group record to the NP RapidDial Table (using Subscriber Group 10 as an example).

Prompts	Example of User Input	Comments
Enter Subscriber Group (1-1000):	**10**	**Assign a Subscriber Group ID of 10.**
Subscriber Group 10 does not exist. Create new Subscriber Group 10? (Y/N)	**Y**	**Begin creating Subscriber Group 10.**

Prompts	Example of User Input	Comments
Enter prefix length:	**5**	**Sets the first five digits of the phone number as the prefix.**
Enter suffix length:	**2**	**Sets the last two digits of the phone number as the suffix.**
Enter prefix:	**12345**	**Sets all phone numbers in this group to begin with 12345.**
Enter suffix range (start-end):	**10-99**	**Sets all phone numbers to end with a number from 10 through 99.**
Enter prefix:	**Enter**	Enter another prefix or press **Enter** to end.
Enter Subscriber Group (1-1000):	**Enter**	Enter a new Subscriber Group or press **Enter** to end.
1 record(s) added.	**Enter**	**A notification appears that the group was created.**

When creating a Subscriber Group, the following rules apply:

- Mailbox numbers in Subscriber Groups can be up to 11 digits.
- The prefix can be a maximum of nine digits.
- The suffix is the NP RapidDial number that group members will use to access mailboxes in their Subscriber Group.

In the example above, the mailbox numbers are set at seven digits with five digits in the prefix and two digits in the suffix. All mailboxes numbers have the prefix 12345. Members of Subscriber Group 10 can use the two-digit suffix to address messages to other mailboxes in the group. For example, the user for mailbox 1234510 can press 99 to address a message to mailbox 1234599.

26.97.4 (C) Clear NP RapidDial Table

To delete all data in the NP RapidDial Table, select **C** from the NP RapidDial Table menu. Do this only if the NP RapidDial Table is corrupt, recently entered data is not valid, or if you need to replace the table with another NP RapidDial Table. Clearing the NP RapidDial Table lets you restore a valid, previously saved version with the Import NP RapidDial table option, described later in this section.

The following table shows you how to clear all records from the NP RapidDial Table.

Note: Use the password “RdtUtil” for all functions that delete data from the NP RapidDial Table.

Prompts	Example of User Input	Comments
Please enter the passcode:	**RdtUtil**	**RdtUtil is the passcode. It is case sensitive.**
Do you really want to delete all entries in the rapid dial table? (Y/N)	**Y** or **N**	
NP RapidDial Table cleared.		

26.97.5 (D) Delete existing record(s)

To delete the record for a single Subscriber Group from the NP RapidDial Table, select **D** from the NP RapidDial Table menu. The following table shows you how to delete a single record from a Subscriber Group (using Subscriber Group 10 as an example).

Prompts	Example of User Input	Comments
Enter Subscriber Group	**10**	**Delete Subscriber Group 10.**
Subscriber Group: nn Number of record(s) : nn Prefix length nn, Suffix length nn		
Enter prefix:	**12345**	
Enter suffix range (start-end):	**10-99**	
Prefix Suffix Range Start Suffix Range End nn nn nn Do you want to delete above record? (Y/N)	Y	
Record deleted.		

Prompts	Example of User Input	Comments
Enter Subscriber Group (1-1000):		

26.97.6 (E) Export NP RapidDial Table

To export and save a copy of the NP RapidDial Table, select **E** from the NP RapidDial Table menu. You can use the export option to back up the current NP RapidDial Table before you modify it. The following table shows you how to export the current NP RapidDial Table. The NP RapidDial Table is automatically saved when you back up the server, but you cannot selectively restore the NP RapidDial Table, only.

Note:
At the prompt, enter a file name. You can enter a full path and file name to store the file in any directory on the hard disk or storage media. The export option uses the .rdt extension.

Prompts	Example of User Input	Comments
Enter export filename:	**<filename>**	**Enter a name for the saved file. If you enter the name of an existing file, that file is overwritten and its contents are lost. To save the file to floppy disk, enter a full path name in the following format: /fd0/<path><filename> If you do not specify a path, the file is stored in this location: /usr/vm/config/<filename>.rdt**
Export file <filename> is created		

26.97.7 (I) Import NP RapidDial Table

To import an NP RapidDial Table from storage media or from another directory, select **I** from the NP RapidDial Table menu. When you import a file, the program searches for the specified file in the “/usr/vm/config” directory. To import a file from another directory or storage media, you must include a path in the file name. Do not specify an extension. NP RapidDial automatically appends .rdt as the extension.

Only new records are imported into the NP RapidDial Table. An existing record is not affected unless a command in the import file deletes that record in the current NP RapidDial Table. To import a completely new table, first clear [option (C)] the current NP RapidDial Table, then import the replacement table.

Import files are text files. You can edit these text files in a text editor and insert the following commands before importing the file:

- **add** inserts a record in the NP RapidDial Table. If a record overlaps or is redundant, the add command fails and an error message appears.
- **del** removes a record from the NP RapidDial Table. If the record does not exist, an error message appears. You can delete an existing record with the del command and then insert a replacement record with a subsequent add command.
- **end** stops the import process. It must appear at the end of the imported data.

For example, a text file for import might include:

These commands:	...cause these changes in the NP RapidDial t able:
add 5,622,2100	Creates Subscriber Group 5 with prefix 622 and suffix 21 00
add 25,345,5000-6999	Creates Subscriber Group 25 with prefix 345 and suff ixes from 5000 through 6999
add 300,7954,100-550	Creates Subscriber Group 300 with prefix 7954 and su ffixes from 100 through 550
del 4,621,3000-4999	Removes Subscriber Group 4 with prefix 621 and suffi xes from 3000 through 4999
add 4,621,5000-5050	Creates Subscriber Group 4 with prefix 621 and suffixes from 5000 through 5050
end	Ends the import process

The following table shows you how to import an NP RapidDial Table.

Prompts	Example of User Input	Comments
Enter import filename:	<file name>	Enter the path and file name to imp ort. Do not specify the default .rdt ext ension in the filename. Records with settings that overlap existing reco rds in the current NP RapidDial Tabl e are not imported. To import the file from another directory, specify a ful l path name in the following format: / fd0/<path><filename> If you do not specify a path, the program searche s for the file in the default directory: / usr/vm/config/
n records added, n records deleted, 1 failed.		The number of imported records a ppears as n records added. If the im port file includes redundant records, an error message appears. Each err or increments the “failed” counter.

26.97.8 (P) Purge Subscriber Group

To remove a Subscriber Group from the NP RapidDial Table, select **P** from the NP RapidDial Table menu. The table below shows you how to purge a Subscriber Group (using Subscriber Group 10 as an example).

Prompts	Example of User Input	Comments
Enter Subscriber Group (1-1000):	10	Purge Subscriber Group 10.
Please enter the passcode:	RdtUtil	The passcode is case sensitive.
Do you really want to remove Subscr iber Group 10? (Y/N)	Y	
Subscriber Group nn with nn record(s) deleted.		
Enter Subscriber Group (1-1000):		Enter a new Subscriber Group num ber or press Enter to exit.

26.97.9 (R) Report on all Subscriber Groups

To obtain a report of the Subscriber Groups in the NP RapidDial Table, select **R** from the NP RapidDial Table menu. You can view the report on the console or save it to a file. The following table shows you how to obtain an NP RapidDial Table report.

Prompts	Example of User Input	Comments
DISPLAY RAPID DIAL TABLE ME NU (C) Display to console (F) Output to file (X) Exit		Option **C** sends the report to the console screen. Option **F** sends the report to a file. Option **X** exits this function.
Subscriber Suffix Suffix Group Pref ix Range Start Range End ======= ========== nn nn nn nn	C	If you select C, a report appears on the console. This display shows 24 lines at a time. To continue scrolling, press the space bar or to scroll a s ingle line, press Enter.
Enter filename:	F <file name>	If you select F, you must specify a full <path> and <filename>. If you do not specify a path, the program uses the .rpt extension to save the report to this location: /usr/vm/config/<filen ame>.rpt
Total of nn tables and nn records s tored to file /usr/vm/config/<filena me>.rpt		After the file is saved, a message similar to this appears on the conso le.

26.97.10 (V) View Subscriber Group

To see a specific Subscriber Group in the NP-UM RapidDial Table, select **V** from the NP-UM RapidDial Table menu. You can view the prefix, suffix range start, and suffix range end for the selected Subscriber Group.

The following table shows you how to view a Subscriber Group (using Subscriber Group 10 as an example).

Prompts	Example of User Input	Comments
Enter Subscriber Group (1-1000):	10	View Subscriber Group 10.
Prefix Suffix Suffix Range Start Range End ========== == nn nn nn		The record for the Subscriber Group appears on the console in a format similar to that shown on the left.
Enter Subscriber Group (1-1000)		Enter a new Subscriber Group to view or press Enter to exit.

26.97.11 Configure Mailboxes for NP RapidDial

Before the NP RapidDial feature can be used, each mailbox must be assigned to a Subscriber Group.

To configure mailboxes to use the NP RapidDial feature:

1. Modify a mailbox (or range of mailboxes) with the following settings:

   - an FCOS that contains feature bit **265** (Enable NP RapidDial Features)
   - a Subscriber Group number (this prompt appears only if feature bit 265 is assigned to the mailbox FCOS)

26.98 NP Receptionist - Description

Note:
This feature must be configured using the **Text Console**.

NP Receptionist is a software product that functions as an automated attendant, typically within an integrated NuPoint Unified Messaging server and PBX system. NP Receptionist can perform the following tasks:

- Pick up an incoming call and greet the caller
- Allow the caller to dial an extension
- Screen a call
- Connect the caller to an intermediate attendant (a person to screen calls or take messages)

- Transfer a caller to a voice mailbox

When a call comes in, NP Receptionist takes the call, then transfers the call, as required. NP Receptionist can make blind, supervised, or screened transfers.

- **Blind transfer:** The system releases the call (“hangs up”) after dialing the extension; used for transferring to extensions that do not have a mailbox on the system.
- **Supervised transfer:** The system stays online until the caller gets through to the desired extension. If the extension is busy or rings but does not answer (referred to as Ring No Answer (RNA) in the rest of this guide), NP Receptionist pulls back the call and the caller can choose to leave a message in the called party's mailbox, or be transferred to another extension.
- **Screened transfer:** NP Receptionist asks for the caller’s name, then notifies the called party about the call and the called party can choose to accept or reject the call. Again, if the call is rejected, the caller can leave a message in the called party’s mailbox or be transferred to another extension. These options are configured by the system administrator.

Operation

The system administrator configures the way NP Receptionist initially answers a call. The administrator then enters call processing instructions for individual mailboxes. NP Receptionist checks these instructions when directing a call to the mailbox and handles the call according to these instructions.

26.98.1 NP Receptionist Features

NP Receptionist has the following features:

Console Attendant Functions

NP Receptionist can answer incoming calls, screen them, dial an extension for the caller, or play menu options for the caller.

NP Receptionist can also allow direct access to an extension directly and/or call forwarding to a mailbox without NP Receptionist assistance.

Day/Night Greetings

You can record separate customized greetings for day answering and night answering. You can configure hours and days that comprise “Day” and “Night/Weekend” to suit the requirements of the individual installation. NP Receptionist can handle “day” calls differently from “night” calls.

Configurable Prompts Languages

System prompts are available in English (American, Australian, New Zealand, UK), French, German, Japanese, Korean, Mandarin, Spanish, Mexican Spanish, and Portuguese.

Automatic Outdialing to Trunks

When callers dial an internal extension number, NP Receptionist can automatically route the call to an outside number (for example, a modem number).

Call Screening/Automatic Announcement for Users

Mailbox users can choose to have all their calls screened. A mailbox user who calls another mailbox user can press the star (*) key, plus his or her own mailbox number, in reply to the prompt “Whom may I say is calling?” NP Receptionist automatically announces the name that is recorded in the mailbox. If the call is not answered (or is rejected by the user), any message that is left is recorded from the caller’s mailbox. This allows the recipient to answer the message simply by pressing the 2, or A (for answer), key.

Flexible Rerouting of Calls

When a call does not go through, users can have their calls routed to a personal attendant’s number, to the Console Attendant, or to their personal mailboxes; or they can choose to have NP Receptionist play one of four redial menus. You can choose different routings for Busy, Ring No Answer, and Rejected calls (for calls to extensions), and call failure (for calls to trunks).

Customized Treatments for Individual Users

You can group together call processing options to make up to 16 “treatment types,” or call processing instructions, that allow an administrator to provide users with the call processing options that they want. Treatments types are stored in the mailbox data file, and the administrator can easily change a treatment type.

Separate Day and Night/Weekend Call Treatments for Individual Users

Each mailbox can store separate Day and Night/Weekend treatment types. NP Receptionist checks the user’s mailbox for the correct treatment type before processing an incoming call.

Directory/Menu Capabilities

You can use mailboxes with “tree” class of service to build directories or menus which direct outside callers to the appropriate extension or mailbox within the system. The tree mailbox can allow the user to access a “chain” mailbox, which plays a mailbox greeting, then prompts the caller to enter an extension number.

Single-Digit Access

You can configure this menu capability so that after the main greeting plays, NP Receptionist allows single-digit access to selected departments and specific extensions.

Dial-by-Name

NP Receptionist can allow users to reach an extension by pressing keys that spell a person’s name. You can configure the feature so that the caller can dial by last name or first name dial by last name or first name.

Dial Around

The # dial around feature allows the caller to act as his/her own receptionist. For example, after leaving a message for one user, the caller can press # (the pound key), and then dial another number when prompted.

Logging Into Your Mailbox

NP Receptionist is a layer of programming that functions on top of the NuPoint Voice application. If you call a number answered by NP Receptionist, you can dial an extension. In addition, you can reach the NuPoint

Voice message center by pressing # (the pound key) to leave a message in a mailbox. You can also log into your mailbox from the NuPoint Voice message center by pressing # (the pound key) again, followed by your mailbox number; alternatively, you can dial your mailbox number, followed by # (the pound key) to log into the mailbox.

26.98.2 Call Flow and Call Processing

Typical Call Transfer

A caller dials the company main number, Receptionist picks up the call and greets the caller, then asks the caller to dial an extension. The caller dials the extension. NP Receptionist then transfers the call. Typically NP Receptionist supervises the transfer - NP Receptionist stays on the line until the called party answers the phone, then releases the call (hangs up).

If the extension has no associated mailbox, NP Receptionist releases the call as soon as the caller dials the extension.

Leaving a Message

NP Receptionist allows the user to dial an extension. If the called party is not available, NP Receptionist gives the caller an option to leave a message.

Screened Transfer

NP Receptionist asks the caller for his/her name, then notifies the called party about the call and the called party can choose to accept or reject the call. Again, if the call is rejected, the caller can leave a message in the called party's mailbox or be transferred to another extension. The options available to a caller (transferring to another extension or leaving messages in mailboxes) are configured by the system administrator.

You can configure NP Receptionist to process a call through an intermediate attendant. NP Receptionist dials the intermediate attendant, who screens the call.

Caller Waits or Dials "0"

If the system allows the caller to reach a person (for example, a console attendant) the caller reaches the person by dialing 0 or waiting, rather than dialing an extension.

Converting an Extension Number to a Mailbox Number

When a caller dials an extension, NP Receptionist converts the extension number to the associated mailbox number, checks the mailbox for instructions, then dials the extension or trunk number that is stored in the mailbox.

If the mailbox numbers are the same as the extension numbers, then NP Receptionist can simply check whether the extension has an associated mailbox. However, a system might require NP Receptionist to convert an extension number-to-mailbox number using the following steps, in the order shown:

1. Delete leading digits, if applicable.
2. Add signed value in offset table, if applicable.

Example

Extension: 3975

For all extensions starting with 3, delete 1 digit

Leading digit deleted: 975

For all extensions starting with “3,” the offset value is -100

Add signed offset value to 975: 975 + (-100)

Mailbox number is 875

For more detailed information on Delete Digit and Offset tables, see Dialing Plan Options.

The flowchart below shows extension-to-mailbox number conversion:



Dialing an Extension

After NP Receptionist validates an extension number and its associated mailbox, NP Receptionist dials the extension number. If screening is not in place, the caller will pick up the call or NP Receptionist will fail to connect the call because of one of the following situations:

- Reorder tone – fast busy tone indicating that switching paths are busy. Depending on the PBX specifications, NP Receptionist is configured to treat the reorder tone as one of the following situations:
    - Dead line
    - Busy
    - Ring No Answer

The administrator can configure the NP Receptionist response, which can take the caller to an attendant, allow the caller to dial another extension, leave a message, or select from a menu that lists the options just mentioned.

Mailbox Call Processing

Each mailbox stores call processing instructions. To simplify mailbox programming, the administrator can enter up to 16 groups of call processing instructions, or treatment types, into the system configuration file. When creating a mailbox, an administrator can use these treatment types to configure separate day and night instructions that best match the choices of the mailbox owner.

Single-Digit Access Menus

You can configure NP Receptionist to present the caller with a menu of options that the caller can access by pressing a single digit. For example, Receptionist II might greet the caller as follows: “Thank you for calling ABC company. Press 1 to dial an extension, press 2 to reach Technical Support, press 3 to reach the Job Hotline.”

26.98.3 NP Receptionist Configuration Overview

Typically, NP Receptionist functions as a layer of programming within an integrated system. This means that you assign a line group to the integration software and configure NP Receptionist parameters within the same line group. Occasionally, an integration might require that you configure Receptionist separately from the application. In this case, as in an in-band integration, the integration instructions direct you to assign NP Receptionist to a separate line group. In either case, the NP Receptionist configuration parameters are the same, whether you reach the Receptionist Menu through the integration software line group or through a line group specifically assigned to NP Receptionist.

Parameter Groups

NP Receptionist instructions, or parameter values, fall into three main groups.

- **Line group assignment**: index number, name, and number of lines in the line group. (See About Line Groups.)
- **Messaging functions**, or the **handling of greetings and messages** from callers. The line group uses the same information that is provided for the NuPoint Voice application, which is discussed in the NuPoint Voice section.
- **Call processing functions**: The administrator sets call processing instructions for NP Receptionist. Configuration instructions are included in the Procedures folders of this section.

  NP Receptionist Configuration

26.99 Dialing Plan Options

This section discusses the dialing plan for the automated attendant functions of NP Receptionist. If NP Receptionist is integrated with the PBX system, then this dialing plan must match the PBX dialing plan.

The mailbox dialing plan for messaging functions is discussed in About Dialing Plans.

(P) Dialing Plan = [4,4,4,4,4,4,4,0,0]

(D) Delete Digits = [0,0,0,0,0,0,0,0,0]

(F) Offset Table

(T) Timeout for Receipt of First Digit (.1 seconds) = [0]

(Y) PBX Console Attendant Day Access Code = [0H]

(Z) PBX Console Attendant Night Access Code = [0H]

PBX Dialing Plan

The dialing plan controls the extension numbers that an outside caller dials to reach a user. A caller reaching NP Receptionist hears the prompt, “Please enter an extension number, or wait for assistance.” When the caller enters a number, NP Receptionist checks the input against the PBX dialing plan.

If the number conforms to the PBX dialing plan, NP Receptionist proceeds to delete any leading digits and add any offsets that are specified (see “Delete Digits Table and Offset Table” later in this section). NP Receptionist then checks the mailbox dialing plan.

If the result is a valid mailbox number, NP Receptionist checks the mailbox data file, and dials the “Mailbox’s Extension Number” set up by the administrator. The call is then processed according to the instructions configured for that mailbox.

If the result is not a valid extension, NP Receptionist dials the number that was originally input by the caller, then hangs up.

The dialing plan is a string of nine numbers. The first number in the string shows the number of digits allowed for extensions that begin with 1. Each number that follows gives the number of digits allowed for extensions that begin with 2 through 9.

A “V” at any position indicates that the number of allowable digits (can have up to eleven) for that position is variable; NP Receptionist accepts any extension input with that particular leading digit. The system uses a three-second timeout to determine when input is finished.

Dialing Plan Example

0,4,3,3,3,A,V,0,0

The values indicate the number of digits allowed for extensions starting with digits 1 through 9. The sample dialing plan is interpreted as follows, for extensions that begin with the numbers listed:

- 1–no extensions starting with “1”
- 2–must have four digits (for example, 2112)
- 3 through 5–must have three digits (for example, 303, 415, 504)
- 6–”A” makes “6” the dial-by-name access digit
- 7– the number of digits is variable (for example, 798, 7734, 765379)
- 8 and 9–no extensions start with 8 or 9

If the PBX dialing plan is 3,3,3,3,3,3,3,0,0, all extensions that begin with digits 1 through 7 must have three digits. No extensions start with the digits 8 or 9. This disallows pressing 8 or 9 to dial out from NP Receptionist; in addition, the Administrator mailbox number (default, 998) and Attendant mailbox number (default, 999) cannot be reached from NP Receptionist.

Delete Digits Table and Offset Table

Ideally, extension numbers are identical to the mailbox numbers within a system. For instances where they do not match, NP Receptionist must convert extension numbers to mailbox numbers, using values contained the Delete Digits Table and the Offset Table.

Delete Digits Table

The delete digits table is a string of numbers that represent, from left to right, extension numbers that begin with 1 through 9. The number shown at each position indicates the number of digits that NP Receptionist must delete from an extension to convert it to a mailbox number.

The digits are deleted in the order received. For example, if the number in the Delete Digits table is 2, NP Receptionist deletes the first two digits that it receives.

Example

If the delete digits table is 0,0,0,1,0,0,0,3,0

- No leading digits are deleted from extensions that begin with 1, 2, or 3 (that is, they are unchanged)
- One leading digit is deleted from all extensions that begin with 4 (for example, 4657 becomes 657)
- Extensions that begin with 5, 6, or 7 are unchanged
- Three leading digits are deleted from extensions that begin with 8 (for example, 8657 becomes 7)
- Extensions that begin with 9 are unchanged

The default Delete Digits table is 0,0,0,0,0,0,0,0,0, which means that all extension numbers are passed through unchanged. If you need to make changes to this table, record the new table on NP Receptionist Worksheet 2 at the end of this section.

Offset Table

To complete the conversion of an extension number to a mailbox number, NP Receptionist can add an offset after deleting any leading digits. The offset can be positive or negative. Offset tables are numbered 1 through 9. The default values for each offset table is 0, as shown below. The table number refers to the leading digit of the extension number before any digits are deleted. Table 1 shows the offset to be added to extensions that begin with 1. If the extension is 1678, the offset value read is the one in Table 1, even if during the conversion, the leading digit might be deleted); Table 2 specifies the offsets for extensions that begin with 2; and so on.

- OFFSET: s
- Table offset for #1 = [0]
- Table offset for #2 = [0]
- Table offset for #3 = [0]
- Table offset for #4 = [0]
- Table offset for #5 = [0]
- Table offset for #6 = [0]
- Table offset for #7 = [0]
- Table offset for #8 = [0]
- Table offset for #9 = [0]

Offset Table

Example

For example, if the offset value for Table 5 is +25, the mailbox number for extension 560 (+25) is 585.

How NP Receptionist Uses These Tables

The following examples shows the process of transforming extension numbers to mailbox numbers:

Example 1

Assume

Delete Digits = 0,0,1,0,0,2,0,0,0

Table offset for #3 = -50

This means that NP Receptionist transforms an extension that begins with 3 to a mailbox number using the following procedure:

3275 (extension that was entered)

275 (delete one leading digit)

-50 (add signed offset from Table 3)

225 (mailbox number)

Under the same circumstances, extension “3276” is converted to mailbox number 226, “3280” is converted to mailbox number 230, etc.

Example 2

Assume

Delete Digits = 0,0,0,0,0,0,0,0,0

Table offset for #1 = 200

This means that any extension number that begins with 1 maps as follows:

17 (extension that was entered)

- (do not delete any leading digits)

+200 (add signed offset from Table 1)

217 (mailbox number)

Timeout for Receipt of First DTMF Digit

This is a timing parameter that the administrator can configure to allow a pause before NP Receptionist starts processing digits that a caller dials. The default timeout value is 0, indicating that the feature is turned off. The timeout value is a number between 0 and 50 in tenths of a second.

PBX Console Attendant Day/Night Access Code

The PBX console attendant day and night access codes usually contain a system attendant number to which a caller is transferred during the configured time period. NP Receptionist dials the appropriate string for the time period under the following circumstances:

- A caller waits for assistance before dialing an extension.
- A call fails to go through after the caller has entered an extension, assistance is required, and there is no attendant’s extension number in the mailbox data file.

Console access codes are PBX-dependent, and can be determined by actually transferring a call to the operator from a station set. The following table shows the coding choices available for day/night access:

Code	Meaning
0-9, *, #	**Numbers and characters on a standard DTMF keypad**
A through D	**Fourth column DTMF keys**
(	**Start pulse dialing**
)	**Stop pulse dialing; resume tone dialing**
T	**Wait for dial tone**
S	**Switch hook flash**
F	**Switch hook flash and wait for dial tone**
+	**Pause one second**
H	**Hang up (go on-hook)**

Note: Do not program a G (wait for greeting) into a PBX Console Attendant Day or Night Access Code, or into the Pre-DN string or Post-DN string; internal NP Receptionist programming does not allow a successful transfer if a G appears in any of these strings.

The default dial string is “0H,” for both the PBX Console Attendant Day Access Code and the PBX Console Attendant Night Access Code. This string means “issue DTMF zero, then hang up.” For most PBXs, this is sufficient to transfer the call to the Attendant.

The NP Receptionist day or night dialing access code proceeds in the following sequence:

- Execute the Pre Directory Number (Pre-DN) dial string that is set under “PBX Dial String Definitions”; the Pre-DN string usually contains all the instructions for the transfer.
- Dial the appropriate PBX console attendant access code
- Execute the Post Directory Number (Post-DN) string, then wait for a greeting (NP Receptionist programming always appends a G to the end of the Post-DN string after a PBX Console Attendant Access Code has been dialed).

The default day and night console access codes are blind transfers, which are available only if the PBX allows a blind transfer to the operator. A blind transfer means NP Receptionist releases the call before the greeting starts. Instructing NP Receptionist to release the call after dialing the number ensures that the PBX does not continue the transfer when the caller has decided to hang up.

If there is no PBX console attendant during the day, or during night/weekend hours, entering a period deletes the access code for that time period. When there is no access code, the caller who “waits” (in response to the prompt, “Please enter a mailbox number or wait”) is prompted to leave a message in the attendant’s mailbox. (NP Receptionist thanks the caller and hangs up if the attendant’s mailbox has also been deleted.)

26.100 Flow Options

The Flow Options parameters contain information about how Receptionist should handle given calls.

Mailbox Message Prompt Greeting/Name

The Mailbox Message Prompt value determines what message the caller hears if the called party is not available. If the default value of G (for greeting) is chosen, the caller hears the mailbox owner’s personal greeting. If N (for Name) is chosen, the caller hears the prompt, “Please leave a message for [name recorded in mailbox].” (If no name was recorded for the mailbox, the caller hears, “Please leave a message for [mailbox number].”)

PBX Console Operation

PBX Console Operation provides the option to specify that the initial welcome greeting be replaced by a short dial tone to prompt the operator that NP Receptionist is ready to receive the extension number.

PBX Console Operation is set to the default value of **N** when normal NP Receptionist call processing is desired.

CAUTION! Do not change the default unless you specifically want to replace greetings with a short dial tone.

26.101 PBX Dial String Definitions

NP Receptionist simulates the actions of a human console attendant. Since different PBXs have different console operator protocols, certain coding must be entered into the NP Receptionist configuration file to tell NP Receptionist how to process calls under all the possible conditions, using signals understood by the PBX.

Pre-programmed dial strings for several different PBXs can be selected from the Online Configuration Menu. If the PBX at the customer site is not shown on the menu, the dial strings must be programmed in the Default PBX Options Menu.

The easiest way to determine the proper coding for each dial string is to attach phone sets to three PBX extensions, one for the “caller,” one for the “called party,” and one for simulating the actions of the PBX console operator, then follow the steps that are given in the descriptions below.

Pre-Directory/Post-Directory Number Dial String

The “directory number” in the Pre-Directory/Post-Directory Number Dial String refers to the extension number associated with a mailbox number. The Pre-Directory Number Dial String puts the caller on hold so NuPoint Voice can dial the PBX attendant. The Post-Directory Number Dial String is the number or letter code that NP Receptionist dials after the extension has been dialed. The following table shows Pre-Directory/Post-Directory Number coding choices.

Code	Meaning
0-9, *, #	Numbers and characters on a standard DTMF keypad
A through D	Fourth column DTMF keys
(	Start pulse dialing
)	Stop pulse dialing; resume tone dialing
T	Wait for dial tone
S	Switch hook flash
F	Switch hook flash and wait for dial tone
+	Pause one second
H	Hang up (go on-hook)

Pre-Directory Number Dial String

The default Pre Directory Number (Pre-DN) dial string is “S+,” which tells the PBX to do a Switch hook flash, then wait one second before dialing the extension number (which may be a trunk number) that is in the mailbox. (Remember that NP Receptionist uses the Delete Digits table, and the Offset Table to transform the extension that is input by the caller into a mailbox number, and then dials the extension number that is stored in the mailbox’s data file.)

The Pre-DN string is also used with NP Receptionist Console Access Codes. **Before** the appropriate Console Access Code is dialed, NP Receptionist executes the Pre-DN string, then waits for the internally programmed greeting to be played.

Note:

- Do not program a **G** (wait for greeting) into the Pre-DN string; internal NP Receptionist programming does not allow a successful transfer to the console attendant if a G appears in this string.
- Do not program Feature Access Codes such as "Called Party Features - Override" into the Pre-DN string. To access this functionality, use the "Override" call flow action in Call Director.

Post Directory Number Dial String

The default Post Directory Number (Post-DN) dial string is “+,” which tells NP Receptionist to wait one second before taking any other action. This gives the PBX enough time to make the connection to the extension. If no Post -DN dial string is needed, enter a period.

The Post-DN string is also used with NP Receptionist Console Access Codes. After the appropriate Console Access Code has been dialed, NP Receptionist executes the Post-DN string, then waits for the internally programmed greeting to be played.

Note: Do not program a G (wait for greeting) or a T (wait for dial tone) into the Post-DN string; internal NP Receptionist programming does not allow a successful transfer to the console attendant if a G or T appears in this string.

When an H appears in the Post-DN string, every call that NP Receptionist makes is a blind transfer. NP Receptionist transfers the call without invoking treatment types, connect strings, or return strings.

Connect Dial String on Called Party Accept

NP Receptionist uses this dial string to connect a caller with the called party in the following situations:

- When call screening is not configured for the extension dialed
- When there is no mailbox associated with the extension dialed
- When a mailbox is configured for call screening, and the call is answered and accepted by the called party

There is no default for Connect Dial String on Called Party Accept, since the automatic release is usually sufficient to connect the caller with the called party. If a dial string is entered, but later it is necessary to reset the value to “no string,” entering a period erases the dial string.

Dial String for Return on Called Party Refused

This dial string is used to reconnect to the caller when call screening is in effect and NP Receptionist has successfully connected with the extension, but the called party has refused the call. The default Dial String for Return on Called Party Refused is “++,” which tells NP Receptionist to wait two seconds before doing anything else. The two second delay gives the called party time to hang up his/her phone. For most PBXs, this action is sufficient to reconnect the caller with NP Receptionist. If no dial string is needed, enter a period.

Dial String for Return on Called Party, Busy, or RNA

When NP Receptionist dials an extension, and the call does not go through because a busy or reorder tone is encountered, or because there is no answer, or because silence on the line indicates that the extension number is not valid, the Dial String for Return on Called Party Busy or RNA is used to tell the PBX to reconnect NP Receptionist with the caller. The default dial string is “S+,” which means that NP Receptionist issues a switch hook flash, and then waits one second before doing anything else. If no dial string is needed, enter a period.

Special Actions on Reorder Tone Encountered

This dial string tells NP Receptionist what to do when an extension is dialed, and a reorder tone is encountered.

- Some PBXs return a reorder tone when an extension is set to “Do Not Disturb.” If NP Receptionist is integrated with this type of PBX, enter “R” for the Special Actions on Reorder Tone Encountered dial string. When NP Receptionist receives a reorder tone, it returns to the caller, says “I’m sorry, [called party’s name] did not answer,” then follows the RNA treatment of the called party’s mailbox.
- A dial string can be entered to direct the call to an assistance number, or to a number where the caller can report that the extension is malfunctioning.
- If no string is found here, NP Receptionist treats the call like a dead line: the Dial String for Return on Failure to Connect is dialed and the caller is told, “That is not a valid extension number. Please enter another extension number.”

There is no default Special Actions on Reorder Tone Encountered dial string. If a dial string is entered, but later it is necessary to reset the value to “no string,” enter a period to erase the dial string.

26.102What is a Treatment Type?

Treatment types tell NP Receptionist how the user wants calls handled under different situations. Different treatment types can be specified for day and night answering. Any available treatment type may be chosen for either time period. If no treatment type is configured, the NP Receptionist default treatment is to play the mailbox greeting.

Individual treatment types belong to one of two categories: **extension** or **trunk**. NP Receptionist offers 16 extension and trunk treatment types, ten of which are defaults. The administrator can configure six additional treatments. The appropriate treatment type depends on the extension number of the mailbox.

- **Extension Treatment Types** are assigned to mailboxes when the mailbox’s extension number is expected to be answered by a person (rather than a machine). Extension treatment types tell NP Receptionist whether to screen calls. They specify the actions to be taken when
  - the extension rings, but there is no answer.
  - the extension is busy.
  - a screened call is rejected by the called party.
- **Trunk Treatment Types** are usually assigned to mailboxes that outdial to numbers that are not answered by a person (for example, non-dial 1 long distance services). There is less flexibility in how calls are processed. When the number is dialed, NP Receptionist
  - receives a response indicating that the connect criteria have been met; or
  - considers the call a failure, and follows the specified failure treatment.

You must determine the appropriate treatment type (extension or trunk) for the mailbox and choose, from that category, the day and night treatment types that best meet the user’s needs.

26.102.1 Extension Treatment Types

Extension treatment types consist of the following elements; all choices are determined by user preferences. Refer to NP Receptionist Treatments Report.

Call Screening Is/Is Not in Effect

When call screening is in effect, NP Receptionist (a) asks the name of every caller and puts the caller on hold, (b) calls the desired extension, (c) announces the name of the caller, and (d) gives the called party the opportunity to accept or reject the call.

System users can press the * key (star) and their mailbox numbers, when asked for their names; the system announces the names recorded in the mailboxes. If a message is left, it is made from the caller's mailbox (which enables the called party to answer it by pressing **A** while logged into his own mailbox).

RNA (Ring/No Answer) Treatment

The RNA treatment tells NP Receptionist what to do when an extension rings but no one answers it. The treatment options are described below.

RNA Treatment Options	
A	Caller is transferred to the attendant's extension numb er stored in the mailbox data file. If no attendant's extens ion number has been specified, caller is transferred to the Console Attendant.
M	Caller is prompted to leave a message in the called part y's mailbox.
R	The redial menu that is selected under "Redial Menu to Use" (Table 3-3) is played, and NP Receptionist follows the caller's instructions.

Busy Treatment

The busy treatment tells NP Receptionist what to do with incoming calls when the extension is busy. Choices are the same as the RNA treatment.

Reject Treatment

The reject treatment tells NP Receptionist what to do with screened calls that are rejected by the called party. Choices are the same as the RNA treatment.

Redial Menu to Use

When R (redial) is selected as the treatment for any of the failure conditions (RNA, Busy, or Rejected), "Redial Menu to Use" selects the redial menu to play and the associated action to perform. The menus are named for the action taken if the caller does not do anything. Choices are R (retry), M (message), A (assistance), and D (disconnect); the default value is M. The text of each menu is given below.

Redial Menu Options	
R	Press zero for assistance; Press "*" to hold for <called party's name>; Enter another extension number; or Wait to leave a message.
M	Enter another extension number; Press zero to return to the attendant; or Wait to leave a message.
A	Press "*" to leave a message; Enter another extension n umber; or Wait for assistance.

Redial Menu Options	
D	Press "*" to leave a message; Press zero to return to the attendant; or Enter another extension number. (Recept ionist hangs up after three tries.)

Authorized Periods

Access to a mailbox (and to its associated extension number) may be restricted to daytime hours or night/weekend hours only by using the authorized period. Callers who try to access a number at a time that is not within the authorized period hear the message, "I'm sorry, that number is not available for access at this time."

Authorization Codes

When a treatment type contains an authorization code, all callers must enter the code before NP Receptionist allows access to any extension or trunk with this treatment type. An authorization code is used under special circumstances (for example, to restrict access to a modem or to a WATS line).

Default Treatment Types

Ten treatment types are pre-programmed in the NP Receptionist configuration. These are extension treatment types that do not require authorization codes and do not specify authorized times. The default features are shown in the following table.

No trunk treatment types are pre-programmed into the default configuration because they tend to be site-specific. These treatment types can be modified by the system technician.

Default Treatment Types				
Treatment Type	**Ring/No Answer**	**Extension is Busy**	**Call is Refused**	**Call Screening?**
1	Play Redial Menu D	Play Redial Menu D	Play Redial Menu D	Yes
2	Play Redial Menu D	Play Redial Menu D	Not Applicable	No
3	Play Redial Menu A	Play Redial Menu A	Play Redial Menu A	Yes
4	Play Redial Menu M	Play Redial Menu M	Play Redial Menu M	Yes
5	Prompt caller to le ave a message	Prompt caller to le ave a message	Not Applicable	No
6	Prompt caller to le ave a message	Prompt caller to le ave a message	Prompt caller to le ave a message	Yes
7	Prompt caller to le ave a message	Play Redial Menu R	Prompt caller to le ave a message	Yes
8	Play Redial Menu R	Play Redial Menu R	Prompt caller to le ave a message	Yes
9	Play Redial Menu R	Play Redial Menu R	Not Applicable	No
10	Transfer caller to assistance number	Transfer caller to assistance number	Transfer caller to assistance number	Yes

Selecting a Treatment Type for a Mailbox

You can ask all users to choose from the pre-programmed default treatment types, or you can assign special treatment types that you or the technician create for your system. Run a Receptionist Treatment Types Report (Text console only) to display the features of the treatment types on your system.

26.102.2 Trunk Treatment Types

The technician programs two features: the connect criteria and the failure treatment. These features are unique to trunk treatment. Default trunk treatment types do not exist.

Connect Criteria

Connect criteria are the conditions when a trunk call is considered to successfully connect with the called party. The default value is C (cut through), which means that all trunk calls outdialed are considered successful. Other choices are T (the call is successful if it is answered by a computer tone or a dial tone) and R (the system knows that the trunk call has gone through if the receiving telephone rings). When you enter a trunk number in the extension number field, ensure that you know what conditions are necessary for connection.

Failure Treatment

The failure treatment tells NP Receptionist what to do with a trunk call if the connect criteria are not met. The user is given the choices listed in Extension Treatment Types.

26.102.3 Hidden (’Blind’) Mailbox Extension Number Programming

Dial strings to transfer to the mailbox extension number are contained in the pre-DN and post-DN dial strings that are programmed into the configuration by the technician.

NP Receptionist programming adds certain characters to the end of the mailbox extension number. These "hidden" characters depend on the mailbox’s treatment type:

- If the mailbox has an extension treatment type, NP Receptionist automatically appends a **G** (wait for a person or computer tone greeting) unless you insert an **H** (hang up) at the end of the dial string.
- If the mailbox has a trunk treatment type, the hidden character depends on the connect criteria chosen:
    - If the connect criteria is "Tone," a T (wait for dial tone) is appended.
    - If the connect criteria is "Ring," a special character that tells NP Receptionist to wait for a single ring is appended.
    - If the connect criteria is "Cut through," NP Receptionist checks whether the last character in the mailbox extension number is an H. If it is not, NP Receptionist automatically hangs up after it outdials the dial string.

26.102.4 Programming NP Receptionist to Dial an Outside Mailbox Extension Number

The "mailbox extension number" does not have to be a PBX extension number. Specific mailbox programming in NP Receptionist is used to allow callers to reach an outside number when they input an extension number.

EXAMPLE:A mailbox can be created to outdial to a Wide Area Telephone Service (WATS) line.

- Users who make long distance calls can access NP Receptionist and input the number of the mailbox.
- NP Receptionist automatically dials the numsber and connects dddthe user to the WATS line.

This programming offers the caller the convenience of dialing a shorter number. Additionally, this technique gives the administrator the opportunity to choose treatment types that restrict access to the WATS line by requiring an authorization code and/or requiring calls to be made during an authorized time period (see NP Receptionist Treatment Types).

When you want NP Receptionist to dial an outside number, you must program the system to duplicate the steps that a caller uses to dial that number. Enter certain codes in the mailbox extension number field.

EXAMPLE: Characters such as **T** (wait for dial tone) must be included in the extension number dial string and in the number itself.

A maximum of 15 alphanumeric characters can be entered in the mailbox's extension number field. If your dial string exceeds this number, you must use one of the extension pre-dial indexes that are programmed by the technician during configuration. (You may use these indexes even when the number does not exceed 15 characters.)

When you want NP Receptionist to outdial a number (other than a simple extension) when a mailbox is accessed, use the following procedure to program the number into the mailbox.

Step 1: Formulate a Coding String

The easiest way to formulate a coding string that directs NP Receptionist to outdial a number is to manually place a call to this number and note what steps were taken. Use codes from the following list to describe your actions:

0-9,#,*	Send out these DTMF tones (just as though they are b eing dialed from a standard touch-tone telephone)
A-D	Outdial these fourth column DTMF tones (keys are fou nd on special telephones)
T	Go offhook (equivalent to lifting the receiver on a stan dard telephone) and wait for a dial tone
(	Send the digits that follow as pulses (10 pps)
)	Stop pulsing digits; resume sending digits as DTMF t ones
+	Pause for one second
G	Greet - wait for a person or pager to answer
F	Switchhook flash and wait for dial tone

S	Switchhook flash (no wait required)

EXAMPLE A:

Company A has an account with a long-distance carrier that employees must use when placing long-distance calls. To outdial to this service, the administrator is instructed to set up a mailbox for each department. (Each department has a separate mailbox to enable billing counters to keep track of long-distance use by department.)

To program the mailbox extension number, the administrator places a call and notes the steps:

To access the long distance carrier, the administrator

1. Lifts the receiver and listens for a dial tone
2. Dials 9 to get an outside line
3. Dials the long-distance carrier number:**1-408-5556783,**
4. Waits for a computer tone greeting, then
5. Dials the company account number: **25439**.

The system follows this procedure with one exception: the "clicks and pops" of particularly noisy switching equipment may be mistaken for a greeting. Since you have no control over the telephone company's switching equipment, it is best to give the telephone connection a second or two to "settle" before giving the instruction *to listen for a greeting. The coding for placing this call is:*

T	Wait for dial tone
9	Tell the PBX that you want an outside line
14085556783	Dial the long distance company's number
++	Wait two seconds for the line to settle
G	Listen for a computer tone
25439	Dial Company A's account number

Thus, the coding string for outdialing this number is **T9T14085556783++G25439**.

Step 2: Choose a Mailbox Extension Pre-Dial Index

When the technician configures the system, the pre-extension dial strings may be programmed. Each of these is represented by a number (the pre-dial index) to simplify programming for the administrator.

To obtain a printout of pre-dial indexes and their dial strings, enter "**?**" (to request help) in response to the "Mailbox's extension pre-dial index" prompt. The available indexes, dial strings, and pre-dial string descriptions are provided, as in the following display for Example A:

Index	Pre-dial Strings	Description
1	T9	Outside line
2	T914085556783	Non-"Dial 1" Account

Choose a mailbox extension pre-dial index that represents the coding string for the first part of the number to outdial, or enter "**n**" for none. In Example A, choose **Index 2**.

Step 3: Enter the Mailbox Extension Number

The mailbox extension number consists of the balance of the dial string. Referring to Example A, Index 2 directs NP Receptionist to outdial "T9T14085556783." The balance of the string, "++G25439," must be entered as the mailbox's extension number.

Note:
The system prompts for the mailbox's extension number and for the pre-dial index even though the string represented by the pre-dial index is outdialed first.

26.102.5 Programming an Outside Attendant's Extension Number

This procedure is used to program an attendant's extension number outside of the PBX network.

Step 1: Formulate a Coding String

When the attendant's extension number exceeds 15 digits, you must formulate a coding string that directs the system to dial the number. The coding string must simulate the steps that a caller takes to place the call by using special characters to simulate certain actions. The following codes are allowed:

0-9,#,*	Send out these DTMF tones (just as though they are b eing dialed from a standard touch-tone telephone)
A-D	Outdial these fourth column DTMF tones (keys are fou nd on special telephones)
T	Go offhook (equivalent to lifting the receiver on a stan dard telephone) and wait for a dial tone
(	Send the digits that follow as pulses (10 pps)
)	Stop pulsing digits; resume sending digits as DTMF t ones
+	Pause for one second
G	Greet - wait for a person or pager to answer
F	Switchhook flash and wait for dial tone
S	Switchhook flash (no wait required)

EXAMPLE B:

Company B is a large corporation with central assistance number 1-408-555-9867. To keep track of system use, the company issues department and personal account numbers to all employees.

To get assistance, this mailbox user must (1) lift the receiver and listen for a dial tone, (2) dial 9 to get an outside number, (3) listen for a dial tone to confirm that an outside line has been reached, (4) dial the main

number, (5) wait for another dial tone, and (6) dial the department account number (0678787) and his or her personal account number (693201).

To duplicate and code this process, perform the following procedure:

T	Wait for dial tone
9	Tell the PBX that you want an outside line
14085559867	Dial the toll number
T	Listen for a dial tone
0678587693201	Dial the account numbers

Note:
NP Receptionist always appends a **G** (wait for a greeting) to the end of the attendant's extension number. To make NP Receptionist perform a blind transfer (in other words, transfer the call by putting the called party on hold, dialing the number, and hanging up), put an **H** at the end of the dial string. ("Hidden ('Blind') Mailbox Extension Number Programming".)

Step 2: Choose an Attendant Pre-Dial Index

Your system may be configured with pre-extension dial strings. To obtain a printout of pre-dial indexes and their dial stings, enter "**?**" (to request help) in response to the "Attendant's extension pre-dial index" prompt. The available indexes, dial strings, and pre-dial string descriptions are provided, as in the following display for Example B:

Index	Pre-dial Strings	Description
1	T9	Outside line
2	T923759	Non-"Dial 1" Account
3	T914085559867	Central Assistance

Choose an attendant's pre-dial index that represents the coding string for the first part of the number to outdial. In Example B, choose **Index 3** because it will direct the system to outdial all numbers except the department account and employee's personal account numbers.

Step 3: Enter the Attendant Extension Number

The balance of the dial string must be entered as the attendant's extension number. Using Example B, the department account number and user's personal number are not covered by the pre-dial string. Thus, the user's attendant extension number becomes **0678587693201**.

26.102.6 Attendant's Dialing Sequence

NP Receptionist

When a caller requests assistance, NP Receptionist

- Executes the pre-DN string programmed into the system configuration.
- Dials the string represented by the attendant's extension pre-dial index (if one was selected).
- Dials the attendant extension number.
- Executes the post-DN string.

If the attendant's number is busy, the call is rejected. If the attendant does not answer, NP Receptionist follows the RNA (Ring/No Answer), Rejected call, or Busy treatment dictated by the *original* called party's treatment type.

Applications Other Than NP Receptionist

When a caller requests assistance after leaving a message, or when a user presses 0 (zero) while logged into his or her mailbox, the system

- Executes the attendant's transfer string programmed into the system configuration.
- Dials the string represented by the attendant's extension pre-dial index (if one was selected).
- Dials the attendant extension number.
- Hangs up (that is, the internal programming automatically appends an **H** to the end of the attendant extension number).

26.103 About NP Receptionist Worksheets

This section provides information about using NP Receptionist worksheets.

Worksheet 1: If NP Receptionist is integrated with a PBX system, you may not have to assign a separate line group for NP Receptionist. To determine if you need to assign a line group to NP Receptionist, refer to the guide for your integration.

- If you assign a separate line group for NP Receptionist, complete both Offline Parameters and Online Parameters sections of NP Receptionist Worksheet 1.
- If the integration manual for the PBX switch at your installation site instructs you to configure Receptionist through the integration application menu, complete only the Online Parameters sections of NP Receptionist Worksheet 1.

The online parameters on Worksheet 1 are those that NP Receptionist shares with the NuPoint Voice application.

Worksheet 2: Worksheet 2 contains parameters that are specific to NP Receptionist software. Complete the Default options section only if the PBX switch at your site is not listed in the preceding section, PBX Dial String options.

Worksheet 3 and Worksheet 4: Worksheets 3 is the Extension Treatment Type worksheet into which you enter frequently-used instructions for specific mailboxes. You might have one set of instructions for managers' mailboxes, another for customer support staff, and another for sales representatives. Putting these instructions in a Treatment Type allows you then to provide a customize mailboxes by using the Treatment Type, rather than by individually configuring each mailbox.

26.103.1 NP Receptionist Worksheets

NP Receptionist Worksheet 1

Offline Parameters

Define line groups

Current group

Add lines to current group

Name of current group

Drop lines from current group

Line group only applications

Group selected

Assign VoiceMemo

Online Parameters

Dialing plan options

Dialing plan

1 2 3 4 5 6 7 8 9

Delete digits table

Console day access code

Offset table

Console night access code

Flow options

Message prompt? O yes O no

Greeting

Name

Console operation mode? O yes O no

PBX Dial String options

ROLM	O	Hitachi DX	O	75/85	
SL-1	O	Mitel Focus	O	Telex	
AT&T Dimension	O	NEC	O	Siemens Saturn	
Centrex	O	AT&T System	O	Fujitsu	

Default options

Post-DN string

Dial string for return on

NP Receptionist Worksheet 2

Online Parameters

Day/Night

Start time of workday ☐ AM ☐ PM

End time of workday ☐ AM ☐ PM

Weekend days ☐ M ☐ T ☐ W

Dialing Plan Menu

Dialing plan ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9

Optional star* prefix dialing plan ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9

Dial string and mailbox menu

System attendant's extension

Aministrator's mailbox #

E-mail transfer string

Pre-company name dial string

Attendant's transfer string or PBX predirectory #

Attendant's mailbox #

General greeting mailbox #

Pre-mailbox greeting dial string

Dial-by-Name menu

Last name first flag? O yes O no

Single digit access? O yes O no

Number of names threshold

Exact match break? O yes O no

Supress mailbox number? O yes O no

Allow Dial an Extension menu

Allow dial and extension for callers? O yes O no

Allow dial and extension for users? O yes O no

NP Receptionist Worksheet 3

Extension Treatment Types

Index number _____ Index name _____

Authorized period: O all O day only O night only

Authorization code _____

Extension type setup

Screen calls? O yes O no

RNA treatment: O Redial menu O Assistance only O Mailbox only

Busy treatment: O Redial menu O Assistance only O Mailbox only

Reject treatment: O Redial menu O Assistance only O Mailbox only

Extension Treatment Types

Index number _____ Index name _____

Authorized period: O all O day only O night only

Authorization code _____

Extension type setup

Screen calls? O yes O no

RNA treatment: O O O

NP Receptionist Worksheet 4

Trunk Treatment Types

Index number _____ Index name _____

Authorized period: O all O day only O night only

Authorization code _____

Trunk Type Setup

Failure treatment: O Cut through O Tone O Ring

Redial menu to use: O Redial menu O Assistance only O Mailbox only

Reject treatment: O Redial O Assistance O Disconnect

Trunk Treatment Types

Index number _____ Index name _____

Authorized period: O all O day only O night only

Authorization code _____

Trunk Type Setup

Failure treatment: O Cut through O Tone O Ring

Redial menu to

26.103.2 NP Receptionist Configuration

This procedure sets the values for parameters that NP Receptionist uses to process calls and to interact with mailboxes. Set the parameters by entering the values that you recorded on NP Receptionist Worksheets 2, 3, and 4 (see NP Receptionist Worksheets).

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**.
2. Do one of the following:

   - Select **(F) Modify Inactive Configuration** if you just made a change through the Offline Menu without activating it
   - Otherwise, select **(E) Modify Active Configuration**.
3. Select **(G) Group Selected** and enter the **number**of the line group (1-24) for NP Receptionist.

Set PBX Dialing Plan Options

1. Select **(M) Modify Application** and then select **(R) NP Receptionist Menu**.
2. Select **(D) Dialing Plan Options**.
3. To change the dialing plan, if required, select **(P) Dialing Plan** and then change the values to match Worksheet 2.
4. If the onsite PBX requires that digits be deleted for some numbers in the dialing plan, configure the Delete Digits table by selecting **(D) Delete Digits** and changing values to match those on Worksheet 2.
5. If the onsite PBX requires offsets in the dialing plan, define the offset table by:

   a. selecting **(F) Offset Table** and then **(D) Define Table**.
   b. at the **Define table number** prompt, enter the**first digit**(before any deletions) of the extensions to which the offset will be added.
   c. at the **Table Offset =** prompt, enter the **offset value** for this table.
   d. repeat this step as required. The Offset Table menu is displayed again each time you enter an offset value.
6. To change the Timeout for Receipt of first DTMF Digit value, if required, select **(T) Timeout for Receipt of First Digit** and enter the new**timeout**value from your worksheet.
7. To change the PBX Console Day Access Code, if required, select **(Y) PBX Console Attendant Day Access Code** and enter the new**access code**value from your worksheet.
8. To change the PBX Console Night Access Code, if required, select **(Z) PBX Console Attendant Night Access Code** and enter the new**access code**value from your worksheet.
9. Exit to the NP Receptionist menu.

To set flow options:

1. In the NP Receptionist Menu, select **(F) Flow Options**.
2. To change Mailbox Message Prompt from its current setting (Greeting or Name), select **(M) Mailbox Message Prompt Greeting/Name** and enter the option (G or N) you want.
3. To change the initial welcome greeting to a short dial tone to prompt the operator that the NP Receptionist is ready to receive the extension number, select **(P) PBX Console Operation**, and then select **Y** to enable, or **N** to disable.

4. Exit to the NP Receptionist menu.

To set PBX Dial String Definitions:

1. From the NP Receptionist menu, select **(P) PBX Dial String Definitions** and enter the **letter**that corresponds to the PBX at the installation site OR press**Z**for default PBX options.
2. At the**Initialize to Default Values** prompt, select **Y** to keep the default values, or **N** to change one or more values. You can change the values for any of the following parameters to the new values on your worksheet:

   - (A) Post Directory number dial string
   - (B) Pre Directory number dial string / Attendant xfer string
   - (C) Connect Dial string on Called Party Accept
   - (E) Dial string for Return on Called Party Refused
   - (F) Dial string for Return on Called Party Busy
   - (G) Special actions on Reorder Tone Encountered
   - (H) Dial string for Return on Called Party RNA
3. To change a value, enter the new value from your worksheet at the DEFAULT prompt.
4. Exit to the NP Receptionist Menu.

To set Extension Treatment Types

1. In the NP Receptionist menu, select **(T) Trunk/Extension Treatment Types**.
2. Select **(C) Current Index Number** and enter the **index number**of an extension treatment type on Worksheet 3.
3. Select **(N) Name of Current Index** and enter the **name**that corresponds to the index number you entered in the previous step.
4. To limit mailbox access to either days or nights/weekends, if required, select **(P) Authorized Periods** and enter **A** for any, **D** for day only, or **N** for night and weekend only.
5. To require users to have an authorization code to use mailboxes with the current treatment type, select **(A) Authorized Code** and then enter the **code**shown on your worksheet.
6. Exit to the NP Receptionist menu and then select **(T) Trunk/Extension Treatment Types**.
7. To change values, select **(E) Extension Type Setup** and enter the **values**for any or all of the options that follow, as applicable.

   - Select **(S) Screen Calls?** and enter **Y** to announce the caller's name to the called party to accept or reject, or **N** to connect the call after greeting the called party.
   - Select **(R) RNA Treatment?** and then select **R** to go into the Redial Menu, **A** to call the attendant, or **M** to drop into NuPoint Voice to take a message.
   - Select **(B) Busy Treatment?** and then select **R** to go into the Redial Menu, **A** to call the attendant, or **M** to drop into NuPoint Voice to take a message.
   - Select **(J) Reject Treatment?** and then select **R** to go into the Redial Menu, **A** to call the attendant, or **M** to drop into NuPoint Voice to take a message.
8. Exit to the Trunk/Extension Treatment Types Menu to save the values.

9. You can specify where the caller is to be routed after a Busy or Ring-No-Answer condition, when the caller does not enter any new instruction by selecting **(D) Redial Menu to Use** and then selecting:

    - **M** to call extension's mailbox in 3 seconds
    - **A** to call the PBX attendant in 6 seconds
    - **D** to disconnect from receptionist after 6 seconds
    - **R** means to redial the call
10. Exit to the Receptionist Menu to save your changes.
11. Repeat steps 20 to 29 of this section until you have configured all the extension treatment types you need.
12. Exit to the Configuration Main Menu.
13. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

To set Trunk Treatment Types

1. In the NP Receptionist menu, select **(T) Trunk/Extension Treatment Types**.
2. Select **(C) Current Index Number** and enter the **index number**of a trunk treatment type on Worksheet 4.
3. Select **(N) Name of Current Index** and enter the **name**that corresponds to the index number you entered in the previous step.
4. To limit mailbox access to either days or nights/weekends, if required, select **(P) Authorized Periods** and then select **A** for any, **D** for day only, or **N** for night and weekend only.
5. To require users to have an authorization code to use mailboxes with the current treatment type, select **(A) Authorized Code** and then enter the **code**shown on your worksheet.
6. To change connect criteria or failure treatment values, if required,

    - select (T) Trunk Type Setup and enter Y to change the index number to trunk type.
    - select (C) Connect Criteria? and enterCto tell NuPoint Voice to assume that the connection is successful,Tto expect a dial or modem tone, orRto expect a ring back tone.
    - select (F) Failure Treatment? and enterRto go into the Redial Menu,Ato call the attendant,Mto drop into NuPoint Voice to take a message.
7. Exit to the Trunk/Extension Treatment Types Menu to save the values.
8. If required, specify where the caller is to be routed after a Busy or Ring No Answer condition, when the caller does not enter any new instruction by selecting **(D) Redial Menu to Use** and then entering **M**to call extension's mailbox in 3 seconds,**A**to call the PBX attendant in 6 seconds,**D**to disconnect from Receptionist after 6 seconds, or**R**to redial the call.
9. Exit to the NP Receptionist menu to save values.
10. Repeat steps 33 to 41 until you have configured all the trunk treatment types you need.
11. Exit to the Configuration Main menu.
12. If you chose to modify the Inactive Configuration in step 2, you need to Activate the Inactive Configuration before your changes appear.

26.103.3 NuPoint Voice Configuration

This topic summarizes the steps necessary to configure the messaging functions of NP Receptionist:

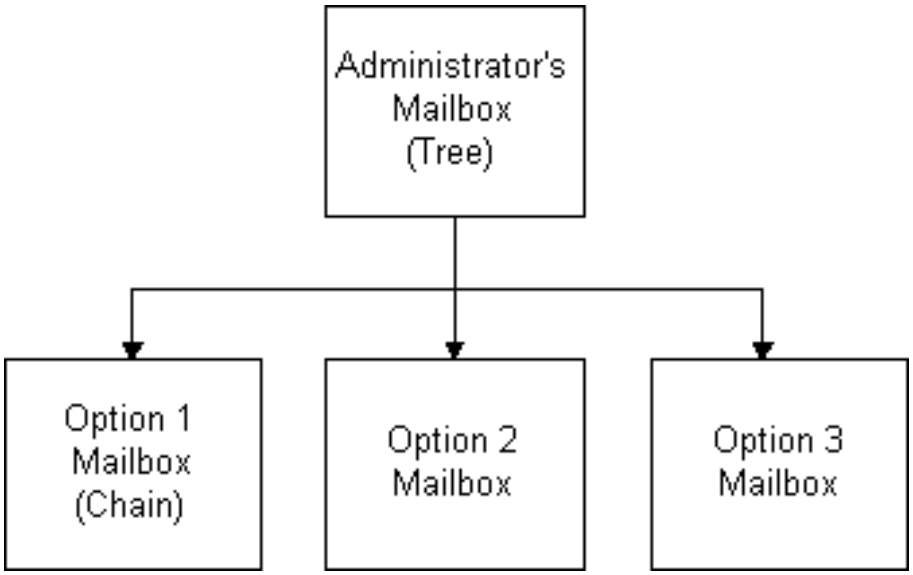
Procedure	Reference
Schedule company greetings. Use the Day/Night Menu to: • Designate the start of the work day • Designate the end of the work day • Designate the weekend	Schedule Company Greetings
Establish a dialing plan. If no star prefix is desired, use the Dialing Plan Menu. If a star prefix is desired, use the Star Prefix Dplan Menu to: • Specify the trigger digit if Dial-by-Name is desired OR • Specify the signal digit if off-system messaging is desired	Configure a Dialing Plan
If required, enable Call Placement	Enable Call Placement
If required, configure for transfer to a system attendant.	Transfer to a System Attendant
Define an administrator mailbox if you require: • Master distribution lists • Company greetings and alternate greeting • Phone administration	Define an Admin Mailbox
Define an attendant mailbox if you require: • Collecting or preventing unaddressed messages • Message of the day • Site tutorial	Define an Attendant Mailbox
If required, prevent unaddressed messages	Prevent Unaddressed Messages
If required, enable multiple messages for outside callers.	Enable Multiple Messages for Outside Callers
Set a default language for prompts, if other than English.	Language Prompts

Procedure	Reference
If required, enable Dial-by-Name: • Code the dialing plan with an A in the digit position that triggers a prompt about spelling the name. • Set the Dial-by-Name parameters. • Include feature bit 92 (user will be in Dial-by-Name database) in the FCOS assigned to mailboxes.	Enable the Dial-by-Name Function
Configure the mailbox passcode parameters.	Configure Mailbox Passcode Parameters by Line Group
Verify that the configuration is correct.	Verify Configuration Parameters
If you chose the inactive configuration at the beginning of this procedure, activate the inactive configuration to make the parameter settings take effect.	Activate the Inactive Configuration

26.103.4 Create a Single-Digit Access Menu

This procedure configures a single-digit access menu. Use this procedure to give callers quick access to frequently-called departments or persons.

1. Using the following tree structure, create the required mailboxes. See Configure a Tree Mailbox.



2. Assign FCOS **15** to the administrator's mailbox. Configure the other mailboxes as subordinate mailboxes in a tree configuration; if one of the options allows the user to dial an extension or dial by name, assign FCOS **8** to the mailbox.

   Sample subordinate mailboxes:

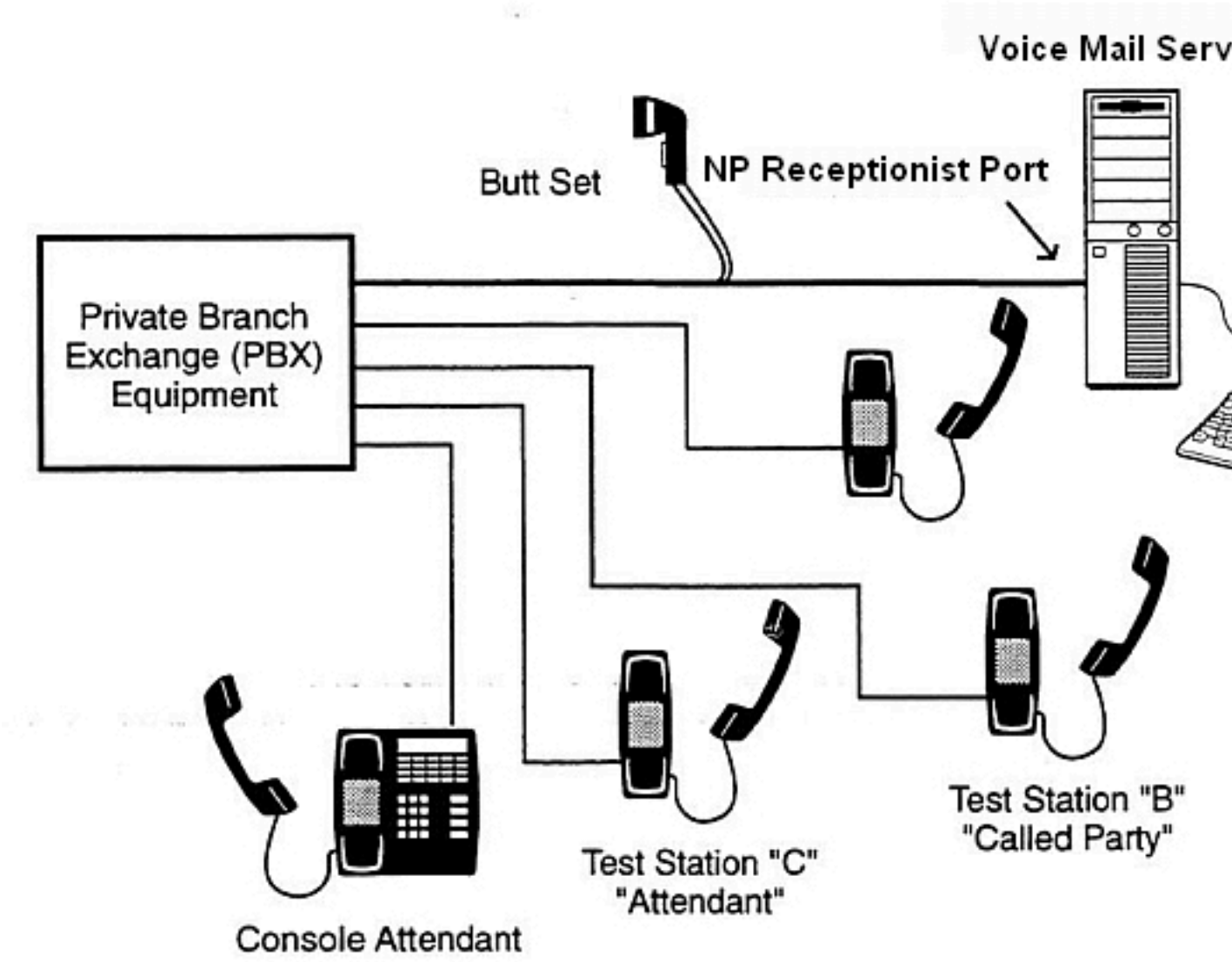
   - **Option 1**- Dial an extension or dial by name
   - **Option 2**- Technical Support
   - **Option 3**-Job Hotline

26.103.5 Set Up NP Receptionist Test Configuration

This topic summarizes the procedures for testing NP Receptionist configuration. The test setup uses three sets, designated as Station A, Station B, and Station C. The test Console Attendant is the actual Attendant (if any) who provides assistance to callers who "wait," in response to the prompt, "Please enter an extension number, or wait for assistance."

To set up telephone sets:

1. Set up three telephone sets, Station A, Station B, and Station C, as shown.
2. Record the **extension numbers** of Stations B and C. You will be associating mailboxes with these telephones.
3. If required, set up a Console Attendant phone.
4. Connect a PBX line to the NP Receptionist port.
5. Record the Reception II**extension number**.



To create mailboxes for tests:

1. Test NP Receptionist setup: greetings and assistance call processing, dialing plan and mapping of mailboxes to extension, call screening, reorder tone (see Test NP Receptionist Setup).
2. Test mailbox treatment types.
3. *Test intermediate attendant call processing.*

26.103.6 Test Mailbox Treatment Types

Use the test setup and this test plan to verify that your extension and trunk treatment types process calls correctly in the following situations:

- Busy
- Ring No Answer (RNA)
- Call screening

The test plan also tests whether your trunk treatment types process calls correctly in the following situations:

- Successful connection
- Failure treatment on Busy

Busy

1. Take Station B (the “Called Party”) off-hook.
2. Dial NP Receptionist from Station A (the “Calling Party”). Be sure that Receptionist-II answers with the appropriate greeting.
3. Enter the **mailbox number** of Station B. NP Receptionist says, “I will ring Called Party. Who may I say is calling? (if the treatment type has call screening) Please hold.”
4. Listen on the butt set for:

    - Pre-DN string dialing
    - Extension number dialing
    - Post-DN string dialing
    - A busy tone
    - Return string
    - NP Receptionist’s response to the failure condition

Ring No Answer (RNA)

1. Dial NP Receptionist from Station A. Be sure that NP Receptionist answers with the appropriate greeting.
2. Enter the **mailbox number** of Station B. NP Receptionist says, “I will ring Called Party. Who may I say is calling? (if the treatment type has call screening) Please hold.”
3. Listen on the butt set for:

    - Pre-DN string dialing
    - Extension number dialing
    - Post-DN string dialing
    - Ringing - Count the number of rings!
    - Return string
    - NP Receptionist’s response to the failure condition
4. If the treatment type does not perform as expected (for example, the caller was forced to assistance when a redial menu was desired), go back into the configuration program and change the treatment type programming.

Test Failure Test

Note: This test can only be done for trunk treatment types with connect criteria T (Tone) or R (Ringing).

1. Busy out Trunk B (the “Called Party”).

2. Note the proper connect criteria for the treatment type:

   - **C** = Cut through (All calls that are dialed are considered successful.)
   - **T** = Tone (A call is successful if NP Receptionist encounters a dial tone or computer tone after dialing the number)
   - **R** = Ringing (NP Receptionist considers the call successful only if it receives ringing in response to dialing the number)

   Be sure the trunk number that you are dialing can answer with the response that matches the connect criteria.
3. Dial NP Receptionist Trunk A. Check that NP Receptionist answers with the appropriate greeting.
4. Enter the number of Mailbox B.
5. NP Receptionist says, “I will ring Called Party. Please hold.”

   - Listen on the butt set for:

     a. Pre-DN string dialing
     b. Mailbox’s extension number dialing
     c. Post-DN string dialing
6. If the failure treatment does not perform as expected, go back into the configuration program and adjust the treatment type programming.

26.103.7 Test Intermediate Attendant Call Processing

Use the test setup and this procedure to determine if NP Receptionist processes calls to the Attendant’s extension number.

1. Take Station B (the “Called Party”) off-hook.
2. Dial NP Receptionist from Station A (the “Calling Party”). Be sure that NP Receptionist answers with the appropriate greeting.
3. Enter the **mailbox number** of Station B. NP Receptionist says, “I will ring Called Party. Whom may I say is calling? (if there is call screening) Please hold."
4. When NP Receptionist returns to Station A, choose the assistance option.
5. Listen on the butt set for:

   - Pre-DN string dialing, including the switch hook flash
   - Attendant’s extension number dialing
   - Post-DN string dialing (Menu 8)
   - Ringing
6. Answer station C. NP Receptionist should announce, “Hello. You have a call for Called Party.”

   - If Mailbox B’s treatment type specifies call screening, NP Receptionist will issue the call screening prompts. Accept the call.

Troubleshooting

- Check switch hook flash timing. If the NuPoint Voice program does not put Station A on hold before dialing, the switch hook flash timing may be too short; if Station A is disconnected almost immediately, the switch hook flash timing is too long.
- If a dial string in step 6 fails, go back into the configuration program and adjust the dial string programming.
- If the treatment type does not perform as expected, go back into the configuration program and change the treatment type.

26.103.8 Test the NP Receptionist Setup

Use the test setup and the procedures in this section to test NP Receptionist setup for processing calls:

- Greetings and Assistance Call Processing
- Dialing plan and mapping of mailboxes to extensions
- Call screening
- Reorder tone

Test Greetings and Assistance Call Processing

1. Call into the NP Receptionist main number from Station A. Check that the proper greeting, Day or Night, is played for the time period.
2. Allow the call to time out (wait).
3. If a PBX Console Attendant's Access Code is configured for the time period, listen on the butt set for:
    - Pre-DN string dialing, including the switch hook flash
    - PBX Console Attendant Day Access Code dialing
    - Post-DN string dialing
    - Answer
4. If no PBX Console Attendant's Access Code is configured, but the line group does have an Attendant's Mailbox:
    - The wait prompt, if enabled, should say "Please enter an extension number or wait." (NP Receptionist should automatically eliminate the prompt for assistance).
    - Upon timeout, you should be prompted to "Please leave your name, the name of the person you are calling, and a message."
5. If neither a Console Attendant nor an Attendant's Mailbox is configured, be sure that the Wait Prompt is disabled.
6. Repeat steps 1 and 2 for the other time period, to be sure that greetings and assistance call processing are correct for both day and night/weekend hours.

Test Dialing Plan

1. Refer to NP Receptionist Worksheet 2.
2. For each leading digit that does not have a zero in the dialing plan, call at least one extension with the correct number of digits, and one extension that is incorrect, to be sure that NP Receptionist accepts the valid extension number, and rejects the invalid one.

3. When the dialing plan specifies “V,” for variable length, test several lengths to be sure that they are accepted.
4. Enter one extension number for each group of extensions that show a zero in the dialing plan. NP Receptionist should reject all such extensions.
5. Repeat steps 2 through 4 for the other time period, to be sure that greetings and assistance call processing are correct for both day and night/weekend hours.

Test Mapping

1. If delete digits or offsets are set for any group of extensions, enter the number of the “called party” test extension into the extension field of a mailbox that will be reached by this mapping. If the number is mapped correctly, the test extension will ring. Follow this procedure for each group of mailboxes with leading digits that specify mapping.
2. Repeat the procedure for the other time period.

Test Call Screening: Call Accepted

1. Dial NP Receptionist from Station A. Be sure that NP Receptionist answers with the appropriate greeting.
2. Enter the mailbox number of Station B.
3. When NP Receptionist says, “I will ring [called party]. Whom may I say is calling?”, say your name. NP Receptionist says, “Please hold.”
4. Leave Station A off hook, and listen on the butt set for:

   - Pre-DN string dialing
   - Extension number dialing
   - Post-DN string dialing
   - Ringing - Count the number of rings!
5. Answer the call at Station B. Listen for “Hello, you have a call from [your name]. Press A to accept the call, R to refuse it.”
6. Press A. Listen on the butt set while NP Receptionist dials the Connect dial string on called party accept (Menu 8), then releases the call. Adjust this string if Station A fails to connect with Station B.

Test Call Screening: Call Rejected

1. Dial NP Receptionist from Station A. Be sure that NP Receptionist answers with the appropriate greeting.
2. Enter the mailbox number of Station B.
3. When NP Receptionist says, “I will ring Called Party. Whom may I say is calling?” say your name. NP Receptionist says, “Please hold.���
4. Leave Station A off hook, and listen on the butt set for:

   - Pre-DN string dialing
   - Extension number dialing
   - Post-DN string dialing
   - Ringing - Count the number of rings!

5. Answer the call at Station B. Listen for “Hello, you have a call from [your name]. Press A to accept the call, R to refuse it.”
6. Press R, then hang up the phone at Station B. Listen on the butt set while NP Receptionist dials the Dial string for return on called party refused. Adjust this string if NP Receptionist fails to return to Station A.
7. Listen at Station A as NP Receptionist says “I’m sorry [your name] did not answer.”

   The system then acts according to the Reject treatment type for Station B (play a redial menu, force to assistance, or force to the mailbox to leave a message).
8. If the treatment type does not perform as expected (for example, the caller was forced to assistance when a redial menu was desired), go back into the configuration program, and change the Reject treatment type programming.

Test Reorder Tone

1. Call into NP Receptionist from Station A.
2. Dial an invalid extension number that conforms to the PBX dialing plan (or an extension that is set to “do not disturb,” if the PBX gives reorder tone on do not disturb).
3. Listen on the butt set to the reorder tone.
4. NP Receptionist should return to Station A, and play the prompt that is appropriate for the “Special actions on reorder tone encountered” dial string.

26.103.9 Add NP Receptionist Extensions

Under normal circumstances, we recommend that you leave the NP Receptionist table undefined, but, in unusual circumstances, you can set up the table to prevent NP Receptionist ports from calling each other.

This table will identify that the defined extension that is forwarding back in to the pilot is one of the Receptionist extension numbers. This will then activate the use of the Receptionist dial string, which sends a +#+ to the calling port. The call will then properly connect to the user's mailbox where they will hear the mailbox greeting within three seconds. The treatment type does not come into effect.

Note:

- If this table is not defined, then under the above conditions, the station will ring four times (this is switch dependent), and then forward to the pilot number. The caller is then held for 14 to 18 seconds until they hear the mailbox user's name and the treatment type that is defined for the mailbox.
- Defining a non-Receptionist extension in this table causes all calls to that extension to be dropped.

To configure NP Receptionist Extensions:

1. From the Main menu, select **(S) System Maintenance** and then **(B) NP Receptionist Extensions**.
2. You can add or delete extensions from here.

26.104NP WakeUp - Description

Note: This feature must be configured using the **Text Console**.

The NP WakeUp optional feature provides automatic wakeup calls. These calls can be set either at the server or Text console by the system administrator or at a telephone by the user.

Wakeup call requests are stored in the mailbox and in the Wakeup Administrator. In the Wakeup Administrator, a timer checks every minute for wakeup requests for all mailboxes, then delivers all wakeup requests that have a time less than the current time. When a daily call is completed, the system increments the request by 24 hours and adds it to the end of the list.

Standard NP Wakeup, enabled by Feature Classes of Service (FCOS) feature bit 015, allows the user to set up multiple wakeup calls. These can be one-time only, or on a long-term basis every day, Monday through Friday, or Saturday and Sunday. Users can also cancel the calls at any time.

The standard NP Wakeup telephone user interface (TUI) is located in the User Options menu, choice A, Automatic wakeup.

Enhanced NP Wakeup, designed for hospitality settings and enabled by FCOS feature bit 287, allows the user to set up one daily call. The system administrator can configure a snooze function, as well as how many times and how often the server can repeat a call that is not answered. If the user chooses snooze (presses any key within 10 seconds) or the call is ring no answer or busy, the request will be retried at the configured interval for the configured number of times.

The enhanced NP Wakeup TUI is located at the Call Schedule Options menu, choice **W**, Wakeup.

26.104.1 NP WakeUp - Description

Note: This feature must be configured using the **Text Console**.

The NP WakeUp optional feature provides automatic wakeup calls. These calls can be set either at the server or Text console by the system administrator or at a telephone by the user.

Wakeup call requests are stored in the mailbox and in the Wakeup Administrator. In the Wakeup Administrator, a timer checks every minute for wakeup requests for all mailboxes, then delivers all wakeup requests that have a time less than the current time. When a daily call is completed, the system increments the request by 24 hours and adds it to the end of the list.

Standard NP Wakeup, enabled by Feature Classes of Service (FCOS) feature bit 015, allows the user to set up multiple wakeup calls. These can be one-time only, or on a long-term basis every day, Monday through Friday, or Saturday and Sunday. Users can also cancel the calls at any time.

The standard NP Wakeup telephone user interface (TUI) is located in the User Options menu, choice A, Automatic wakeup.

Enhanced NP Wakeup, designed for hospitality settings and enabled by FCOS feature bit 287, allows the user to set up one daily call. The system administrator can configure a snooze function, as well as how many times and how often the server can repeat a call that is not answered. If the user chooses snooze

(presses any key within 10 seconds) or the call is ring no answer or busy, the request will be retried at the configured interval for the configured number of times.

The enhanced NP Wakeup TUI is located at the Call Schedule Options menu, choice **W**, Wakeup.

26.105 NP WakeUp - User Interface

Standard TUI

1. At the telephone, log in to the mailbox and press the **U** key to reach the User Options menu.
2. At the User Options menu, press the **C** key to reach Call Schedule Options.
3. At the Call Schedule Options menu, press the **W** key to reach NP WakeUp.
4. At the NP WakeUp menu, schedule or cancel calls.
5. To schedule a call, press the **S** key, then at the Prompts, enter the time for a wakeup call: two digits for the hour, two digits for the minute, then press the **A** key for a.m. or the **P** key for p.m.

   - To make this a daily call, press the **D** key.
   - To cancel the call, press the **C** key.
   - To change the time, press the **R** key.
   - To cancel all calls, press the **C** key.
   - To schedule another call, repeat step a.
   - To exit to the User Options menu, press the **X** key.

Enhanced TUI

1. At the telephone, log in to the mailbox and press the **A** key to reach NP WakeUp. If a call is already scheduled, a Prompt announces it.
2. To keep a scheduled call, press the **K** key.
3. To delete a scheduled call, press the **D** key.
4. To set a new call (this automatically replaces any scheduled call), press the **A** key.
5. Follow the Prompts to schedule a call. Enter the time for the call: two digits for the hour, two digits for the minute, then press the **A** key for am or the **P** key for pm.

   The call will be made daily at this time until the user changes or deletes the call through the TUI or the administrator changes or cancels the call at the console.

Note:
If the user does not set AM or PM, the server will call at the next occurrence of that time. For example, if the user sets a call for "8:00" at 9 PM, the server will call at 8:00 AM. If the user sets a call for "8:00" at 7 PM, the server will call at 8:00 PM.

- To exit the mailbox, press the **X** key.

26.106 Call Records

Wakeup calls will be entered in the Event Recorder for these reasons:

- The user answered the call.
- The user chose snooze.
- The user did not answer, but the system allows more retries.

If the call is not answered and all snoozes and retries are used, the system records the failure in the Error Log and sends a message to the WakeUp administrator's mailbox.

For more information about Event Recorder, see the Troubleshooting section of the *NuPoint Unified Messaging Technician's Handbook*.

26.107 Overview of PMS Integrations

Note:

- The PMS feature is not supported for MiCollab NuPoint systems.
- Only one PMS system can integrate with NuPoint at one time.
- Direct physical serial connections to Virtual NuPoint (vNuPoint) systems are not supported.

Property Management Systems (PMS) are computerized systems used to manage guest bookings, online reservations, telephone systems and other amenities. PMS systems can integrate with NuPoint UM to provide automated telephone and voice mail services for hotel guests. Integrated PMS systems communicate with NuPoint UM using check-in and check-out messages to alter the state of NuPoint UM voice mail mailboxes. Default check-in/check-out state changes are configurable by the system administrator.

The PMS feature is installed with the **NPMHospitality** blade. This is an optional feature that needs to be added to the AMC record for the site before the blade can be installed. The option name on the AMC is "NuPoint Messaging: PMS - Hospitality Integration". PMS configuration must be performed using the Web Console.

PMS connects with the NuPoint system in one of two ways:

- **Serial connection**: The PMS connects to a physical serial port on a NuPoint UM system.
- **IP connection**: Internet connection. This can be accomplished directly, or by using a Serial-to-IP converter.

Using a Serial-to-IP Converter

If the PMS system only has a serial connection, it can still be connected to NuPoint UM via IP using the Precidia iPocket 232 converter. The iPocket converter is also used when the NuPoint UM hardware has no available serial ports.

To be compatible with NuPoint UM, your PMS must emulate one of the following PMS systems:

- EECO
- HIS
- Hyatt/Logistix/Encore
- Marriott

There are three basic steps required for installation of a PMS integration:

1. **Install** the PMS Integration optional feature on the NuPoint Voice server. Note that NuPoint Voice must be rebooted after the installation.
2. **Link** the NuPoint UM Voice server and the PMS. The PMS can be connected directly to an IP port or a serial port on the NuPoint UM server, or to the Precidia iPocket 232 serial-to-IP converter.
3. **Configure** the integration to meet the needs of the specific site. Configuration changes are done online and take effect within one minute, making the integrations very flexible.

26.107.1 Installation Using a Physical Serial Port

If your server has two physical serial ports, we recommend that you connect the PMS system to **COM Port 2**. For systems with only one physical serial port, it is necessary to reprogram **COM Port 1** from its default assignment for the NuPoint UM PPP service (an external dial-up modem service).

Note:

- By default, the NuPoint UM server always displays two serial port choices. You must verify the actual existence of serial ports before programming.
- Virtual NuPoint (vNuPoint) systems do not support direct serial port connections.

To connect the PMS to a physical serial port on the single-node NuPoint UM system:

1. Connect a null modem serial cable between the PMS COM Port and a NuPoint UM COM Port. Make note of which NuPoint UM COM port you use.
2. Log in to the Web Console.
3. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
4. When prompted to **Duplicate Active Configuration**, click **Yes**.
5. In the navigation tree, click **External Applications**.

6. Do one of the following:

   - **To connect to COM1:**

     - Click **Serial Port 1**. You are warned that the PPP service will be disabled.
     - Click **OK**.
     - In the **Application** list, select the appropriate application (**Hyatt**,**EECO, HIS,** or **Marriott**). This selection automatically sets the appropriate serial port settings.
   - **To connect to COM2:**

     - Click **Serial Port 2**.
     - In the **Application** list, select the appropriate **PMS Integration**option for your system. This selection automatically sets the appropriate serial port settings.
7. Click **Save**.
8. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.107.2 To Restore NuPoint UM PPP Service

If you disabled the NuPoint UM PPP service to use COM1 for a serial connection, and later, you decide to use COM1 for PPP again, you can restore the PPP service as follows:

1. Remove the null modem serial cable between the PMS serial port and the NuPoint UM COM1 port.
2. Connect a serial-based dial-up modem to the NuPoint UM COM1 port.
3. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
4. When prompted to **Duplicate Active Configuration**, click **Yes**.
5. In the navigation tree, click **External Applications** and then click **Serial Port 1**.
6. In the **Application** list, select **NP-UM PPP Service**.
7. Click **Save**.
8. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.107.3 Serial Port Settings

The following table lists the required Serial Port settings for PMS integrations:

Setting	Hyatt-Encore	HIS	EECO	Marriott
Baud	1200 Asynch	2400 Asynch	1200	1200 Asynch
Bits	10	10	10	11
- Start	1	1	1	1
- Data	7	7	8	7
- Parity	1	1	0	1

Setting	Hyatt-Encore	HIS	EECO	Marriott
- Stop	1	1	1	2
Parity	Even	Even	-	Even

26.107.4 Configure IP Connectivity

Depending on your system setup, you configure NuPoint UM in one of the following modes:

- **Client mode**: configure the NuPoint UM system in this mode if your PMS system is set up to listen for incoming connections. (Use this mode when using Precidia serial-to-IP converter.)
- **Server mode**: configure the NuPoint UM system in this mode if your PMS system needs to connect to the voice mail system.

Note:
If you are using a serial-to-IP converter, you must configure PMS iPocket solutions with NuPoint UM in IP PMS Server Mode.

Configuring Client Mode

Before you begin, ensure that:

- the PMS system has a valid IP address for the IP network, and is programmed to listen on a local PMS TCP port
- the Precidia iPocket (if required) is programmed with the correct IP address and port

To configure NuPoint UM in client mode:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **External Applications** and select the IP port (1,2,3, or 4) to configure.
4. In the **Application** list, select the appropriate PMS Integration type for your system.
5. In the **Connection Mode** list, select **Client**.
6. In the **IP Address** field, enter the IP address of the remote PMS system, OR the Precidia iPocket232 if used.
7. In the **Server Port Number** field, enter the remote PMS port number, OR the virtual port number you configured as the local and remote port number when configuring the Precidia iPocket232.
8. Click **Save**.
9. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.
10. The PMS administrator must program the PMS system to connect to the NuPoint system at the NuPoint UM IP Address on the PMS TCP port.
11. You can now configure PMS integration options that will change NuPoint Mailbox states when PMS check-in/check-out messages are received.

After the PMS system connects, messages are exchanged between NuPoint UM and the PMS system to perform PMS-related actions.

Configuring Server Mode

Before you begin, ensure that:

- the PMS system has a valid IP address for the IP network, and is set up to connect to a remote IP address and port on the NuPoint UM system
- NuPoint UM is connected to the IP network and configured with a valid IP address in MSL
- all integration components are licensed and installed

To configure NuPoint UM in server mode:

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **External Applications** and select the IP port (1,2,3, or 4) to configure.
4. In the **Application** list, select the appropriate integration type (**Hyatt**,**EECO**or**HIS**).
5. In the **Connection Mode** list, ensure that **Server** is selected.
6. In the **Server Port Number** field, enter the port number to use as the PMS TCP port.
7. Click **Save**.
8. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.
9. The PMS administrator must program the PMS system to connect to the NuPoint system at the NuPoint UM IP Address on the PMS TCP port.
10. You can now configure PMS integration options that will change NuPoint Mailbox states when PMS check-in/check-out messages are received.

After the PMS system connects, messages are exchanged between NuPoint UM and the PMS system to perform PMS-related actions.

26.107.5 Installation Using a Serial-to-IP Converter

Follow this procedure if you are connecting the PMS to the NuPoint Unified Messaging server using a Precidia iPocket232:

1. Install and configure the Precidia iPocket232.
2. Configure IP Connectivity between the NuPoint UM server and the iPocket232.
3. Connect the Precidia iPocket232 to the PMS unit.

26.107.6 Install and Configure the Precidia iPocket232

The RS232-to-IP serial port converter, Precidia Technologies iPocket232 (provided by the distributor and its resellers), is required to connect the customer's PBX to the customer's Local Area Network (which, in turn, connects to the NuPoint UM server).

Installing the Precidia iPocket232 Converter

To install the Precidia iPocket232:

1. Connect the Ethernet cable between the Ethernet port on the Precidia iPocket232 and the network.
2. Connect one end of the RS-232 serial cable to the DB-9 serial connector on the Precidia iPocket232 and apply power.
3. Connect the other end of the serial cable to the PC COM port.

Configuring the Precidia iPocket232 Converter

1. Launch a terminal program on the PC (such as Hyperterminal).
2. Configure the following settings in the Hyperterminal window:
   - 8N1 (eight bits, no parity, one stop bit)
   - 9600 baud
3. Press and hold the **reset** button on the Precidia iPocket232 until the Configuration screen appears.
4. Select **1) Ethernet Settings**.
   - Select **A) IP Address** and enter the IP address of the Precidia iPocket 232.
   - Select **B) Subnet Mask** and enter a subnet address to apply to the IP address of the Precidia iPocket 232.
   - Select **C) Gateway** and enter the gateway address for the Precidia iPocket 232.
5. Select **2) Serial Port Settings**.
   - Select **A) Protocol.** A list of protocols will display. Enter **D1** for Transparent and tcp(tunnel).
   - Select **B) PortSetting** and enter the appropriate serial port settings.
   - Select **D) Local Port Settings** and enter 5001, or the number you entered for your remote port.
   - Select **E) Remote IP** and enter the IP address of the NuPoint server. If you are using the NuPoint 640 model, enter the cluster IP address.
   - Select **F) Remote Port** and specify the PMS TCP Port to connect to on the NuPoint UM IP Address.
   - Select ***** to save the configuration parameters.
6. Disconnect the RS-232 serial cable from the PC.
7. Connect the applicable RS-232 serial cable between the SMDI-compatible switch and the Precidia iPocket232.

Note:
For any additional installation and configuration information for the Precidia iPocket232, refer to the Precidia iPocket232 User Guide, which is located on the Precidia website at www.precidia.com.

Verifying the iPocket Configuration

Perform the following steps to test your Precidia iPocket232 configuration:

1. Verify that the Link lamp is lit.
2. Verify that the Status lamp is flashing.
3. Ping the IP address assigned to the Precidia iPocket232.

26.107.7 Configuration for PMS Integrations

Note: This configuration is available in the **Text Console** only. LEAVE VISIBLE TO WEB CONSOLE!

EECO, HIS, and Encore PMS Integration Set-Up

The PMS menu is accessed as follows:

1. From the Main menu, select **(S) System maintenance**, **(R) Reconfiguration**, and then**(E) Configure PMS integration**.
2. Answer the following questions to configure PMS:

   - **Clear passcode on Check-out = [Y]**: To have the mailbox passcode cleared on Check-out enter "Y" otherwise, enter "N"
   - Clear messages on Check-out = [Y]:To have the mailbox messages cleared on Check-out enter "Y" otherwise, enter "N"
   - Clear name on Check-out = [Y]:To have the mailbox name cleared on Check-out enter "Y" otherwise, enter "N"
   - Clear greeting on Check-out = [Y]: To have the mailbox greeting cleared on Check-out enter "Y" otherwise, enter "N"
   - On Check-in set the mailbox FCOS = [0]: Enter the Features Class of Service (FCOS)number between 1 and 64 OR enter 0 to prevent the number from being changed.
   - On Check-out set the mailbox FCOS = [0]:Enter the FCOS number between 1 and 64 or enter 0 to prevent the number from being changed.

Marriott PMS Integration Set-Up

The PMS menu is accessed as follows:

1. From the Main menu, select **(S) System maintenance**, **(R) Reconfiguration**, and then**(P) Configure Marriott PMS integration**.

2. Answer the following questions to configure PMS:

- **Clear passcode on Check-out = [Y]**: To have the mailbox passcode cleared on Check-out enter "Y" otherwise, enter "N"
- **Clear messages on Check-out = [Y]**: To have the mailbox messages cleared on Check-out enter "Y" otherwise, enter "N"
- **Clear name on Check-out = [Y]**: To have the mailbox name cleared on Check-out enter "Y" otherwise, enter "N"
- **Clear greeting on Check-out = [Y]**: To have the mailbox greeting cleared on Check-out enter "Y" otherwise, enter "N"
- **On Check-in set mailbox FCOS = [2]**: Enter the Features Class of Service (FCOS) number between 1 and 64 OR enter 0 to prevent the number from being changed.
- **On Check-out set mailbox FCOS = [3]**: Enter the FCOS number between 1 and 64 or enter 0 to prevent the number from being changed.
- **On Check-in set mailbox LCOS = [1]**: Enter the Limits Class of Service (LCOS) number between 1 and 64 OR enter 0 to prevent the number from being changed.
- **On Check-out set mailbox LCOS = [1]**: Enter the LCOS number between 1 and 64 or enter 0 to prevent the number from being changed.

Mailbox Set Up

EECO Only:

Once the application has been set up, the user must create guest mailboxes with either the Check-out or the Check-in FCOS (it is important to match the existing room status since the integration does not handle a re-synchronization of the NuPoint and PMS databases when it first starts up).

HIS Only:

Once the application has been set up, the user must create guest mailboxes with either the Check-out or the Check-in FCOS. (It is not critical to match the existing room status since the integration offers a System Maintenance menu choice to provide a re-synchronization of the databases when PMS first starts up). It is important to set the **MWI type** for the guest mailboxes to be type **16: HIS PMS**.

This is so that the guest room's message waiting light is controlled by the PMS system. (Note: this integration does NOT preclude the use of another integration running on a different serial port).

After both the configuration and the mailboxes have been set up, the integration updates the room status.

Encore

Once the application has been setup, the user must create guest mailboxes with either the Check-Out or Check-In FCOS (it is not critical to match the existing room status since the integration handles a re-synchronization of the databases when it first starts up). It is important to set the **MWI type** for the guest mailboxes to be type **16**: **HIS PMS**

This is so that the guest room's message waiting light is controlled by the PMS system. (Note: this integration does NOT preclude the use of another integration running on a different serial port).

After both the configuration and the mailboxes have been set up, the integration will update the room status.

26.108 EECO Troubleshooting Guide

Implementation

The EECO PMS integration within NuPoint Voice polls the Property Management System once a minute in order to find out which rooms have been checked-in/checked-out since the last poll. This information is used to perform user configurable check-in/check-out procedures to mailboxes on the NuPoint Voice system. For more information on the NuPoint Voice Check-in/Check-out procedures, contact your distributor.

Protocol

1. After 60 seconds of no activity NuPoint Voice sends an ASCII "C" followed by an ETN ($03).
2. The PMS replies with the character "C" within two seconds.
3. If no reply is received within the two second window up to two additional attempts will be made by the server. If there is still no response from the PMS, NuPoint Voice will return to sleep for 60 seconds and start over at 1.
4. Once the PMS replies it then has 6 seconds to start sending room info packets to NuPoint Voice for processing. These packets are as follows:

   - Start of record character * ($2A).
   - Room status character: A = newly checked-in; V = newly checked-out.
   - Room number followed by the delimiter character semicolon ($3B). Room numbers are in ASCII readable. Only numeric room numbers are supported at this time. Note, at this time the Room number is assumed to be the mailbox number and as such needs to conform to the dial plan. Eventually the ability to translate alphanumeric room numbers to mailbox numbers will be added.
   - End of record character % ($25).

   These packets can be no longer than 80 characters including the start and end of record characters. When there is no more data to send to NuPoint Voice, the interface sends the single ASCII character "@" ($40).
5. Upon receiving the packet from the PMS, NuPoint Voice will then process the information. If the packet is good, all check-in/check-out procedures are carried out and NuPoint Voice requests the next packet (if any) by sending an "M" followed by an ETN ($03). If the packet is bad, NuPoint Voice re-requests it by sending an "L" followed by an ETX ($03). If the PMS sent the empty reply ("@"), NuPoint Voice will go back to sleep for 60 seconds without responding to the PMS.

Note:
The PMS must first echo the "L" or "M" before sending any other information to NuPoint Voice.

6. When the PMS receives either the "L" ETX or "M" ETN requests from NuPoint Voice, it has six seconds to respond. NuPoint Voice will try either of these requests up to three times before giving up and sleeping for 60 seconds before starting at 1) again.

Physical Characteristics

- RS-232 compatible signal.
- 1200 baud.
- 1 start bit, 1 stop bit, 8 bit data, and no parity.
- NuPoint Voice is configured to be a DCE device.
- No flow control is supported.
- Data signals required are transmit data, receive data, logic ground (pin 7), data terminal ready (should always be high).
- No control signals are used.

Diagnostic Information

See the Appendix for detailed diagnostic information available through the error log file, the CDR file and the system console.

26.108.1 HIS Troubleshooting Guide

Introduction

In order to integrate reliably between the HIS PMS system and the NuPoint Voice system, the following protocol has been developed. The protocol contains three layers; physical, link, and message. This protocol conforms to the "HIS Standard Communications Protocol for Full Duplex Operations" fully with the following stipulations:

Physical Layer

Electrical Interface: EIA RS232C - Type D electrical standard compatibility. Connection is via a DB25-pin male connector.

Signal Form: EIA RS404.

Interface Distance: Maximum 50 feet. Interface unit to Interface Processing Unit direct connection. Distances exceeding 50 feet require a line driver.

Operation Mode: Full duplex.

Link Layer

Appearance:

Data Rate: 2400 Baud Asynchronous

Byte Framing: 10 bits, (1 start, 7 data, 1 parity, 1 stop), even parity.

Message Layer

There are six messages defined for the protocol as follows:

- Message number 1 is RESYNC.
- Message number 2 is ROOM OCCUPIED.
- Message number 3 is ROOM VACANT.
- Message number 4 is MESSAGE WAITING STATUS.
- Message number 5 is BAD MAILBOX ADDRESS.
- Message number 6 is SEND MESSAGE WAITING STATUS.

Mailbox Re-synchronization

With the HIS PMS integration, an additional menu choice (G) has been added to the System Maintenance Menu to allow the system administrator to re-synchronize the state of all the mailboxes being supported by the PMS.

Message Waiting

The HIS PMS Integration supports message waiting notification through the PMS system. A message waiting type has been added to the system called "HIS PMS." See Assign Message Waiting Type to a Mailbox.

7.0 Diagnostic Information

See the Appendix for detailed diagnostic information available through the error log file, the CDR file and the system console.

26.108.2 Hyatt Encore Configuration and Troubleshooting

Encore Configuration and Troubleshooting

Introduction

The Hyatt Encore PMS is an optional feature enhancement that allows integration between NuPoint Voice and the Encore Property Management System.

Under this integration, it is possible to not only automatically assign vacant and occupied mailboxes to guests (checked in or out), but it also allows for room reassignment and text message waiting indication.

The NuPoint Voice to Hyatt Encore PMS Integration is designed to offer hotels a reliable and simple way of relaying communication between the voice messaging system (VMS) and the property management system (PMS).

It is designed to work with software release 5.00 and later.

This integration provides:

- Check In - Automatic check in of a guest mailbox upon arrival (PMS to VMS message)
- Text Message Notification - VMS notification of number of text messages in the PMS.
- Message Waiting Indication - Automatic voice message waiting indication (controlled by the PMS)
- Played Message Indication - Automatic signaling from the VMS to the PMS when a message is played.
- Multiple Classes of Service - Allows the automatic check in of guests with different classes of service which may include different language prompts.
- Check Out - Automatic check out of a mailbox, by disposing of any recorded messages, recorded name (if any), or recorded mailbox greeting (if any).
- Mailbox Modify - The Hotel should be able to modify the mailbox number of a particular guest without losing any of the recorded information in that mailbox.

Text MWI

It is possible for a guest to find how many (if any) text messages are waiting at the front desk (in the PMS system). This is done both upon login and logout of the mailbox:

"Hello <name>, you have N unplayed messages, X messages total. Y text messages at the front desk. Press P to play the first message..."

"You have X messages remaining." (No prompting done when there are NO text messages.)

This announcement of text messages is controlled with FCOS feature bit **154** (Announce text (E-Mail) message count.)

Communication Description

This integration is based on communication between the PMS and the NuPoint UM server via an RS-232 Full Duplex link.

Link Setup

Baud = 1200 Asynchronous,

Bits = 10, (Start = 1, Data = 7, Parity = 1, Stop = 1)

Parity = Even.

Note: A Null Modem adapter may be needed with an Encore PMS Integration. Test the RS-232 link without one, and if the data packets are not received correctly, install a Null Modem Adapter.

Message Formats

Each fixed length record will contain:

S	Message	E	L
T	Text	T	R
X		X	C

All messages start with an STX, followed by the message text. All message text must be followed by ETX and the last byte LRC, to guarantee integrity.

ACK and NAK are sent by the receiver to the sender to indicate positive or negative acknowledgement to the transmitted message. A NAK should be used by the message sender as a request to retransmit the last message sent. ENQ is a sender request for a repeat of the acknowledgement (ACK or NAK) as a reply to the last transmitted message.

The following is a summary table of the valid data transferred between the PMS and the VMS:

STX = 02H Start of data text

ETX = 03H End of data text

ENQ = 05H Request for retransmission of acknowledgement

ACK = 06H Positive acknowledgement

NAK = 15H Negative acknowledgement

SP = 20H ASCII space character (to padd fields)

LRC = Longitudinal redundancy check (XOR of all bytes after STX including the ETX character, with a 00H Null seed)

MBOX = A 6 digit (left justified and space filled) mailbox ASCII number

MSG = "1" RESYNCHRONIZE

"2" CHECK IN

"3" CHECK OUT

"4" MESSAGE WAITING STATUS

"5" BAD MAILBOX ADDRESS

"6" QUERY MESSAGE WAITING STATUS

"7" MOVE MAILBOX

"8" MODIFY LCOS

"9" TEXT MESSAGE MW

Where the message is sent in hex (ex: "4" is 34H). (See Message Format Table, below.)

FCOS = A 2 byte number (00-64) representing the Feature Class of Service to use when modifying the mailbox (set up via the console configuration menus)

UNP = A 2 byte number (00-99) representing the number of unplayed messages in the guest mailbox (valid ranges 30H to 39H)

URG = A 2 byte number (00-99) representing the number of all unplayed messages with URGENT priority found in the guest mailbox (valid ranges 30H to 39H)

UNR = A 2 byte number (00-99) representing the number of unread text messages in the PMS system (valid ranges 30H to 39H)

Note:
All messages are of a fixed length record (16 bytes), space padded.

Diagnostic Information

See the Appendix for detailed diagnostic information available through the error log file, the CDR file and the system console.

NuPoint Voice/Encore PMS Message Format

Message Format Table

	Message Text														
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
STX	"1"	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	SP	ETX	LRC
STX	"2"	MBOX						SP	SP	SP	SP	SP	SP	ETX	LRC
STX	"3"	MBOX						SP	SP	SP	SP	SP	SP	ETX	LRC
STX	"4"	MBOX						UNP		URG		SP	SP	ETX	LRC
STX	"5"	MBOX						SP	SP	SP	SP	SP	SP	ETX	LRC
STX	"6"	MBOX						SP	SP	SP	SP	SP	SP	ETX	LRC
STX	"7"	MBOX						MBOX						ETX	LRC
STX	"8"	MBOX						LCOS		SP	SP	SP	SP	ETX	LRC
STX	"9"	MBOX						UNR		SP	SP	SP	SP	ETX	LRC

26.108.3 Marriott Troubleshooting Guide

Physical Communication Link

The interface shall be asynchronous and shall use an EIA RS-232 connection. The PMS will support transmit data, receive data, signal ground, and data terminal ready. The vendor must support transmit data, receive data, and signal ground.

Each data character shall contain 11 bits in the format consisting of:

- 1 start bit
- 7 data bits
- 1 even parity bit
- 2 stop bits

The possible serial asynchronous communication bit rates are 110, 300, 600, 1200, 2400, 4800, and 9600 bits per second. The preferred bit rate is 1200 bits per second or lower. The actual rate shall be defined by the application that implements this specification.

Data Link Control

The function of this communication specification is to effect the orderly transfer of data from one system to another. The data messages are comprised of text and data-link control characters. Data-link control characters are required in each message to act as delimiters and to control the transmission.

Transmission Codes

The data is transferred as binary-coded characters as defined by the ASCII character set.

Data Link Control Characters

All hexadecimal representations of the control characters are in a 7 bit ASCII format and do not contain any parity bits.

Data Link Control Characters	
All hexadecimal representations of the control characters are in a 7 bit ASCII format and do not contain any parity bits.	
ENQ	A 0516 is the enquiry character. An ENQ is used to bid for the link when using a point-to-point link connection.
ACK0	A 1016 0616 is the ready sequence. An ACK0 shall be sent in response to an ENQ to indicate the communic ation link is established and the receiving station is r eady to receive a data block.
ACK1	A 1016 0816 is the acknowledge sequence. An ACK1 shall be sent in response to a data block transfer indicat ing successful reception of the data.

NAK	A 1516 is the negative acknowledge character. A NAK shall be sent in response to an ENQ to indicate the rec eiving station is not ready to receive a data block. A NAK shall also be sent in response to a data block transfer, indicating unsuccessful reception of the data block (par ity error, block check error, message framing error) and requests the data block be retransmitted.
STX	A 0216 is the start of text character. A STX is the first c haracter in a data block. All data blocks must begin with an STX. The STX also triggers the start of the block che ck calculation. The STX character is followed immediate ly by the message text.
ETX	A 0316 is the end of text character. An ETX is the last character in a data block. Each data block transfer must terminate with an ETX (followed by the BCC). The ETX triggers the end of the block check calculation. The ET X character is followed immediately by the block check c haracter (BCC).
EOT	A 0416 is the end of transmission character. An EOT is used to signify the termination of a data message transm ission. When this code is received, the communication l ink has been released by the controlling station.

Operation of the Data Link

The data link shall be designed to operate in a half duplex point-to-point mode. For half duplex operations, a contention situations exists, whereby both stations can attempt to use the communication link simultaneously. To account for this possibility, a station bids for the link using the ENQ (enquiry) control character. The ENQ sequence provides a clear and concise means for requesting control of the link, while leaving a maximum amount of time to monitor the link for bids by the other station. Once a station gains control (this station shall be known as the controlling station and the other station shall be known as the receiving station) of the link, message transmission can start.

To avoid the problem of simultaneous transmission requests, each station shall be assigned a priority, primary and secondary. If simultaneous bidding occurs, the primary station shall continue to bid the link until the secondary station responds or until the retry limit is reached. If the primary stations receives an ENQ and it has not initiated a request for the link, then it replies with an ACK0 if it is ready to receive, or a NAK if not. Thus the secondary station can gain control of the communication link for transmission only when the link is left free by the primary station. The vendor shall be considered the primary station, while the PMS shall be secondary.

Message transmission is terminated and the link is returned to the idle state upon transmission of an EOT by the controlling station. Once the controlling station transmits an EOT to release control of the link, it must wait a minimum of the T1 value before transmitting an ENQ to attempt to regain control of the link. This method gives each station a fair opportunity to obtain control of the link.

Timeout Timers

Since timing is very critical when competing for control of the line, several timers have been defined. The actual value of the timers shall be defined by the application that implements this specification. These timers are defined as:

T1	This timeout value represents the time interval the prev ious controlling station must wait before attempting to regain control of the

T2	This timeout value represents the time interval the stat ion attempting to gain control must wait for a response. (After sending ENQ, the time to wait for an ACK0 or NA K response). The receiving station must respond within this interval, or a timeout condition will exist.
T3	This timeout value represents the time interval the cont rolling station must wait for a response to a data block. (After sending STX (text data) ETX BCC, the time to w ait for an ACK1 or NAK response). The receiving station must respond within this interval, or a timeout condition will exist.
T4	This timeout value represents the time interval the rece iving station must wait for a data block from the controllin g station. (After sending ACK0 to an ENQ, the time to w ait for STX (text data) ETX BCC). The controlling station must transmit the data block within this interval, or the lin e is assumed to be in an uncontrolled
T5	This timeout value represents the time interval the rece iving station must wait for the controlling station to relea se control of the line or resend the data block. (After sen ding ACK1 or NAK to a data block, the time to wait for E OT or the retransmission of the data block, respectively). The controlling station must release control or resend t he data block within this interval, or the line is assumed t o be uncontrolled.
T6	This timeout value represents the time interval the stat ion attempting to gain control delays after being denied control of the line. (The time to delay after receiving a N AK response to an ENQ).

Text Data

Text data is transmitted in complete units called data blocks. A data block is initiated by a start of text (STX) character, and concluded by an end of text (ETX) character. Text data is defined as all characters that occur in a data block between, the STX and the ETX. Text data shall be limited to the ASCII characters between 2016 and 5A16 inclusive.

The content of the text data shall be defined by the particular application that implements this specification.

Error Detection

Each data block is checked for accuracy by the receiving station. This specification defines two types of error detection that will be used to verify data blocks.

Parity

Parity checking (also referred to as a vertical redundancy checking) allows individual characters to be validated. When using the 7-bit ASCII character set, an 8th bit can be used as a parity bit. The 8th bit will be defined as the parity bit, using an even parity scheme. For even parity, the parity bit is set a "1" or "0" so the resulting 8 bit character will have an even number of "1" bits in it.

Block Check Character (BCC)

The block check character (also called a longitudinal redundancy check) is a verification of the total data block. The BCC is accumulated at both the transmitting and receiving stations during the transmission of

a data block. This BCC is transmitted immediately following the end of text (ETX) character. The receiving station compares the transmitted BCC with the calculated BCC and determines whether or not the data block was received free of errors.

The BCC is calculated by starting with a zero value and performing an exclusive or operation on each character in the data block beginning with the character immediately following the STX character and ending with, and including, the ETX character. As an example, the transmission STX+A+B+C+ETX would have a BCC of 4316 (not including parity). This would be the result of A XOR B XOR C XOR ETX. In hexadecimal, this would be represented as 4116 XOR 4216 XOR 4316 XOR 0316.

Line Control Protocol

The line control protocol is designed to give maximum flexibility in the transmission of data between the stations. This protocol is patterned after standard binary synchronous interface protocols. Each control sequence has one or more expected response sequences. The following descriptions identify those expected sequences.

ENQ: A station wishing to transfer a data block transmits an ENQ to gain control of the line. The station attempting to gain control should wait the T2 interval for a response. An ENQ control sequence has one of the following allowed responses:

ACK0: An ACK0 indicates the receiving station is ready to receive the data message at this time. The controlling station must begin transmission of the data block within the T4 interval. If the receiving station does not receive the transmission within the T4 interval, it should assume the line is in an uncontrolled state.

NAK: A NAK indicates the receiving station is not ready to receive the message at this time. The transmitting station should retry the ENQ procedure after a T2 interval delay.

STX (text data) ETX BCC: After a station has successfully obtained control of the line, it must transmit the data block within the T4 interval. After transmitting the data block, the controlling station should expect one of the following responses within the T3 interval:

ACK1: An ACK1 indicates the data was received correctly. Within the T5 interval, the controlling station shall transmit an EOT to release control of the line.

NAK: A NAK indicates the data was not received correctly. Within the T5 interval, the controlling station shall retransmit the data block a maximum of three times before aborting the transfer by sending EOT to release control of the line. The protocol will resume at the line contention level (ENQ).

Protocol Examples

The following diagrams provide examples of how the PMS and vendor should use the protocol for data block transfer.

Normal delivery of data blocks

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

<---------- ACK0

(expect data block to begin within T4)

STX (text data) ETX BCC --->

(expect response within T3)

<---------- ACK1

(expect line release within T5)

EOT ---------->

(OK to ENQ immediately)

<---------- ENQ

.

.

.

The receiving station is ready to accept data and acknowledges the bid for the line and prepares to receive a data block. Upon receiving the data block and determining it is valid data, the receiving station acknowledges the data block. The controlling station then releases control of the line by transmitting the EOT. At that time, the line is considered uncontrolled and either station may attempt to gain control. However, the station that just released the line must wait the T interval before attempting to regain control.

Receiving station is busy

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

(receiver not ready)

<---------- NAK

(must wait T6 before another attempt)

ENQ ---------->

In this case, even though the receiving station is busy and cannot accept a data block at this time, it responds to the ENQ from the station attempting to gain control of the communication line. The station attempting to control the line should retransmit the ENQ after waiting the T6 interval. This process should continue until the receiving station gives permission to transmit the data message by responding with an ACK0.

No response from the receiving station

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

(nothing from receiver)

(ENQ after T2)

ENQ ---------->

(expect response within T2)

(nothing from receiver)

(ENQ after T2)

ENQ ---------->

(expect response within T2)

.

.

.

This condition most likely indicates either the receiving station is down (power off or in an off-line mode) or the communication line is down (communication hardware or cable problem). The station attempting to control the line should continue to retransmit the ENQ after the T2 interval has elapsed.

Negative response to a data block transfer

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

<---------- ACK0

(expect data block to begin within T4)

STX (text data) ETX BCC --->

(expect response within T3)

(receiver detects error)

<---------- NAK

(expect data block to begin within T5)

STX (text data) ETX BCC --->

(all is good this time)

<---------- ACK1

(expect EOT within T5)

EOT ---------->

In this example, the receiving station detects a receive error in the data block. The receiving stations NAK's the data block, and the controlling station sends the data block again. The receiving station then detects no error, and the data transfer continues in a normal fashion.

Continued negative responses to a data block

transfer

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

<---------- ACK0

(expect data block to begin within T4)

(initial try)

STX (text data) ETX BCC --->

(expect response within T3)

(receiver detects error)

<---------- NAK

(expect data block to begin within T5)

(1st retry)

STX (text data) ETX BCC --->

(expect response within T3)

(receiver detects error)

<---------- NAK

(expect data block to begin within T5)

(2nd retry)

STX (text data) ETX BCC --->

(expect response within T3)

(receiver detects error)

<---------- NAK

(expect data block to begin within T5)

(3rd retry)

STX (text data) ETX BCC --->

(expect response within T3)

(receiver detects error)

<---------- NAK

(expect data block to begin within T5)

(sender gives up)

EOT ---------->

In this example, the receiving stations detects an error in each successive attempt to transmit the data block. After the controlling station retries to send the message three times, it gives up, issuing an EOT to inform the receiving station that the control of the communication line is released.

No response to a data block transfer

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

<---------- ACK0

(expect data block to begin within T4)

STX (text data) ETX BCC --->

(expect response within T3)

(nothing from receiver)

(release control)

EOT ---------->

(wait for T1)

ENQ ---------->

.

.

.

In the event of no response to the data block, the controlling station shall terminate the transfer by releasing control of the data link. The transfer should begin again from the line contention level (ENQ).

No data block transferred

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

<---------- ACK0

(expect data block to begin within T4)

(nothing from sender)

If the station in control does not transmit the data block after receiving the ACK0, the line is assumed to be in an uncontrolled state, and data transfer must be restarted at the line contention level (ENQ).

No release of line control

(line has been idle for at least T1)

ENQ ---------->

(expect response within T2)

<---------------------- ACK

(expect data block to begin within T4)

STX (text data) ETX BCC --->

(expect response within T3)

<---------------------- ACK

(expect line release within T5)

(nothing from sender)

If the station in control does not release the line (transmit EOT), the transfer is complete and the line is assumed to be in an uncontrolled state.

26.108.4 Reconnecting PMS to NuPoint

If the property management system becomes disconnected from NuPoint due to a network disruption or other service problem, you must use the following procedure to manually reconnect the two systems and restore communication.

To manually reconnect PMS to NuPoint:

1. Launch an SSH client such as PuTTY.
2. Enter <NuPoint IP address> and press **Enter** to access the text console.
3. Log in as "root" and type the root password.
4. Exit to the Linux prompt.
5. Use the following script to restart the system:

sh /usr/vm/bin/restartPMS.sh

The system will be restarted and the connection between PMS and NuPoint will be restored. Communication will recommence.

26.108.5 Appendix - Diagnostic Specification

HIS/Encore PMS Integration

Reference: Document Part No. 2750-0009-00 "NuPoint Voice/Encore PMS Integration ENGINEERING SPECIFICATION"

Definitions

ACK	An ASCII control character used in the RS232C serial protocol for positive acknowledgement of a single character or full message packet.
CDR	A group of routines, data and files that allow the NuPoint Voice system to do call detailed recording of selected information for diagnostics.
cdrmenu	A NuPoint Voice routine that runs only when the system administrator requests to inspect or modify the CDR log file and/or configuration.
EECO	An OAA record that stores the configured data set up by eecomenu.
ENQ	An ASCII control character used in the RS232C serial protocol. It is used to request retransmission of the last character or full message packet.
eecomenu	A NuPoint Voice routine that runs only when the system administrator requests to inspect or modify the EECO OAA record for the HIS/Encore PMS integration.
hisinit	A NuPoint Voice routine that is started by hissnd to read though all mailboxes on the system and update message waiting for any with message waiting type 16.
hismwi	A NuPoint Voice routine that receives message waiting update requests from the mwla, reformats the data and requests hissnd to transmit the message across the serial link to the PMS system. Upon completion it reports the status back to the mwla.
hisrcv	A NuPoint Voice routine that receives the serial link data from the PMS system.

hisresync	A NuPoint Voice routine that is started by hisrcv if it receives a resync message from the PMS system. It sends a message to hissnd to start hisinit and then dies.
hissnd	A NuPoint Voice routine that sends data across the serial link to the PMS system.
mwla	A NuPoint Voice routine that oversees message waiting updates for all the message waiting integrations.
NAK	An ascii control character used in the RS232C serial protocol for negative acknowledgement of a single character or full message packet.
OAA	Open Account Administrator. The method to store NuPoint Voice mailbox and configuration data in 4K records.
PMS	Property Management System.
TTY	Tele-typewriter.

The purpose of this document is to explain the available diagnostic information for the HIS/Encore PMS Integration. The information is located in three areas: the log file, the CDR file and the system console. Any messages that are displayed on the system console are from the running tasks hissnd, hisrcv, hismwi or hisinit showing that they aborted and why.

Log File

When NuPoint Voice is running, there are two possibilities: the link is up or the link is down. When NuPoint Voice is booted, the PMS system integration software starts with the assumption the link is up. If the NuPoint Voice system sends any data over the link to the HIS/Encore PMS system and it is not acknowledged within two seconds, the data is resent for a maximum of four times. If still no acknowledgement, the NuPoint Voice system considers the link down and logs it. At any future time if the HIS/Encore PMS system sends valid data to the NuPoint Voice system, it is acknowledged and the link is considered up and it is logged.

At any time while NuPoint Voice is running, if a message waiting notification sent to the HIS/Encore PMS system fails due to an internal error, the mailbox number and message waiting state lost is logged.

If the NuPoint Voice system is requested to do a move message command (swap) and for any reason the event fails, it is logged with both the source and destination mailbox numbers. It is also possible during a swap that the source mailbox is deleted and can not be recreated. If this event occurs, it is logged with the mailbox number that is deleted.

To check the log file for information including HIS/Encore PMS integration:

1. From the console Main menu enter **(R) Report generation**.
2. Select **(L) Log file** and then select **(S) Show logfile**.

Log File Entries

"HIS PMS Link is up"

"HIS PMS Link is down"

"Unable to update MWI (ON/off) for mailbox (x)"

"Failed to swap mailbox (x) with (y)"

"Deleted mailbox (x), unable to re-create"

CDR File

While the NuPoint Voice system is running, **cdrmenu** provides an interface to cause selected information to be written to a CDR log file. For the HIS/Encore PMS system interface, the CDR level is 23, HIS/EECO/Encore PMS. It is useful to have this level active for short periods of time for full diagnostic monitoring of the integration. Listed below are methods to operate CDR.

The **cdrmenu** is accessed via menu options S-V from the main menu.

The data logged is from one of three active tasks and two short lived spanned tasks that make up the running programs of the HIS/Encore PMS system interface. The names of the tasks are hissnd, hisrcv, hismwi, hisinit and hisresync where hisinit and hisresync are the short lived spanned tasks. Each of these tasks when enabled with CDR level 23 logs data to the CDR file for specific events. Data logged by hissnd starts with "hissnd:" in the CDR file. Data logged by hisrcv starts with "HISRCV:" in the CDR file. Data logged by hismwi starts with "HISMWI:" in the CDR file. Data logged by hisinit starts with "hisinit:" in the CDR file. Data logged by hisresync starts with "HISRESYNC:" in the CDR file.

Level 22, HIS/EECO/Encore PMS

Messages logged at this level are logged for link and program level diagnostics. This level of diagnostics should not run on an unmonitored system. The CDR data logged is of a large quantity and may cause problems with disk utilization.

Some of the error messages logged are followed by task aborts. These messages are identified below by an additional comment line bracketed with asterisks. Any of the tasks below may abort, either during a system boot or while the system is in full operation. Only the tasks hissnd, hisrcv and hismwi will be restarted. It may be that the task immediately aborts again for the same or another error condition. After five aborts of a task, the system will auto reboot to try and solve the problem by re-initialization. The reason for the task abort is reported to the console and if CDR logging is enabled also to the CDR log file.

hissnd:

"hissnd: Link is up" (Link failure recovery)**"hissnd: Link is down"** (Link failure)	This data is logged at the same time and for the same reason as it is defined in the log file section above.
"hissnd: Link down condition, timeout" (Link failure)	This data is logged if after sending any form of message across the link, the PMS system does not reply even after four attempts. At this point the link is logged as down.
"hissnd: Configuration change" (Normal operation)	This data is logged after a message from eecomenu reports that the system administrator has changed the check-in or check-out mailbox configuration data. This information is passed on to hisrcv so it will reread the information from the disk file. It is this communication that allows changes to check-in and check-out handling without a system reboot.
"hissnd: Got send resync message" (Normal operation)	This data is logged when hissnd is redirected a message from hisresync via hisrcv. NuPoint Voice sends a resync message out on the RS232C serial link to the PMS system.
"hissnd: Got send MWI" (Normal operation)	This data is logged when hissnd is redirected a message from hismwi via hisrcv to update a mailboxes message waiting. NuPoint Voice sends a MW status message with the requested mailbox number, number of urgent and number of unplayed messages out on the RS232C serial link to the PMS system.
"hissnd: Got send bad mailbox" (Mailbox undefined in database)	This data is logged when hissnd is told by hisrcv to report the bad mailbox number. NuPoint Voice sends a bad mailbox message out on the RS232C serial link to the PMS system.

"hissnd: Store MWI command" (Normal operation)	This data is logged when hissnd is actively sending or hisrcv is actively receiving a message from the PMS system when a got send MWI command is delivered. The message can not be directly sent out over the link and is saved until the link becomes idle. Once idle, the MW status command is sent out and the entry is removed from the saved message state. At most one MW update can be held at any one time. This is because the mwla is not replied to until the MW status message is sent out, weather it was temporarily held on an active link state or not.
"hissnd: Add to bad mailbox queue" (Normal operation)	This data is logged when hissnd is actively sending or hisrcv is actively receiving a message from the PMS system when a got send bad mailbox is delivered. The message can not be directly sent out over the link and is saved until the link becomes idle. Once idle, the MW status command is sent out and the entry is removed from the saved message state. The entries are queued up and sent out in order as the link idle state permits. If the queue is full, any new bad mailbox messages are lost.
"hissnd: Send ACK" (Normal operation)	This data is logged immediately after one character is transmitted over the RS232C serial link. The character sent is an <ACK>, hex 06.
"hissnd: Send NAK" (Normal operation)	This data is logged immediately after one character is transmitted over the RS232C serial link. The character sent is a <NAK>, hex 15
"hissnd: Send ENQ" (Normal operation)	This data is logged immediately after one character is transmitted over the RS232C serial link. The character sent is an <ENQ>, hex 05.
"hissnd: Send (h)" (Internal error, report condition)	This data is logged immediately after one character is transmitted over the RS232C serial link. The character sent is in error and its value in hex is shown.
"hissnd: (m)" (Normal operation)	This data is logged immediately after one data packet is transmitted over the RS232C serial link. The packet sent should be of the form: <STX>message<ETX>LRC=l.

"hissnd: Received a bad request" (Internal error, report condition)	This data is logged when hissnd receives an unknown request from another task on the NuPoint Voice system. The task hissnd tries to get that task to be reset in an attempt to keep the condition from reoccurring.
"hissnd: Use hissnd $port [+hyatt]" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started without a port first parameter. The +hyatt is the optional setting that tells the software to interface to an Encore PMS system at 1200 baud. Without the setting, the software assumes to interface to a HIS PMS system at 2400 baud.
"hissnd: Bad RS-232 port name" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started with an undefined port parameter.
"hissnd: Unable to attach port" (Internal error or configuration error, check configuration and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started with a port number that can not be attached by this task. Check the configuration of all CPU serial ports of the system for conflicts. If the configuration is altered to repair the problem, reboot the system and monitor for recurrence.
"hissnd: Unable to attach name" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started and is not able to attach a task name for its use.
"hissnd: Unable to open serial port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started and it is not able to open the serial port that it just attached to this task.

"hissnd: Unable to get stty on RS-232 port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started and it is not able to get the current TTY options of the serial port.
"hissnd: Unable to SET stty on RS-232 port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started and it is not able to set the desired TTY options of the serial port. This includes baud rate, parity, data and stop bit settings.
"hissnd: Unable to SET device attributes for RS-232 port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hissnd is started and it is not able to set the desired device attributes for the serial port. This includes disabling break, X-on/X-off, escape and other features.

hisrcv:

"HISRCV: Checked in mailbox (x)" (Normal operation)	This data is logged when the PMS system sends valid data to change the configuration of mailbox (x). The changes to the mailbox are configured for FCOS. The changes to the mailbox are complete.
"HISRCV: Checked out mailbox (x)" (Normal operation)	This data is logged when the PMS system sends valid data to change the configuration of mailbox (x). The changes to the mailbox are FCOS, password, name recording, greeting #1 and messages. The changes to the mailbox are complete

"HISRCV: Swapped mailbox (x) with (y)" (Normal operation)	This data is logged when the PMS system sends valid move mailbox data to move source mailbox (x) to destination mailbox (y). Destination mailbox (y) is also swapped to source mailbox (x). The fields that are swapped are FCOS, password, text message count, all four mailbox greetings, name recording and all messages and message data. 1 **Note**: Because all message data is swapped, if messages in the mailbox are from other mailbox users (as apposed to outside callers), the source of the message may play as the wrong user name. This will happen if mailbox 100 sends a user message to mailbox 200 and then swaps to 101. At this time, the name recording for room 101 is now in 100 and so if user 200 listens to the source of the message it will say the name now associated with 100 (the old 101), the wrong name recording. This is not a problem when a message is left by an outside caller or with integrations that do not supply the calling number.
"HISRCV: Modified FCOS (f), MBOX (x)" (Normal operation)	This data is logged when the PMS system sends valid modify FCOS data packet. The FCOS number of the mailbox is updated to the requested value.
"HISRCV: Text update COUNT (c), MBOX (x)" (Normal operation)	This data is logged when the PMS system sends valid text message data packet. The text message count of the mailbox is updated to the requested value.

"HISRCV: Received a BAD MAILBOX (x)" (Mailbox undefined in database)	This data is logged if the PMS system sends any message packet that includes an undefined source mailbox number. It is invalid because the mailbox passed could not be found in the NuPoint Voice database. This message is discarded. No change to the mailbox database is made. The NuPoint Voice system responds by sending a bad mailbox packet to the PMS system.
"HISRCV: Received a BAD NEW MAILBOX (x)" (Mailbox undefined in database)	This data is logged if the PMS system sends a move mailbox message packet that includes an undefined destination mailbox number. It is invalid because the mailbox passed could not be found in the NuPoint Voice database. This message is discarded. No change to the mailbox database is made. The NuPoint Voice system responds by sending a bad mailbox packet to the PMS system.
"HISRCV: Received a BAD NEW MAILBOX (same number)" (Error in PMS system)	This data is logged if the PMS system sends a move mailbox message packet that includes the same source and destination mailbox number. This message is discarded. No change to the mailbox database is made. The NuPoint Voice system responds by sending a bad mailbox packet to the PMS system.
"HISRCV: No check in FCOS configured" (Check Nu Point Voice system configuration, configure PMS inte gration)	This data is logged if NuPoint Voice reads nonconfigured or invalid data configured for the PMS integration in the EECO OAA record.
"HISRCV: No check out or bad configuration" (Check NuPoint Voice system configuration, configure PMS integration)	This data is logged if NuPoint Voice reads nonconfigured or invalid data configured for the PMS integration in the EECO OAA record.
"HISRCV: Unable to lock source mailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to lock the source mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Unable to open sourcemailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to open the source mailbox record as part of the move mailbox message sent by the PMS system.

"HISRCV: Unable to delete source mailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to delete the source mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Unable to lock destination mailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to lock the destination mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Unable to open destination mailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to open the destination mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Unable to close destination mailbox (x)"	This data is logged when hisrcv is unable to close the destination mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Unable to create swapped source mailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to create the swapped source mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Unable to re-create original source mailbox (x)" (Internal error, report condition)	This data is logged when hisrcv is unable to re-create original source mailbox record as part of the move mailbox message sent by the PMS system.
"HISRCV: Failed to swap mailbox (x) with mailbox (y)" (Internal error, report condition)	This data is logged when hisrcv is unable to swap the source and the destination mailbox records during a move mailbox. This message follows the specific reason listed above listing the level of the failure in the swap.
"HISRCV: Invalid FCOS request (f)" (PMS system error)	This data is logged when hisrcv receives an invalid FCOS value in a modify FCOS message sent by the PMS system.

"HISRCV: Received an <ENQ> = send <NAK>" (Link failure, test link protocol using data scope)	This data is logged when hisrcv reads a first character from the RS232C serial port and it is an <ENQ>. This choice to send out a <NAK> is made if NuPoint Voice has already sent a message four times and the PMS system continues to reply with an <ENQ> rather than the expected positive result <ACK>. The information is sent by hisrcv to hissnd.
"HISRCV: Received an <ENQ> = send last msg" (Link failure, test link protocol using data scope)	This data is logged when hisrcv reads a first character from the RS232C serial port and it is an <ENQ>. This choice to send out the last message is made if NuPoint Voice has not sent this message four times with the PMS system continuing to reply with an <ENQ> rather than the expected positive result <ACK>. The information is sent by hisrcv to hissnd.
"HISRCV: Received an <ACK>" (Normal operation)	This data is logged when hisrcv reads a first character from the RS232C serial port and it is an <ACK>. The information is sent by hisrcv to hissnd.
"HISRCV: Received a <NAK>" (Link failure, test link protocol using data scope. If error is not consistent, suspect PMS system overload or stressed RS232C data connection)	This data is logged when hisrcv reads a first character from the RS232C serial port and it is a <NAK>. The information is sent by hisrcv to hissnd.
"HISRCV: (data packet)" (Normal operation)	This data is logged when hisrcv reads in any packet that begins with an <STX>. This message is displayed if it is a good or bad packet. The packet is shown in the format <STX>message<ETX>LRC=(h).
"HISRCV: BAD LRC" (Link failure, test link protocol using data scope)	This data is logged when hisrcv reads a packet from the RS232C serial port and the LRC passed in the packet does not match hisrcv's calculated LRC. LRC is defined as longitudinal redundancy check (XOR of all bytes after <STX> including the <ETX> character, with a 00Hex null seed).
"HISRCV: Received a Resynchronize" (Normal operation)	This data is logged when hisrcv reads a good resynchronize packet from the RS232C serial port.

"HISRCV: Received a Check-in or Check-out" (Normal operation)	This data is logged when hisrcv reads a good check-in or check-out packet from the RS232C serial port.
"HISRCV: Received a Message Waiting Status" (Normal operation)	This data is logged when hisrcv reads a good message waiting status packet from the RS232C serial port.
"HISRCV: Received a Move Mailbox" (Normal operation)	This data is logged when hisrcv reads a good move mailbox packet from the RS232C serial port.
"HISRCV: Received a Modify FCOS" (Normal operation)	This data is logged when hisrcv reads a good modify FCOS packet from the RS232C serial port.
"HISRCV: Received a Text Message MW" (Normal operation)	This data is logged when hisrcv reads a good text message MW packet from the RS232C serial port.
"HISRCV: Received a bad packet" (Link failure, test link protocol using data scope)	This data is logged when hisrcv reads a bad packet from the RS232C serial port. The information is sent by hisrcv to hissnd. The partial packet is displayed in a preceding message showing what data has been received, complete or incomplete.
"HISRCV: Received <STX> and then a timeout" (Link failure, test link protocol using data scope. If error is not consistent, suspect PMS system overload or stressed RS232C data connection)	This data is logged when hisrcv gets a two second timeout while trying to read the full packet length from the RS232C serial port. The data is thrown away and hisrcv resets to look for a first character.
"HISRCV: Received a good mailbox" (Normal operation)	This data is logged when hisrcv reads a good mailbox number in a check-in or check-out packet. The mailbox was able to be found in the open account database.

"HISRCV: Check in packet (x)" (Normal operation)	This data is logged when hisrcv reads a good check-in packet. The extension number (x) in the packet is used to read in the mailbox and change the state of the mailbox depending on the hismenu configuration. If hissnd has sent hisrcv a configuration change message, the data stored on disk by hismenu is reread before the changes to the mailbox are made. This allows the system manager to change how check-in and check-out effect mailboxes without a NuPoint Voice system reboot.
"HISRCV: Check out packet (x)" (Normal operation)	This data is logged when hisrcv reads a good check-out packet. The extension number (x) in the packet is used to read in the mailbox and change the state of the mailbox depending on the hismenu configuration. If hissnd has sent hisrcv a configuration change message, the data stored on disk by hismenu is reread before the changes to the mailbox are made. This allows the system manager to change how check-in and check-out effect mailboxes without a NuPoint Voice system reboot.
"HISRCV: Request MW for mailbox (x)" (Normal operation)	This data is logged if a valid check-out packet with an extension number that lead to a good mailbox was received. And if the current configuration in hismenu for the check-out packet is configured to delete all messages in the mailbox. A message is sent to the mwla to eventually return to hissnd turn off this station numbers message waiting.
"HISRCV: Ignored bad start character, HEX (h)" (Link failure, test link protocol using data scope)	This data is logged if hisrcv is looking for a start character and the character read in from the RS232C serial port is unknown. Valid start characters are <ENQ>, <ACK>, <NAK> and <STX>. The received unknown start character is displayed in hex and the packet is labeled bad.
"HISRCV: Incomplete packet" (Link failure, test link protocol using data scope)	This data is logged when the first characters of the packet (<STX>) has been read in successfully, but the two second packet timer expires before the full number of characters for a packet are read. The packet is labeled bad. The partial packet is displayed in a preceding message showing what data has been received, complete or incomplete.

"HISRCV: Unable to locate hissnd" (Internal error, may locate next transmission, else report condition)	This data is logged when hisrcv needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. Each time data is received over the data link from the PMS system, hisrcv retries to locate hissnd. If it is again unsuccessful, this message is again logged. At this point, the PMS system sees the link as down. When hissnd successfully restarts and attaches it's name, hisrcv and hismwi can locate it and link communication will proceed as expected.
"HISRCV: Unable to locate hissnd, data lost" (Internal error, message lost, report condition)	This data is logged when hisrcv needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. The data is lost and hisrcv continues to run looking for further link data. The PMS system is probably not getting any data from hissnd and so it will consider the link down. When hissnd successfully restarts and attaches it's name, hisrcv and hismwi can locate it and link communication will proceed as expected.
"HISRCV: Unable to send to hissnd, data lost" (Internal error, message lost, report condition)	This data is logged when hisrcv needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. The data is lost and hisrcv continues to run looking for further link data. The PMS system is probably not getting any data from hissnd and so it will consider the link down. When hissnd successfully restarts and attaches its name, hisrcv and hismwi can locate it and link communication will proceed as expected.
"HISRCV: Unable to re-send to hissnd, data lost" (Internal error, message lost, report condition)	This data is logged when hisrcv needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. It tries to send once to hissnd and fails, then it is temporarily able to attach by name to hissnd again, tries to send a second time and fails. The data is lost and hisrcv continues to run looking for further link data. The PMS system is probably not getting any data from hissnd and so it will consider the link down. When hissnd successfully restarts and attaches its name, hisrcv and hismwi can locate it and link communication will proceed as expected.

"HISRCV: Unable to read eeco OAA record" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started and it is not able to read from disk the configuration data set by hismenu.
"HISRCV: Use hissnd $port [+hyatt]" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started without a port first parameter. The +hyatt is the optional setting that tells the software to interface to an Encore PMS system at 1200 baud. Without the setting, the software assumes to interface to a HIS PMS system at 2400 baud.
"HISRCV: Bad RS-232 port name" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started with an undefined port parameter.
"HISRCV: Unable to open serial port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started and it is not able to open the serial port that it just attached to this task.
"HISRCV: Unable to get stty on RS-232 port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started and it is not able to get the current TTY options of the serial port.
"HISRCV: Unable to SET stty on RS-232 port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started and it is not able to set the desired TTY options of the serial port. This includes baud rate, parity, data and stop bit settings.

"HISRCV: Unable to SET device attributes for RS-232 port" (Internal error or serial port error, check serial port and report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisrcv is started and it is not able to set the desired device attributes for the serial port. This includes disabling break, X-on/X-off, escape and other features.

hismwi:

"HISMWI: MWI ON for station number (x)" (Normal operation)	This data is logged after the following task communication completes. The task mwla requests hismwi to send a message waiting request for station number (x). The task hismwi in turn requests hissnd to send out the specific message waiting packet. The task hissnd completes the packet transfer and replies to hismwi. At this time the CDR message is logged and hismwi replies to mwla.
"HISMWI: MWI off for station number (x)" (Normal operation)	This data is logged after the following task communication completes. The task mwla requests hismwi to send a message waiting request for station number (x). The task hismwi in turn requests hissnd to send out the specific message waiting packet. The task hissnd completes the packet transfer and replies to hismwi. At this time the CDR message is logged and hismwi replies to mwla.
"HISMWI: Unable to locate hissnd" (Internal error, may locate next transmission, else report condition)	This data is logged when hismwi needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. Each time data is received over the data link from the PMS system, hismwi retries to locate hissnd. If it is again unsuccessful, this message is again logged. When hissnd successfully restarts and attaches its name, hisrcv and hismwi can locate it and link communication will proceed as expected.

HISMWI: Unable to send to hissnd, data lost at level (x)" "HISMWI: Unable to turn MWI (ON/off) for mailbox (x)" (Internal error, message lost, report condition)	This data is logged when hismwi needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. The data is lost and hismwi continues to run looking for further link data. The PMS system is probably not getting any data from hissnd and so it will consider the link down. When hissnd successfully restarts and attaches it's name, hisrcv and hismwi can locate it and link communication will proceed as expected. The level number is for engineering use to determine which one of three levels of sending the failure occurred. The second half of the message informs what mailbox was involved and if message waiting failed for an on or off attempt.
"HISMWI: Unable to locate mwla" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hismwi starts and it tries to locate the mwla task and fails.
"HISMWI: Unable to locate mwla in loop" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hismwi tries to send a response to the mwla at any time and fails.

hisresync:

"HISRESYNC: Resync message sent" (Normal operation)	This data is logged when hisrcesync sends a resync message to the PMS system.
"HISRESYNC: Resync message failed" (Internal error, report condition)	This data is logged when hisresync fails to send a resync message to the PMS system.
"HISRESYNC: Unable to locate hissnd" (Internal error, report condition)	This data is logged when hisrcesync needs hissnd to send a resync message to the PMS system. The task hisresync returns to hisrcv without completing the command.

"HISRESYNC: Unable to send to hissnd, data lost" (Internal error, message lost, report condition)	This data is logged when hisresync needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. The data is lost and hisresync returns to hisrcv without completing the command.
"HISRESYNC: Unable to re-send to hissnd, data lost" (Internal error, message lost, report condition)	This data is logged when hisresync needs hissnd to send data allowing the link to stay active but the task hissnd can not be found by name. It tries to send once to hissnd and fails, then it is temporarily able to attach by name to hissnd again, tries to send a second time and fails. The data is lost and hisresync returns to hisrcv without completing the command.

hisinit:

"hisinit: Mailbox (x) MWI update" (Normal operation)	This data is logged for each mailbox in the system that has a message waiting type #16 (HIS PMS). This is the result of a resync command sent from the PMS system.
"hisinit: Exit mailbox resynchronize loop" (Normal operation)	This data is logged after all the mailboxes in the system have been scanned for the ones that have a message waiting type #16 (HIS PMS).
"hisinit: Unable to attach to HISINIT port" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisinit is started with a port number that can not be attached by this task.
"hisinit: Unable to locate mwla" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisinit tries to send a response to the mwla at any time and fails.
"hisinit: Unable to locate oaa" (Internal error, report condition)	*Error condition causes abort, error displayed on console and task restart* This data is logged when hisinit tries to send a response to the oaa at any time and fails.

26.109 Description

Record-A-Call (RAC) is an optional feature that allows mailbox subscribers to record both ends of a two-party external call in progress at their phone. Recorded conversations are delivered to the user's voice mailbox. Unlike regular voice mail messages, Record-A-Call messages are stored immediately as saved messages, so they do not trigger Message Waiting Indicators on the user's telephone.

Record-A-Call users require the Record-A-Call feature option enabled on their telephones and mailboxes.

Note:
Record-A-Call on Mitel MiVoice Business systems depends on softkey integration with the MiVoice Business systems via MiNET, so Record-A-Call does not work with integrations using Digital Media Gateways (formerly PIMGs). Record-A-Call does not depend on softkey integration with the 5000 CP. Also, Record-A-Call only works on the following ICP/Release combinations:

MiVoice Business ICP Software		Mitel MiVoice Office 250	
ICP Software	NP-UM Software	ICP Software	NP-UM Software
5.1 UR2 or later	9.0 or later	3.2 or later	4.0 or later

Record-A-Call interacts with Unified Messaging for both Standard UM and Advanced UM users. Record-A-Call messages will appear in the user's Web View. For Advanced UM users, a copy of the message is sent to the e-mail client.

26.109.1 Conditions

The following are conditions for the Record-A-Call (RAC) feature on the NuPoint Unified Messaging system when using a MiVoice Business or a MiVoice Office 250:

Note:
Record-A-Call should only be used in conjunction with the laws of the jurisdiction where the call is placed from, and/or the laws of the jurisdiction of the place being called. Mitel is not liable for use of this feature in a manner that does not conform with the applicable law (for example, laws involving wiretapping, eavesdropping, electronic surveillance, call recording, etc.). Dealers should warn customers in writing that they are responsible for the of use this feature in accordance with the law and that in many jurisdictions, both parties must be made aware that the call is being recorded in order.

Conditions for Record-A-Call on a MiVoice Business System

- Tones are not given to either party to indicate that the call is being recorded.
- Record-A-Call does not work with PIMG integrations.

- For best performance, Record-A-Call requires softkey event capability. However, if Record-A-Call is purchased without the Superset Softkey feature option, and is implemented on a MiVoice Business Release 5.1.3 or later, Record-A-Call is fully supported.
- Record-A-Call is limited to calls involving one trunk party and one RAC-enabled desk telephone. Record-A-Call softkeys are only functional when the telephone is connected to a trunk.
- The voice mailbox and telephone must be on the same network node.
- In order to receive Record-A-Call softkey events, NuPoint must register its telephones as 5240 devices, **except** the lines that are used for MWI, which must always be registered as 5020 devices. However, if the Record-A-Call feature is not installed, all telephones must remain registered as 5020 devices.
- In order for Record-A-Call to function, the COV/ONS/E&M Voice Mail Port feature must not be enabled in the Class of Service on incoming trunks. If the COV/ONS/E&M Voice Mail Port feature is enabled on the trunk of incoming calls, Record-A-Call will not work.
- Unlike regular voice mail sessions, Record-A-Call sessions do not time out after five seconds of silence in the conversation. In RAC sessions, 60 seconds of silence will cause automatic saving and termination of the Record-A-Call session.
- If the system goes out of service while a message is being recorded (that is, before the user saves the message), the message will not be available once the system is rebooted.
- A backup of voice mail messages will back up RAC messages just as it backs up regular voice mail messages. A backup and restore of the database will back up and restore the RAC option as well as any RAC FCOSs previously assigned to mailboxes. However, in an upgrade scenario where the previous software version is pre-release 9.0, the RAC licensable option is set to disabled by default. In this scenario, the RAC FCOS is also unassigned to any mailbox by default.
- If the Start Recording Automatically COS option is set to YES and the Record-A-Call user wishes to save the recording, the user must manually save by pressing the Save softkey before hanging up. If the Save Recording on Hang-up COS option is set to YES by the system administrator, the user's recording is saved automatically when the user hangs up. To avoid filling up the user's mailbox, the system administrator should use the Save Recording on Hang-up COS option with discretion.
- During the recording, if the Record-A-Call user presses the pause softkey, the recording stops. The recording can be paused for a maximum of ten minutes. At any time during this ten minute period, the user can resume the recording of the conversation.
- During the recording, if the Record-A-Call user places the call on hold, the recording stops. The recording does not automatically continue when the user retrieves the call from hold. If the user wishes to continue recording, the user must manually re-start the recording. Note that retrieving a call from hold, and restarting the recording generates two recordings for the call.
- During the recording, if the called party places the Record-A-Call user on hold, the recording continues.
- Record-A-Call has a 60-minute recording limit. When the recorded conversation reaches this limit, NuPoint saves the conversation and hangs up the call. The Record-A-Call softkeys disappear on the telephone (if the telephone supports softkeys) of the user who activated the recording session; however, the user remains in a two-way call with the called party. The user may start another Record-A-Call session, which is saved as another message, not appended to the previous message.
- If disk space runs out during a Record-A-Call session, NuPoint will stop the recording and save the message. If a Record-A-Call user's mailbox is full, the user will not be able to initiate a Record-A-Call session.
- Each Record-A-Call session requires three conference resources of the available 64 on the MiVoice Business ICP.

Conditions for Record-A-Call on a MiVoice Office 250 System

- Record-A-Call on the MiVoice Office 250 requires MiVoice Office 250 Release 3.2 or higher and NuPoint Unified Messaging 4.0 or higher.

- MiVoice Office 250 users are automatically assigned the MiCollab FCOS (14) which does not have the required feature bits. Add the following feature bits to the MiCollab FCOS:

  - **007** Pause in record or play
  - **022** Make to multiple destinations
  - **023** Make and mark confidential
  - **027** Give and mark confidential

26.109.2 Configuration

The Record-A-Call (RAC) feature requires programming on both the ICP and the NuPoint Unified Messaging server. The tasks for enabling the Record-A-Call feature for licensed users can be divided into the two following task groups:

- Configuration required for MiVoice Business or MiVoice Office 250 systems
- Configuration required for NuPoint UM

Configuration Required to Enable Record-A-Call on a MiVoice Business System

To enable the Record-A-Call feature for licensed users on the MiVoice Business , you must:

- Upgrade to MiVoice Business Release 5.1.3 or higher (includes MiVoice Business**Note**: Mitel has separate brands for its range of hardware and software-only solutions for the IP communications market. MiVoice Business is the brand name of the call-processing software that runs on hardware platforms such as the MiVoice Business ICP. The MiVoice Business ICP name continues as the brand for Mitel hardware platforms that run MiVoice Business software. MiVoice Business ICP Release 9.0 is the last software release under the old branding scheme; its successor is MiVoice Business 4.0. Release 4.0 or later)
- Purchase and enable the Advanced Voice Mail feature license.
- Configure voice mail integration ports that are representing NuPoint ports (other than MWI ports) as 5240 phone types. After configuring the phones to be 5240 types, reboot NuPoint so that it can re-register its sets. Note that telephones other than 5240 devices do not have sufficient softkey functionality and require additional feature key programming in order to support the Record-A-Call feature.
- Configure voice mail integration ports that are representing NuPoint ports (other than MWI ports) as 5240. **Note**: The MWI ports must remain as type 5020.
- Set the Record-A-Call Class of Service (COS) to "RAC Active - Yes" for the COS number applied to the user's telephone to enable Record A Call functionality on the user's telephone. Enable the other RAC COS options as required.
- Set the Recorder Hunt Group and add the appropriate voice mail ports as Recorder Hunt Group members.

For additional information or detailed procedures for enabling Record-A-Call on a MiVoice Business ICP system, refer to the *MiVoice Business System Administration Tool Help*.

Configuration Required to Enable Record-A-Call on a MiVoice Office 250 System

For configuration instructions for the MiVoice Office 250 system, refer to the *Mitel MiVoice Office 250 and NuPoint Integration Guide.*

Configuration Required to Enable Record-A-Call on the NuPoint UM Server

To enable the Record-A-Call feature for licensed users, you must

- Upgrade to NuPoint Messenger Release 9.0 or higher.
- Purchase the Record-A-Call Option.
- Reboot or re-activate the NuPoint system.
- Customize an FCOS to include the Record-A-Call feature bit **291**. For MiCollab deployments, add the Record-A-Call feature bit to FCOS 14. Do *not* include feature bit 122 (Define Broadcast Mailbox) in the FCOS.
- Assign the Record-A-Call FCOS to all mailboxes that will use the Record-A-Call feature.

Note:
Each Record-A-Call user's telephone and mailbox must have a Record-A-Call-enabled COS (PBX programming) and FCOS (NuPoint UM programming) assigned to it in order to be activated with the Record-A-Call feature.

26.109.3 Recorded Announcement Device (RAD)

Description

One application of Call Director is to create a Recorded Announcement Device (RAD) for a line group. Recorded Announcement Device (RAD) functionality eliminates the need for external tape machines or other audio-playing devices. RADs are commonly employed in ACD environments to automatically answer lines and deliver pre-recorded messages such as, "All of our representatives are busy helping other callers, please continue to hold to maintain your call priority." When the RAD message finishes playing, the caller usually hears music-on-hold while waiting for an agent to become available. RAD messages may also give the caller information that answers their questions, thus resulting in a 'good' abandoned call. They may also provide advertising or promotional information to callers while they're waiting for someone to take their call.

To configure RAD functionality, create a call flow containing any number of Message actions and assign it to a Line Group.

Conditions

The following conditions apply to the Recorded Announcement Device (RAD) feature:

- Use Call Director to create a call flow for line groups.
- When integrating NuPoint UM with a MiVoice Business ICP System, configure the NuPoint UM ports on the MiVoice Business ICP as 5240 IP devices if Record-A-Call is installed, and as 5020 IP devices if Record-A-Call is not installed.
- There cannot be more than one RAD per line group.
- To enable callers to press non-numeric DTMF keys such as # and * during playback of the RAD message, ensure that the ACD group interflow paths are configured correctly on the ICP.

Programming

To program a RAD using Call Director, see the Call Director online help topic *Voice Mail RADs*.

To access Call Director online help:

1. Open your browser, and enter ***<IP address or host name of the NuPoint UM server>*** **/npm-admin** and sign in with the administrator user name and password.
2. In the Web Console window, click the **Help** link in the upper right corner.

26.109.4 Softkeys - Description

The Voice Mail Softkeys feature allows users to control voice mail functions through context-sensitive keys on the telephone. This feature is available to NuPoint Unified Messaging systems that are integrated to:

- the MiVoice Business ICP (Release 5.1 UR 2 or later) using an IP integration
- the 5000 CP (Release 3.2 or later) using a SIP integration

Note:
The Softkeys feature is not supported for Digital Media Gateway (formerly PIMG) integrations.

26.109.5 Softkeys - Conditions

The following conditions apply to the Softkeys feature:

- Configuring Softkeys integration on the NuPoint UM server must be done using the **Text Console**.
- The Softkey feature option is available only to NuPoint UM systems that are integrated:
  - via IP to a MiVoice Business ICP, Release 5.1 UR 2 or later, or
  - via SIP to a MiVoice Office 250 , Release 3.2 or later
- Releases of the MiVoice Business ICP software prior to 5.1 UR2 have softkey functionality via the embedded voice mail feature; however, the NuPoint Softkeys feature can not be integrated with these earlier releases.
- All extension numbers enabled with the Softkey feature must be registered as 5020 or 5240 IP telephones on a MiVoice Business ICP system. Note that if you are configuring the Softkey feature for use with Record-A-Call optional feature, you may need to re-register the 5240 IP telephones accordingly. Refer to the Record A Call section for more information.

26.109.6 Configuring Softkeys on a MiVoice Business ICP System

For additional information or detailed procedures for enabling Softkeys on a MiVoice Business ICP system, refer to the *MiVoice Business System Administration Tool Help*.

To enable the Softkey feature on the MiVoice Business ICP:

1. Upgrade to MiVoice Business ICP Release 5.1 UR 2 or later. Releases of the MiVoice Business ICP prior to 5.1 UR 2 have softkey functionality via the embedded voice mail feature, however, the NuPoint Softkeys feature can not be integrated with these earlier releases.
2. Ensure that all the IP telephones representing NuPoint ports are registered as 5240 IP devices if Record-A-Call is installed or 5020 IP devices if Record-A-Call is not installed. If you need to re-configure the telephones, reboot NuPoint so that it can re-register its devices.
3. Note that you must add as many phones of type 5020 or 5240 as are programmed on the NuPoint Unified Messaging server. See Mapping New NuPoint Extensions and Voice Mail Ports to the MiVoice Business ICP.
4. Set the set registration access code to match the access code entered in the NuPoint Unified Messaging server during configuration of the softkey MiVoice Business ICP integration. See Configuring the MiVoice Business ICP Softkey Integration for more information.
5. In the MiVoice Business System Administration Tool, enable the following Softkey Class of Service (COS) fields in the COS assignment form that applies to the NuPoint Unified Messaging ports (i.e. the phones used as ports):
   - Voice Mail Softkey set to "Yes".
   - COV/ONS/E&M Voice Mail Port
   - HCI/CTI/TAPI Call Control Allowed
   - HCI/CTI/TAPI Monitor Allowed.
6. Set **Voice Mail Softkey** to "Yes" in the COS assignment form that modifies the user's IP phone. This enables softkey functionality on the phones that can support it.

26.110SMS Notification (UK Only) - Description

NuPoint Unified Messaging can also use Short Message Service (SMS) Notification to send text messages to mobile phones using the RS-232 interface. The NuPoint Unified Messaging system sends call information via the RS-232 interface to a PC running the SMS Notification application. This application sends an SMS notification to a GSM device (Global System for Mobile Communications), which calls the mobile phone and transmits a text message.

Note:
SMS Notification is available in the UK only. Beginning with NuPoint UM Release 4.1 and later, SMS programming must be done using the **Web Console**.

26.110.1 Configure SMS

To configure the programmable External Applications interface for SMS Notification:

Note:
You will need to configure the SMS Notifier server before SMS Notification will work. Refer to the SMS Notifier documentation for instructions to configure the SMS Notifier server.

1. From the navigation tree, click **Offline Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **External Applications** and select the Serial Port to use for SMS.
4. In the **Application** list, select **Programmable**and enter the following values:

   - In **Delay between requests**, enter **2**
   - In **Pre-DN ON string**, enter **ON** followed by a **space**
   - In **Pre-DN OFF string**, enter **OFF** followed by a **space**
   - In **Post-DN ON string**, enter **\R**
   - In **Post-DN OFF string**, enter **\R**
   - Set **Dept Code as DN ?** to **N**
   - Set **Unplayed number sent?** to **Y**
   - Set **Delay after Post-DN string** to **3**
   - Set **Suppress updates to MWL (y/n)** to **N**
5. Click**Save**.
6. In the navigation tree, select**Commit Changes and Exit**. Confirm the**commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

To complete the RS-232 configuration for SMS Notification, you must now assign the correct message waiting type to the mailboxes that will be using it:

1. Assign message waiting type **7** (programmable interface) through the first or second message waiting type prompt in mailboxes that are to receive message waiting indicator requests. See Assigning Message Waiting Indicators to a Mailbox.

You have now configured the NuPoint Unified Messaging system for SMS Notification to send text messages to mobile phones using the RS-232 interface.

26.110.2 External Application (RS232) Programmable Application Parameters

Parameter	Description	Value
Programmable Parameters		

Parameter	Description	Value
Initialization String	Enter the ASCII string required by the PBX. To create the string, consult the PBX operating manual or the PBX vendor for the correct code.	0-30 characters
Reply String	Enter the ASCII string sent by the PBX.	0-30 characters
Delay between requests	Enter the time to wait between requests.	0 - 255 seconds
Pre-DN ON string Pre-DN OFF string	If the PBX requires the string **before** the directory number (sometimes called extension number), create an ASCII string . If the PBX sends the string **after** the directory number: - enter a period (.) to delete an existing string, if necessary. - enter values for the Post-DN ON String and Post-DN OFF String parameters.	0-30 characters
Post-DN ON string Post-DN OFF string	If the PBX requires the string **before** the directory number (sometimes called extension number), create an ASCII string . If the PBX sends the string **after** the directory number: - enter a period (.) to delete an existing string, if necessary. - enter values for the Post-DN ON String and Post-DN OFF String parameters.	0-30 characters

Parameter	Description	Value
Department Code as DN	Select this check box to use the department code instead of the mailbox extension as the DN to turn lights on/off.	
Unplayed Number Sent	Select this check box to send the number of unplayed messages currently in a mailbox to be included after the mail-box number.	
Delay after Post-DN String	Enter the time to wait between Post-DN and Trailing String.	0 - 255 seconds
Ending Trailing String	If the PBX requires this string, create an ASCII string If the PBX does not require this string, enter a period (.) to delete an existing string.	0-30 characters
Suppress Updates to MWL	Select this check box to suppress updates of MWL after a user accesses the mailbox without changing status.	

Parameter	Description	Value
Modem Result Code	This modem result code will be used to compare against the actual result code returned from the modem after it has finished outdialing the MWI string. If they are not matched, NuPoint Voice will retry the MWI request again later on. **Recommendation**: For *better display* of CDR events, please turn OFF the Local Echo mode of the modem, ie. if the modem has dialed a MWI string like "ATDT*13658", it should not echo back this same string prior to returning the result code. If event messages for modem dial result are desired, enable "Pager" CDR in the Event Recorder menu.	See Valid String Characters table below.
Connection Settings		
IP Address	Enter the IP address of the remote system.	(Used for PMS configuration)
Server Port Number	Enter the port that the remote device/system is listening on.	

Valid String Characters

Character	Explanation
\b	Backspace
\f	Form Feed
\n	New Line

\r	Carriage Return
\t	Tab
\\	Backslash
\"	Double Quotes
\?	Question Mark

26.110.3 Speech Auto Attendant - Description

Note:
You configure SAA using Web Console.

Speech Auto Attendant (SAA) is a speech-enabled application that allows users to place calls to people quickly and efficiently by speaking their names. In addition to placing calls by name, users can say a department name or telephone number. A tutorial introduces users to the system features, and voice-based help is available to answer questions.

The SAA feature uses an automated attendant to route incoming calls based on spoken commands. Typically, you say the name of the person you want to speak to and the system transfers your call to the requested party.

SAA also supports up to 15 departments. When a callers states the word " Department " (to select a department), the caller hears, "The departments are..." followed by a list of department names. Upon hearing the list, the caller states the department name and is transferred to the department. If the Barge In command has been enabled, the caller can state the department name without having to listen to the list and be transferred directly. If no department names have been configured in the Speech Auto Attendant, the system states "there are no departments".

Note:
When callers say “Department”, NuPoint UM uses the Text To Speech (TTS) option to list the departments even though you may have recorded the department names. Callers can also ask for a particular department (for example, “Sales”). In this case, NuPoint confirms the department name using the recorded name, if available.

SAA can be installed as a standalone application (without any of the voice mail features included in NuPoint UM), or it can be installed along with NuPoint UM. When installed with NuPoint UM, SAA stores up to 4 telephone numbers per person and provides the user-configurable option of selecting which

number will be called. When installed as a standalone application, SAA stores 1 number per person, and this number is configurable only by the domain administrator.

SAA and Digital Media Gateway (formerly PIMG)

If you are planning to use the Speech Auto Attendant feature with the DMG integration, then you need to set the "Voice Activity Detection" option to **OFF** to ensure that the Speech Auto Attendant functions properly. See the *NuPoint Unified Messaging Technician's Handbook* for information about configuring DMGs.

SAA Users

There are three types of users for the Speech Auto Attendant feature: the system administrator, registered users, and unregistered users. Each of these users can perform a specific set of SAA tasks. See Users for more information.

User Data Source

SAA can connect and interact with Microsoft Active Directory, the MiCollab , or with the NuPoint system mailboxes. For systems that are installed with NuPoint UM, the default data source is NuPoint UM, and all user mailboxes with FCOS bit 92 assigned are included in the data source. NuPoint UM administrators may also select Active Directory as the data source. For MiCollab systems, the data source is always MiCollab. For standalone systems, the default source is Active Directory.

SAA Languages

The supported prompt languages for Speech Auto Attendant are North-American (NA) English, British (UK) English, Canadian French, and European French. The bilingual option allows you to combine any two of the four languages, setting one as Primary language and one as Secondary. Callers are prompted first in the Primary language and then in the Secondary. When properly configured, the Bilingual option allows callers who speak a language name (or an extension number) in the secondary language to be automatically prompted in that same language. Callers may also select a language using the dial pad.

Note:
For MiCollab installations, supported languages are North-American (NA) English and British (UK) English only.

For system and department prompts, you can use the default greetings, import customized greetings, or you can record your own prompts.

Note:
Names that include accents (especially the French *accent grave*) may not be pronounced correctly by the Speech-to-Text engine before you record your own name. See Name Pronunciation During Playback for more information.

SAA Licensing

SAA is an optional feature that must be licensed in order for the configuration fields to be enabled. SAA licensing includes the required number of telephony channels and the Text-to-Speech (TTS) core license that is required for all speech-enabled applications. (Note: The TTS core licensing is shared with the Advanced UM feature.) Licensing is performed on a per-user basis. When the maximum number of licensed users is reached, the administrator receives a warning message that indicates the number of users who are excluded. All licensing is done through the Mitel Applications Management Center (AMC). For more information about the AMC, see Planning and Licensing and the *NuPoint UM Technician's Handbook*. When you add additional licenses to the system, you must restart the server.

Line Group Configuration

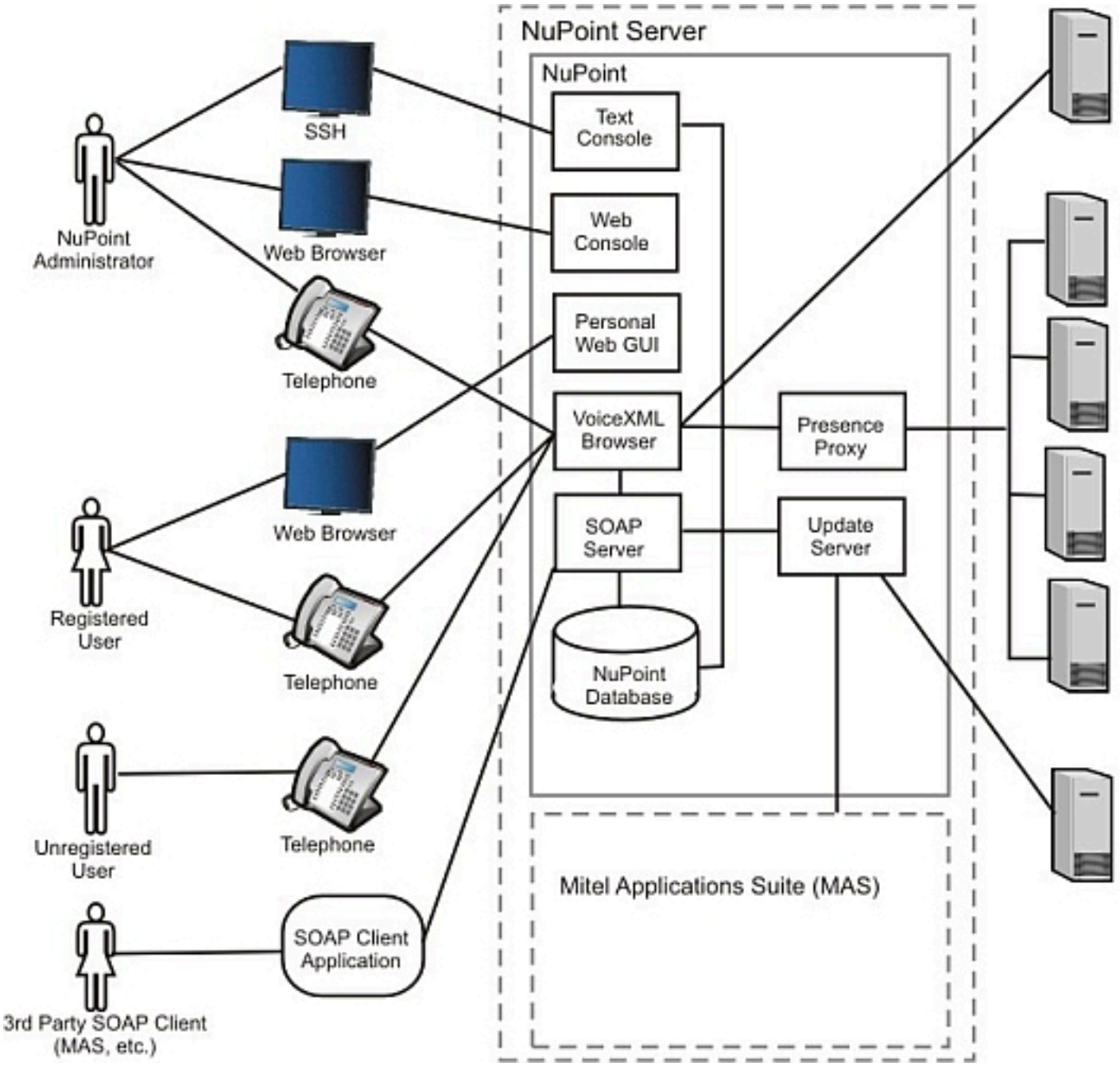
The speech-enabled channels are configured through Line Group assignment. A new type of Line Group is added to indicate that all the channels inside the line group are speech-enabled channels. The licensing of the total number of speech telephony channels is cross-checked when you configure the speech-enabled channels.

SAA System

The diagram below illustrates the high-level system layout. The following table lists components and their relationships to SAA:

Speech Auto Attendant		Outside Speech Auto Attendant	
Admin Web Console	Speech-Recognition service	Microsoft Active Directory	Mitel Unified Communications Server
Web View interface	Update Server	Microsoft LCS 2005 Server	Mitel Application Suite
VoiceXML Browser	NuPoint database	Microsoft OCS 2007 Server	telephony network and users web browsers
Text-to-Speech engine	Grammar files	Lotus Sametime Server	third-party VoiceXML applications

Note:
Microsoft OCS R2 (formerly Office Communications Server 2007 Release 2) is not supported for Release 4.0 of NuPoint UM.



26.110.4 Speech Auto Attendant Users

The Speech Auto Attendant feature has the following user types:

- NuPoint UM Administrator
- Registered User
- Unregistered User

Each of these users can perform a specific set of Speech Auto Attendant tasks. The sections below describe the applicable tasks for each user.

NuPoint UM Administrator

The NuPoint UM Administrator performs the following Speech Auto Attendant tasks:

- Installs, upgrades and uninstalls NuPoint and the Speech Auto Attendant;
- Backs up and restores the Speech Auto Attendant configuration and prompts;
- Configures the user data source;
- Manages departments that can be reached by name;
- Manages system and department prompts for the Speech Auto Attendant;
- Manages the Speech Auto Attendant dialling policies;
- Configures the Speech Auto Attendant and speech recognition engine parameters;
- Configures speech recognition line groups, ports and MiVoice Business ICP integration;
- Changes the default telephone number where a registered user will be reached from the Speech Auto Attendant;
- Configures the default extension of the live operator.

While using the Admin Web Console to manage system or department greetings and prompts, please note the following:

- Upon successful installation of SAA of the language of your choice, 3 standard system prompts are already available;
- Upon successful addition of new departments, TTS generated department prompts will also be available;
- The system and department prompts should be managed by using both the Admin Web Console and login to SAA by means of an internal trusted telephony;
- To play, import, silence or restore to default, please first hang up from the telephony session and use the Admin Web Console (Auto-Attendant/Prompts Recording);
- To play or to record, please log on using an internal trusted phone with the administrator PIN and ensure that you are logged out of the Admin Web Console. After successfully recording the prompts using an internal trusted phone, please re-login to the Admin Web Console to verify the status of each of the prompts.

Registered User

A registered user is a licensed user whose name can be recognized by the Speech Auto Attendant.

A Speech Auto Attendant registered user performs the following tasks:

- Uses a spoken name, spoken digits, or DTMF keys to call someone;
- Performs the first-time caller dialog;
- Records the user name;
- Changes the default telephone number to be reached at from the Speech Auto Attendant.

Unregistered User

An unregistered user is an unlicensed user whose name is not recognizable by the Speech Auto Attendant.

A Speech Auto Attendant unregistered user can only perform the following task:

- Uses a spoken name, spoken digits, or DTMF keys to call someone.

26.110.5 Speech Auto Attendant Features

This topic describes the following SAA features:

- Input Options
- Calling Line Identification
- Confidence Thresholds
- Barge-In
- Tutorial
- Presence
- Disambiguation
- Custom Pronunciation
- Error Handling
- Time-out

Input Options

SAA supports the following input options:

- **Spoken name**: a caller simply says the name
- **Keypad DTMF**: using the keypad to enter digits
- **Spoken DTMF**: speaking the DTMF digits

Some users may use mixed input throughout the call. Input variations include the use of universal commands (such as "help" or "operator"), retry, no input, re-prompt and barge-in.

Refer to the *NuPoint Unified Messaging User Guide* for more information about input options.

Caller Line Identification

The Speech Auto Attendant can distinguish the origin of a call based on the Caller Line Identification (CLID) of the caller and then play the appropriate greeting for that call.

1. **Note:** Three types of system greetings (prompts) can be recorded for the Speech Auto Attendant: Internal Greeting, External Greeting, and Expert Greeting. Refer to Prompts for instructions to record these greetings.

There are four types of callers:

- **Internal trusted caller:** This type of caller places a call from inside the company's telephony network and the caller ID is recognized as an Auto-Attendant user. The system then plays the trusted greeting (the "bingbing" earcon prompt).

- **External trusted caller:** This type of caller places a call from outside the company's telephony network and the caller ID is recognized as an Auto-Attendant user. The system then plays the trusted greeting (the "bingbing" earcon prompt).

- **Internal non-trusted caller:** This type of caller places a call from inside the company's telephony network and the caller ID cannot be recognized as an Auto-Attendant user. The system then plays the internal non-trusted greeting ("Who would you like to call?").

- **External non-trusted caller:** This type of caller places a call from outside the company's telephony network and the caller ID cannot be recognized as an Auto-Attendant user. The system plays the external non-trusted greeting ("Welcome. You are speaking to the auto attendant which uses your voice to direct your call. Say the name of the person or department with whom you would like to speak.")

Note: Barge-In is enabled by default for all three greetings.

All numbers that are configured in the administration web console are trusted. All of the user's desktop directory numbers (extensions) are internal-trusted. All of the alternative numbers under that user (e.g. cell phone, home phone) are also trusted.

All directory numbers (extensions) that do not have a user associated with them (e.g. a phone in a conference room) are all internal non-trusted.

Confidence Thresholds

The system recognizes speech at two confidence levels: low and high.

A low confidence level results when the system does not recognize a requested name, number, or department and instructs the caller to repeat the call request.

A high confidence level results when the system recognizes a requested name, number, or department and thus transfers the call to the appropriate destination.

Confidence thresholds are used to determine whether explicit or implicit confirmation is required. These thresholds are determined by the configurable low/high confidence levels. Refer to Basic Speech Recognition Parameters for confidence level threshold configuration. For troubleshooting help, see Confidence Threshold Recommendations.

Barge-In

This feature allows users to interrupt a system prompt with a speech or keystroke command. The Speech Auto Attendant stops playing the prompt and responds to the command. Barge-in allows experienced system users to skip quickly through the prompts.

Barge-in uses the standard universal commands such as "cancel", "help", and "operator". Experienced users can barge in with voice or DTMF at greetings and questions. Barge-in applies to all three input options.

The system administrator can enable or disable barge-in on a system-wide basis. Refer to Basic Speech Recognition Parameters for configuration.

This single system-wide barge-in configuration is applicable for the following four scenarios:

- During initial greetings (any of the three greetings);
- During the two levels of re-prompt in cases of no input and recognized result below low confidence;
- During the confirmation question of explicit confirmation;
- During the prompting of the implicit confirmation.

Refer to the *Messaging User Guide* for more information about the barge-in feature.

Tutorial

SAA provides a tutorial for new users that allows them to record their name when the Speech Auto Attendant application is configured with a NuPoint Unified Messaging system.

The tutorial is only available to registered internal and external trusted callers. Barge-in will be turned off for first-time callers throughout the tutorial. Trusted callers will be forced to record their name the first time that they call the system. First-time callers are forced to listen to the tutorial to its completion before making any calls.

SAA detects a first-time user only by the CLID of the user's registered desktop phone.

Presence

SAA provides the ability to determine, and optionally play back, the current presence state of the matched person prior to transferring the caller.

Note: The Presence feature is only supported when SAA is configured to use Microsoft Active Directory as its user data source.

The Release 4.0 Presence feature supports the Microsoft Live Communication server (LCS 2005 SP2), Office Communications server 2007 , Lotus Sametime 8.0, and Mitel Unified Communications Server.

The caller is prompted with the current presence status of the person called. The presence information is for reference only, and calls are transferred regardless of the presence status of the called party. Standard universal barge-in commands such as "cancel" and "help" during a call transfer are supported.

Presence status information is optional. It is enabled by default for both internal and external callers, and is independent of whether the caller is trusted or non-trusted. It can be turned off using the **Presence for Internal Callers** and **Presence for External Callers** check boxes in the Web Console. For more information, see the Presence section.

Disambiguation

The Speech Auto Attendant provides the ability for calls to be automatically transferred to the operator for multiple directory matches (for example, two people named "John Doe" in the same directory). Callers will only be notified of duplicate names but not prompted to choose a specific one. Callers will be immediately transferred to the operator and will be asked for more details in order to transfer the call to the right person.

If two or more people have names that sound the same, or are the same, the system transfers the caller to the operator, who can then resolve the ambiguity by asking for the department or location of the person being called.

Custom Pronunciation

The custom pronunciation tool allows administrators to customize name pronunciation. For example, if you want to have a user named Mickey Mouse also recognized as Mickey Rodent, you can add a pronunciation of "rodent" for the word "mouse". When a user calls and says either "mouse" or "rodent", Mickey Mouse will be recognized. Multiple pronunciations can be added for each user. Bilingual pronunciations can also be customized (for example, you can also add a pronunciation of "souris" for "mouse".)

You can add nicknames, such as equating "Bill" or "Will" with the name "William".

You can also add phonetic representations of a user's name. For example, an English SAA system will have a higher match rate for the name "Benoit" when you add a phonetic pronunciation (like "benwah") to its dictionary. See Custom Pronunciations for configuration instructions.

Error Handling

SAA responds to an error by instructing the user to retry the command. After two recognition errors, the system transfers the caller to the operator.

Callers are directed back to the main menu or to the operator as governed by the confidence level of recognition and system errors.

Timeout

SAA times out when it detects no speech or DTMF input, and triggers help prompts to be played to the user. The length of the timeout period is configurable in the Basic Speech Recognition Parameters section.

26.110.6 Speech Auto Attendant Installation

The Speech Auto Attendant can be installed along with NuPoint Unified Messaging or as a standalone application, without any of the voice mail features included in the NuPoint UM product.

The following blades are required to install the Speech Auto Attendant feature:

Option	SAA with NuPoint UM	Standalone SAA
Base SAA	NPUM Speech Attendant	NPUM Speech Attendant
Speech Recognition	Up to two of the following:	Up to two of the following:
(Default is bilingual)	- NPUM Speech Recognition American English	- NPUM Speech Recognition American English
	- NPUM Speech Recognition British English	- NPUM Speech Recognition British English
	- NPUM Speech Recognition Canadian French	- NPUM Speech Recognition Canadian French
	- NPUM Speech Recognition Euro French	- NPUM Speech Recognition Euro French

Option	SAA with NuPoint UM	Standalone SAA
Text-to-Speech	Select up to two blades that match the selected Speech Recognition blades: - NPUM TTS American English - NPUM TTS British English - NPUM TTS Canadian French - NPUM TTS Euro French	Select up to two blades that match the selected Speech Recognition blades: - NPUM TTS American English - NPUM TTS British English - NPUM TTS Canadian French - NPUM TTS Euro French
Full Set Prompts	- Extended set of prompts as required for NuPoint operation	- not required. (Standalone SAA prompts are included in the Speech Recognition blade.)

Installing SAA with NuPoint UM

Speech Auto Attendant software installation is automatic when NuPoint Unified Messaging software is being installed. See the *NuPoint Unified Messaging Technician's Handbook* for NuPoint UM software installation instructions.

Installing SAA as a Standalone Application

You can install the Speech Auto Attendant as a standalone application in one of two ways:

- by clicking the "NPM Master Installer" blade link in the server manager Blades panel, which installs only the packages for which the system is licensed.
- by clicking the "NPM Speech Attendant" blade install link in the server manager Blades panel, which installs the Auto Attendant (including the English recognition package).

To complete the installation, install the appropriate Speech Recognition blades and Text-to-Speech blades.

See Installing an Optional Feature for software blade installation instructions.

Installing SAA Text-to-Speech Package

SAA has a dependency on the Text-to-Speech (TTS) language. The TTS language you install must match the installed Speech Recognition language. TTS is an optional feature that requires licensing. You must purchase at least one TTS license for SAA functionality.

See Installing an Optional Feature for software blade installation instructions.

Installing Additional Speech Recognition Applications

In this release, only the Auto Attendant application is bundled with the system. You can also install other speech recognition applications through the MSL Blades panel. Once a speech recognition application blade is installed, the application will be displayed as an option in the list of speech recognition applications, along with the Auto Attendant.

In order to install an extra speech recognition application on the NuPoint UM system, you must first buy or license it (some applications may also be available for free). You then need to navigate to the MSL Blades panel, find the application in the list and click the "Install" link.

When the installation is completed, the new speech recognition application will be available in the line group form. See Configure a Speech Recognition Line Group.

Note:
Some speech recognition applications have special requirements to configure some parameters or restart services in order to be fully functional. Refer to the documentation provided with the speech recognition application for this information.

Upgrading from a Previous Release of NuPoint UM

Speech Auto Attendant was introduced in NuPoint Unified Messenger Release 12.0. If you are upgrading from Release 11.0 or earlier, you need to perform the following steps to upgrade the system and install the Speech Auto Attendant feature:

1. Acquire the proper licenses to upgrade to the latest NuPoint UM release and to install the Speech Auto Attendant feature.
2. Upgrade the operating system.
3. Upgrade the NuPoint UM system. The software upgrade will install the new NPM Base Speech Auto-Attendant blade automatically if the system is properly licensed.
4. Install the appropriate NPM Speech Auto-Attendant English Text-to-Speech package.

See the *NuPoint Unified Messaging Technician's Handbook* for full instructions.

26.110.7 Configuration Overview

Speech Auto Attendant configuration consists of the following tasks:

Task:	Reference:
1. Set SAA Language and basic speech parameters	Basic Speech Recognition Parameters
2. Set up an administrator password	Administration Parameters
3. Create a speech recognition line group	Configure a Speech Recognition Line Group
4. Define a User Data Source	About User Data Source
5. Configure the User Data Source update schedule	User Data Source Parameters
6. (Optional) Add departments	About Departments
7. (Optional) Add prompts	About Prompts
8. (Optional) Add a dialing policy	About Dialing Policies
9. (Optional) Configure presence	Presence

Task:	Reference:
10. (Optional) Add custom pronunciations	Custom Pronunciations
11. (Optional) Install Active Directory Snap-in	Install AD Snap-in

26.110.8 Planning and Licensing

When a Speech Auto Attendant (SAA) license is purchased and assigned to a user, that user can be configured as one of the following:

- internal trusted
- private internal trusted

Note that licenses are required for both users *and* departments; SAA can support up to fifteen departments.

Type of user/ caller/mailbox	SAA License Required?	Recognizable by SAA?	FCOS Mailbox	Name Field	Typical Use
Administrator	N	Y	N/A	N/A	The SAA administrator role is installed by default and cannot be removed. Its purpose is to execute administrative functions. **Notes**: • To access administrative functionality, call into the system from any internal trusted phone and say "administrative functions," then enter the Administrator PIN. • The administrator does require a mailbox by the name "Administrator." • "Administration" is also a common department name.
Internal trusted user/caller	Y	Y	FCOS bit 92	Proper format	Typical users in the organization whose name should be recognizable by SAA.

Type of user/ caller/mailbox	SAA License Required?	Recognizable by SAA?	FCOS Mailbox	Name Field	Typical Use
Internal trusted users/caller (private)	Y	N	Without FCOS bit 92	Proper format	Public figures in the organization (such as the CEO or executives) who want to use SAA but do not want to be reachable.
Internal non-trusted user/caller	N	N	Without FCOS bit 92	N/A (No mailbox assigned)	Conference rooms or the lobby.
External caller	N	N	Without FCOS bit 92	N/A (no mailbox assigned)	Callers from the public network.
Non-SAA licensed mailbox	N	N	N/A	To assign a name to the mailbox without consuming an SAA license, insert an underscore between the first and last name.	Mailboxes whose owners do not want to consume SAA license.

Mailbox Name Format

When completing the SAA mailbox name field, use the following format:

- the field should *not* be blank (please note that although the name field is optional for mailboxes, it is mandatory for SAA)
- the field should contain, as a minimum, a first and last name
- the name should be pronounceable in the choice of language installed (primary and secondary: en-US, en-UK, fr-CA, fr-FR)
- if a title is included, it should be in long form (Mister, not Mr.)
- the following special characters/spacing can be used:
  - firstname[sp]lastname (Donald Duck)
  - lastname[,]firstname (Pan,Peter)
  - firstname[sp]middlename[sp]lastname (Winnie the Pooh)
- hypens, dots and honorifics are permitted; however, if an honorific is included, it should be in long form (Mister, not Mr.)

- initials are permitted but not desirable (J R is recognized as "J R")

Note:

- Even with FCOS bit 92, if an SAA name field is improperly configured, its mailbox will not use an SAA license and will not be recognized by SAA. To avoid this common error, enter a properly formatted SAA mailbox name.
- If only the first name is programmed (no last name), the mailbox will not become an internal trusted and will not be recognized by SAA, even with FCOS bit 92.
- If the number of departments exceed 15, each additional department can be assigned a mailbox as a "internal trusted user" in order to have its department name made recognizable by SAA. In essence, this enables the system to treat the departments as people. Note that:
  - a license is still consumed for the extra department
  - when callers say "department," any departments not listed in the departments configuration page will not be played back.
  - the department names field does not follow the same format as the name field of mailboxes. Single-word names (such as Sales or Payroll) are allowed.

26.110.9 Mailbox Names and SAA Recognition

If you are using NuPoint UM as your data source, when you configure mailbox settings you must add a name to the mailbox Name field. If the field is blank, the mailbox cannot be used for the SAA user.

Note:
In order for SAA to ring the extension of the recognized called party, you must configure both the phone number and a pronounceable name.

Enter mailbox names according to the following specifications:

- As a minimum, specify a First name followed by a Last name separated by a space. Both names are required as a name cannot be recognized by SAA if only one word exists in the mailbox Name field.
- The maximum combined characters for the First name, Last name, and middle name (separated by commas) is 31.
- The maximum number of characters for the First name, Last name, and Middle name are 29, 29 and 27 respectively.
- The minimum number of characters for the First name, Last name, and Middle name is 1.
- You cannot enter digits 0-9.
- Letters are not case sensitive.
- Common names and special characters, such as apostrophes, hyphens, and periods, are permitted (for example, St.).

- The name should be pronounceable in the language selected (en-US, en-GB, fr-CA, fr-FR).
- Single letters are permitted for First names and Last names.
- The first word, if it is not followed by a coma, is the First name.
- The last word, if it is proceeded by coma, is the First name.

After you manually update the information

- Under "Current Users" verify the names are recognizable.
- Verify the licensing of users and departments to confirm they are included.
- Verify the names by calling into SAA before deployment. (Due to the varying format of user names in the world (different origin, country, translation and language issues), and the source of data (typically from a company database or spreadsheet), you must pay special to non-typical names.)

Examples

Examples of Acceptable Mailbox Name Entries		
Case	**Example**	**Recognized by saying**
Case 1: First name followed by a spaces then Last name	Donald White	"Donald White"
Case 2: First name of one character only followed by a space then Last name	W Smith	" W Smith"
Case 3: First name one character in length followed by a period and a space then Last name	W. Smith	" W Smith"
Case 4: Last name followed by a comma and space then First name	Smith, Harold	"Harold Smith"
Case 5: First name followed by a space then Middle name(s) followed by a space(s) then Last name	W G Smith	"W G Smith"

Special Considerations for Department Names

SAA supports a maximum of 15 departments within its Department List. SAA can support additional departments if they are defined as Mailbox Users. In that case, the additional departments would not appear in the Department List playback, but would be available for speech recognition, similar to system users. Since the department would defined using a mailbox, the mailbox name would need to consist of two words to be recognized by SAA.

26.110.10 Configure a Speech Recognition Line Group

To add a speech recognition line group to your system configuration:

1. From the navigation tree, click Offline **Configuration > Edit Offline Configuration**. The Offline Configuration navigation tree opens.
2. When prompted to **Duplicate Active Configuration**, click **Yes**.
3. In the navigation tree, click **Line Groups** and then click **Add**.
4. Configure the following parameters:

   - **Number:** Add a number for the line group or click on the Next Available button to add an unused list number.
   - **Name:** Enter a name for the line group.
   - **Application:** Select "Speech Recognition" from the list of available applications. The Speech Recognition Application field appears. Note: This line group option is not available if the system is not licensed for speech recognition.
5. On the Speech Recognition tab,

   - **Speech Recognition Application:** Select the application that corresponds to this line group. This list will be populated according to the speech recognition applications that are currently available on the NuPoint Unified Messaging system. If you select the "VoiceXML Application", then the VoiceXML Start URL field will appear. Enter the URL of the VoiceXML application in this field.
   - **Attendant's Extension:**Enter the extension number that callers can dial to contact an operator.
6. On the Lines tab, click **Add**.
7. Configure the following additional parameters:

   - **Line Triplet:** Enter a line number for the line group or click on the Next Available button to add an unused line number.
   - **Number of Lines:** Enter the number of lines in this line group.
   - **PBX:** Select the PBX to use for this line group.
   - **Mapping:** In a multi-node system, enter the module number, line card number, or port designator to add to the line group.

   Note:
   Support for multiple-module servers (e.g. NPM UM 640) was discontinued with NuPoint Release 6.0.

8. Click **Add** to save the configuration data.

9. Click **Save** to add the new line group to the list of existing line groups. A confirmation message regarding the configuration changes appears.
10. In the navigation tree, select **Commit Changes and Exit**. Confirm the **commit**. Your changes are now saved to the duplicate (inactive) configuration. Configuration changes will not take effect until you have activated the inactive configuration.

26.110.11About User Data Source

The user data source is the system from which Speech Auto Attendant retrieves its list of users. The available sources are:

- **NuPoint UM**: this is the default user data source when installing a new NuPoint Unified Messenger system with the Speech Auto Attendant feature. All NuPoint UM mailboxes on the local server that have an FCOS with feature bit **92** assigned are included in the NuPoint UM data source.
- **Microsoft Active Directory**: use this LDAP data source for NuPoint UM or standalone systems if you are planning to use the Presence feature of SAA.
- **Lotus Domino**: use this LDAP data source when the NuPoint UM system is integrated with Lotus Notes.
- **MiCollab**: this is the user data source for SAA when installed with the MiCollab version of NuPoint UM.

You must specify only one user data source.

When a system has been configured for a particular user data source, modifying that data source configuration affects multiple users on the system. For that reason, the user data source fields are disabled in order to prevent accidental changes. User data source configuration can be specifically modified using the Modify the User Data Source procedure.

Note:
Changing data source configuration causes all users of the system to be initialized.

Some user data sources do not provide a mechanism for SAA to detect changes and refresh its user list. After adding, modifying, or deleting users, the changes may not be effective until the next scheduled automatic refresh (as configured in the Speech Auto Attendant parameters). You can force a manual refresh of the system in order to update the SAA user list before the next scheduled automatic refresh. See Update the User Data Source for more information.

Note:
The Speech Auto Attendant feature requires that you enter the accented character for proper recognition of the spoken name. Ensure that your data source contains the accented characters. See Mailbox Names with Accented Charactersfor more information.

26.110.12 Define a NuPoint User Data Source

The current NuPoint UM system is the default user data source when you install a new NuPoint UM system with the Speech Auto Attendant feature.

When the Speech Auto Attendant user data source is configured for the current NuPoint Unified Messaging system, then you can specify the default Speech Auto Attendant number using the Web console. A field entitled "Auto-Attendant Default Extension" appears in the General tab when you edit a mailbox in the Advanced mode. You can select the default number from the list of configured phone numbers.

Note:

- Speech Auto Attendant can only fetch users from the NuPoint UM system on which it resides. It cannot retrieve users from a remote NuPoint Unified Messaging system.
- The "Auto-Attendant Default Extension" field will not appear in the administration web console if Speech Auto Attendant is not installed, or if the user data source is not configured to fetch information from the current NuPoint UM system.

To configure the user data source for the current NuPoint UM system:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Data Source**. The User Data Source window appears.
3. In the **Source Type** field, select **NuPoint** from the drop-down menu.
4. Click **Save**.

The system automatically selects every mailbox that is enabled with FCOS bit **92** (Dial-by-Name database) and a properly formatted display name for the Speech Auto Attendant user data source.

26.110.13 Define an Active Directory User Data Source

You can also choose to retrieve users from an existing Microsoft Active Directory server for the Speech Auto Attendant user data source. Both technologies use the LDAP protocol to look up/retrieve information.

To configure the user data source for Active Directory:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Data Source**. The User Data Source window appears.
3. In the **Source Type** field, select **Active Directory** from the drop-down menu. The data source configuration fields for the LDAP server appear.
4. In the **LDAP Server Address** field, enter the fully qualified domain name (FQDN) of the LDAP server OR its IP address, OR the root Directory Server Entries (DSE).

Note:
To use the FQDN of the data source server or a root DSE, the NuPoint UM system must be configured to communicate with a DNS server that can resolve the FQDN of the LDAP server or root DSE.

5. In the **LDAP Search Base** field, enter the location in the Active Directory data structure from which the list of users should be fetched. **Note**: You can select the **Recursive** check box to tell the Auto-Attendant to browse sub-directories of that location (context) in the data structure.
6. In the **LDAP Object Classes** field, enter the LDAP entities that will be retrieved and used in the Auto-Attendant. You can specify alternate object classes if the LDAP server is configured to use the sub-class of the user. You can enter multiple object classes in this field, separated by commas.
7. In the **LDAP SAA Private User Attribute** field, enter the LDAP server Extended Attribute used to identify users as Private. (For example, the LDAP database might use an attribute called "extensionAttribute10" to hold the True or False flag for Private User? In this case, you would enter **extensionAttribute10** in this field.)
8. In the **LDAP SAA User Attribute** field, enter the LDAP server Extended Attribute used to identify SAA enabled users. (For example, the LDAP database might use an attribute called "extensionAttribute11" to hold the True or False flag for SAA User? In this case, you would enter **extensionAttribute11** in this field.)
9. In the **LDAP SAA Default User Extension Attribute** field, enter the LDAP server Extended Attribute used to identify the extension or telephone number to direct SAA calls to. (For example, "extensionAttribute12" may contain a reference to "homeTelephone" or "mobile". These are variables that are associated with telephone numbers in the LDAP database.
10. In the **LDAP Administrator DN** field, enter the administrator user credentials in order to retrieve data from the LDAP server.
11. In the **LDAP Login Password** field, enter the administrator password in order to retrieve data from the LDAP server.
12. Click**Save**.

The system automatically selects every mailbox that is in the specified LDAP server data structure for the Speech Auto Attendant user data source. All users matching the configuration parameters will be picked up for the user data source.

You can exclude specific users from the Speech Auto Attendant user data source through the optional Active Directory Snap-In.

You can click the **Test Connection** button to test the connection for the current configuration. This test can take a few minutes to execute depending on various parameters (network latency, LDAP server performance, etc.). A dialog shows the progress and reports validity of the connection. In the case of an invalid connection, a message indicating the source of the connection problem is displayed.

26.110.14 Define a MiCollab User Data Source

You can also choose to retrieve users from an existing MiCollab server for the Speech Auto Attendant user data source. **Note**: Only users from the local MiCollab server can be retrieved. The Auto-Attendant cannot retrieve users from a remote MiCollab server.

To configure the user data source for the MiCollab server:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Data Source**. The User Data Source window will appear.
3. In the **Source Type** field, select **MiCollab** from the drop-down menu.
4. Click **Save**.

The system picks up every public user of MiCollab configured on this server for the Speech Auto Attendant user data source.

Note:
The “ MiCollab ” user data source item is not available if MiCollab has not been installed on the server.

26.110.15 Modify the User Data Source

You can modify the user data source configuration for the Speech Auto Attendant using the Edit button.

Note:

- Changing the data source configuration will cause all users of the system to be re-initialized.

- The **Force Update** button will be disabled while editing the user data source.

To modify the user data source:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Data Source**. The User Data Source window appears.
3. Click **Edit**. The User Data Source fields become enabled.
4. Modify the data source type or configuration parameters as required.
5. Click **Save**. A confirmation dialog appears.
6. Click **OK** to confirm the changes.

The Speech Auto Attendant user data source is refreshed upon saving the modifications. The users from the new data source are available after a few minutes.

26.110.16 Update the User Data Source

Some user data sources do not provide a mechanism for Speech Auto Attendant to detect changes and refresh its user list. After adding, modifying, or deleting users on the system, the changes may not be effective until the next scheduled automatic refresh (as configured in the Speech Auto Attendant User Data Source Schedule Parameters on page 1430). You can force a manual refresh of the system in order to update the Speech Auto Attendant user list before the next scheduled automatic refresh.

To force a manual refresh of the system, follow the steps below:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Data Source**. The User Data Source window will appear.
3. Click **Force Update**. The system refresh will begin and a progress window will appear.

The system refresh may take a few minutes to complete. When the refresh is complete, the date and time of the update will appear in the right-hand corner of the User Data Source window.

26.111About Current Users

Current users are those users who have been configured for the Speech Auto Attendant user data source. You can view all current users, search for particular users, or export the list of users to a .CSV file.

The Speech Auto Attendant feature is licensed on a per-user basis. When the maximum number of users allowed by the license is reached, a warning message is displayed indicating the number of users that are being excluded from the user list.

Departments count toward the maximum number of users allowed by the system. They are given higher priority than individual users when determining which entries to exclude from the user list. If the maximum number of licensed users has been reached, the system allows you to continue to add departments to a maximum of 15. When you do a forced update, users who originally had SAA functionality may be excluded from SAA to make room for the newly-added (higher priority) departments.

The user data source allows private users to be defined. Private users are usually public figures, owners or directors of a company, who do not want people to reach them directly. People marked as "private" in the user data sources are not included in the Speech Auto Attendant user list for privacy purposes, but are considered as trusted users when calling the system. Private users count toward the maximum number of users allowed by the license.

Re-using an SAA Mailbox Number

When you use NuPoint as your data source, SAA-recorded information for mailboxes is maintained until the mailbox is deleted and the user data source is updated. If a forced update is not performed, a mailbox number that is being re-used may continue to play the original recorded greeting.

To delete a mailbox and the associated recording, you must perform the following steps:

1. Delete the mailbox.
2. Perform a forced update.
3. Add the new user information to the old mailbox number.
4. Perform a forced update.
5. Have the new user run the SAA tutorial and record the new SAA name.

26.111.1 Find Current Users

You can view a list of users currently configured for the Speech Auto Attendant feature, or you can search for specific users.

Note:

- The user data displayed will vary according to the configured data source type. On a system configured with NuPoint Unified Messaging as the user data source, the user name and extension number will be displayed. For Active Directory systems, the user's work extensions will be displayed. For MiCollab systems, the user's main telephone number will be displayed.
- Private users are identified with a padlock icon next to their name.

To view a list of configured users:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Current Users**. The Auto Attendant Current Users window appears displaying the list of users configured for the Speech Auto Attendant feature. The users will be displayed in a read-only list, which will be sorted alphabetically.

To search for specific users in the Speech Auto Attendant user data source:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Current Users**. The Auto Attendant Current Users window appears.
3. In the **Find** field, enter the name or extension of the person you want to locate.
4. Click **Search**. The information for that user will appear if the user resides in the Speech Auto Attendant user data source. If the user is not in the user data source, then a "No users found matching this criteria" message will appear.

26.111.2 Export Current Users

You can export the list of currently-configured SAA users to a .CSV file.

To export the user list:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu appears.
2. Click **Current Users**. The Auto Attendant Current Users window appears displaying the list of users configured for SAA.
3. Click **Export**. The File Download window appears.
4. Click **Save**and select a location for the file. Rename the file if you want.
5. Click **Save**. The file is saved to the specified location in .CSV format.

Note:
The export function always exports the full list of users, no matter what search may have been performed before. The exported user list is sorted alphabetically.

26.112 About Departments

Speech Auto Attendant can support up to 15 departments in the user data source. Departments are defined by a name and a telephone number, and are sorted alphabetically in the department list window. Departments can be added, edited, or deleted from the user data source.

Note:
Departments count toward the maximum number of users allowed by the system. They are given higher priority than individual users when determining which entries to exclude from the user list. If the maximum number of licensed users has been reached, the system allows you to continue to add departments to a maximum of 15. When you do a force update, users who did have SAA functionality may be excluded from SAA in order to make room for newly-added (higher priority) departments.

26.112.1 Add a Department

You can add up to 15 departments to the Speech Auto Attendant user data source.

Departments count toward the maximum number of users allowed by the system. They are given higher priority than individual users when determining which entries to exclude from the user list. If the maximum number of licensed users has been reached, the system allows you to continue to add departments to a maximum of 15. When you do a forced update, users who originally had SAA functionality may be excluded to make room for newly-added (higher priority) departments.

To add a department to the user data source:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Departments**. The Departments window appears.
3. Click **Add**.
4. In the **Name** field, enter the department name (mandatory). If your system is configured for a Bilingual language, enter the department name as spelled in both the Primary and Secondary languages.

Note:
You can also enter the name of a greeting, but you are limited to characters that can be handled by the speech recognition software. These are the letters from A to Z and spaces. No other characters are allowed.

5. In the **Number** field, enter the telephone number of the department (mandatory).
6. Click **Save**. The new department is added to the list.

Note:
Modifications to the departments do not take effect on the system until the next scheduled automatic update. You can force a manual update by clicking the **Force Update** button. A dialog appears to inform you that the update is in progress. The date and time of the update appear in the right-hand corner of the window and are refreshed as the department information is updated. The **Force Update** button is disabled if no changes were made to the departments since the last update.

26.112.2 Edit a Department

You can edit the name or telephone number of an existing department, one at a time.

To edit department information:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.

1. Click **Departments**. The Departments list appears.
2. Select a department from the list and click **Edit**.
3. Edit the department information as required.
4. Click **Save**. The department information is updated in the list of departments.

Note:
Modifications to the departments do not take effect on the system until the next scheduled automatic update. You can force a manual update by clicking the **Force Update** button. A dialog appears to inform you that the update is in progress. The date and time of the update appear in the right-hand corner of the window and are refreshed as the department information is updated. The **Force Update** button is disabled if no changes were made to the departments since the last update.

26.112.3 Delete a Department

You can delete a department from the existing list of departments, singly, or all departments at one time.

To delete a department from the department list:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Departments**. The Departments list appears.
3. Select a department or departments from the list and click **Delete**. A confirmation dialog for the deletion appears.

4. Click **OK** to confirm the deletion. The department is deleted from the list.

Note:
Modifications to the departments do not take effect on the system until the next scheduled automatic update. You can force a manual update by clicking the **Force Update** button. A dialog appears to inform you that the update is in progress. The date and time of the update appear in the right-hand corner of the window and are refreshed as the department information is updated. The **Force Update** button is disabled if no changes were made to the departments since the last update.

26.113 About Prompts

Speech Auto Attendant prompts are customized greetings that can be recorded or imported so that a specific greeting will be played to callers.

There are two types of prompts:

- **System prompts**: standard auto attendant greetings (Internal Greeting, External Greeting, or Expert Greeting) that are played when a call comes into the system.
- **Department prompts:** specific auto attendant greetings that are played when a caller chooses to call a specific department.

You can import prompts that are shipped with the SAA feature or you can record your own. You can also play and silence (delete) greeting prompts.

26.113.1 Prompt Languages

Speech Auto Attendant supports the following languages:

- North American English (NA)
- UK English (UK)
- Canadian French
- European French

The **bilingual** option of SAA allows you to combine any two of the four languages, setting one as Primary language and one as Secondary. Callers are prompted first in the Primary language and then in the Secondary. Callers have the option of speaking the name of their preferred language, or saying an extension number in their preferred language. The system then returns prompts in the caller's preferred language.

Notes:

- Internal callers are not given a language option. They are prompted in the primary language only.
- Mailbox settings always override Line Group settings. For example, if you configure a Line Group to be bilingual and then assign a custom LCOS with an alternate language to a mailbox, callers will receive

prompts in the mailbox's language, irrespective of which of language they selected when they first reached the system.

- SAA cannot control the language of prompts outside the SAA call flow (for example, in a line group or the user's mailbox).
- If you change primary and secondary languages, you must perform a reactivation.

For more information about configuring bilingual languages, see Basic Speech Recognition Parameters.

26.113.2 Record a Prompt

Speech Auto Attendant prompts can be recorded so that callers hear customized greetings. You can record either system prompts or department prompts.

Note:
If no prompts are recorded, then the system plays the default prompts.

To record a prompt:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Prompts Recording**. The Speech Auto Attendant Prompt window appears.
3. In the **Category** field, select the type of greeting prompt to record (System prompt or Department prompt).
4. In the list of system prompt or department prompt greetings, select a greeting to record.
5. Click **Record**. A window with recording instructions appears.
6. Following the onscreen instructions, call into the system on a speech recognition port and say “Administrative functions”.
7. Enter the administrator pass code using DTMF keys (as set in the Administrator PIN field of Administration Parameters).
8. Record the system greeting or department greeting. The maximum recording length of a greeting is 2 minutes.
9. Click **Save**. The status for the greeting will change to "Recorded" in the list of greetings and the greeting will be effective immediately.

Note:

- All greeting prompts recorded into Speech Auto Attendant are normalized and trimmed to ensure good cohesion with the rest of the Auto Attendant prompts. Prompts are normalized to the RMS value of 2200. Trimming drops any silence (signal below a power of 300) at the beginning and end of prompts.
- You can revert back to the default prompts (factory settings) by clicking **Restore Default** if you are not satisfied with your recording. This action discards your recording and resets the greeting prompt to the default setting.
- If callers are consistently being transferred to the Attendant for help, check the No Speech Time-out value programmed on the Basic Speech Recognition Parameters page. It should be at least 5 seconds longer than the recorded greeting.

26.113.3 Import a Prompt

You can import a prompt instead of recording one manually. You can import either system prompts or department prompts.

Note:
The supported audio file formats are 8 kHz A-Law and m-Law WAV files (as with Call Director).

To import a prompt:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Prompts Recording**. The Speech Auto Attendant Prompt window appears.
3. In the **Category** field, select the type of greeting prompt to import (System prompt or Department prompt).
4. In the list of system prompt greetings or departments, select a prompt for which to import the greeting.
5. Click **Import**. The Import Template window appears.
6. Browse to the location of the audio file of the greeting template to import and enter the path in the template filename field.
7. Click **OK**. A progress dialog will appear to display the status of the audio file upload. Once the file upload is complete, the status for the greeting will change to "Recorded" in the list of greetings and the greeting will be effective immediately.

Note:

- All greeting prompts recorded into the Speech Auto Attendant are normalized and trimmed to ensure good cohesion with the rest of the Auto Attendant prompts. Prompts are normalized to the RMS value of 2200. Trimming drops any silence (signal below a power of 300) at the beginning and end of prompts.
- You can revert back to the default prompts (factory settings) by clicking **Restore Default** if you are not satisfied with your recording. This action discards your recording and resets the greeting prompt to the default setting.
- If you are unable to import a prompt file, verify that your web browser security settings are correct. To do this, click the **Start** button and type **Internet Options** in the search box. Select the **Security** tab and click the **Custom Level** button. In the **Miscellaneous** section, ensure that **Display mixed content** is set to **Prompt**. If **Display mixed content** is disabled, the import process will fail.

26.113.4 Play a Prompt

You can play the recorded prompt for a system or department greeting over a media player. (The default media player for Microsoft Windows is the Windows Media Player.)

To play a prompt, follow the steps below:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Prompts Recording**. The Speech Auto Attendant Prompt window appears.
3. In the **Category** field, select the type of greeting prompt to play (system prompt or department prompt).
4. In the list of system prompt or department prompt greetings, select a greeting to play.
5. Click **Play**. The prompt will be downloaded and played over your media player.

26.113.5 Silence a Prompt

You can silence a recorded or default system or department prompt. This means that no greeting plays for that prompt.

Note:
Silencing a prompt deletes the recording for that prompt.

To silence a prompt:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.

1. Click **Prompts Recording**. The Speech Auto Attendant Prompt window appears.

2. In the Category field, select the type of greeting prompt to silence (system prompt or department prompt).
3. In the list of system prompt or department prompt greetings, select a greeting prompt to silence.
4. Click **Silence**. A confirmation dialog will appear.
5. Click **OK** to silence (delete) the greeting for that prompt. The greeting prompt is now deleted and the status for the greeting will change to "Silence" in the list of greetings. The silenced greeting is effective immediately.

26.114 About Dialing Policies

Note:
For MiCollab NuPoint UM systems, the Dialing Policies menu is not present in the Web Console interface. **Dialing policies must be configured through the MiCollab interface**.

For standalone NuPoint UM systems:

To prevent users from treating the Auto Attendant feature as a long distance call proxy, dialing policies can be used to program rules and determine what numbers can be dialed from the Auto Attendant. The dialing policy also allows numbers to be rewritten before the system places the call.

When making a telephone call, the phone number selected by the user is evaluated against a set of dialing policies to determine whether it is an extension, a local phone number, a long distance number or an international number. The phone number is evaluated against the dialing policies one at a time, from top to bottom. The first dialing policy that matches the phone number determines the call type.

In order for the phone number to match a dialing policy, the phone number being evaluated must start with the same numbers as the ones entered in the “Prefix” column. These numbers must then be followed by the quantity of digits (N), as determined by the “Quantity to Follow” column.

When a phone number matches a dialing policy, the following logic is applied to determine the phone number that will be dialed by the system. First, N numbers are removed at the front of the phone number. The “Prefix to Inject” is then inserted in front of the phone number. The resulting number is what will be dialed if the user policies allow for that type of call.

The table below lists the default dialing policies:

Prefix	Quantity to Follow	Quantity to Remove	Prefix to Inject	Type
1800	7	0	9	Local
800	7	0	91	Local

Prefix	Quantity to Follow	Quantity to Remove	Prefix to Inject	Type
1888	7	0	9	Local
888	7	0	91	Local
	10	0	91	Long Distance
	12	0	91	Long Distance
	7	0	9	Local
	3	0		Extension
	4	0		Extension
	5	0		Extension
	6	0		Extension

You can add, edit, delete, move, and test a dialing policy.

Add a Dialing Policy

Note:
Dialing policies for MiCollab NuPoint UM must be configured through the MiCollab interface.

To add a dialing policy:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Dialing Policies**. The Auto Attendant Dialing Policies window appears.
3. Click **Add**. The Adding an Auto-Attendant Dialing Policy window appears.
4. In the **Prefix** field, enter the character(s) that must exactly match the characters at the beginning of the dialed phone number (from zero to eleven characters; valid characters are “0” to “9”).

5. In the **Quantity to Follow** field, enter the number of characters that must follow the prefix (an integer from 0 to 11).
6. In the **Quantity to Remove** field, enter the number of characters to be removed from the front of the dialed phone number (an integer from 0 to 11).
7. In the **Prefix to Inject** field, enter the character(s) to insert at the beginning of the dialed phone number (from zero to eleven characters; valid characters are “0” to “9”).
8. In the **Type** field, select the type of call to which this dialing policy applies.
9. Click **Add**. Clicking the Add button adds the new policy at the end of the list.

Note:
The added policy does not become effective until you click the **Save** button. This allows you to test the policy before enabling the changes. See Test a Dialing Policy.

Edit a Dialing Policy

You can edit configured dialing policies one at a time.

To edit a dialing policy:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Dialing Policies**. The Auto Attendant Dialing Policies window appears with a list of the configured dialing policies.
3. Select a dialing policy to edit.
4. Click **Edit**. The Edit an Auto-Attendant Dialing Policy window appears with the existing parameters for the selected dialing policy.
5. Edit the parameter configuration as required.
6. Click **Save**. The new parameters will be applied to the dialing policy.

Note:
The configuration changes will not be effective until you click the **Save** button. This allows you to perform some tests before enabling the changes. See Test a Dialing Policy.

Delete a Dialing Policy

You can delete configured dialing policies, singly, or all at once.

To delete a dialing policy:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Dialing Policies**. The Auto Attendant Dialing Policies window appears with a list of the configured dialing policies.
3. Select a dialing policy to delete. (You can select multiple or all dialing policies.)
4. Click **Delete**. A confirmation dialog for the deletion appears.
5. Click **OK** to confirm the deletion.

Note:
The deletion does not take effect until you click **Save**.

Move a Dialing Policy

You can order the dialing policies in the sequence against which you want the dialed telephone number to be matched. Several dialing policies can be moved up or down within the list at one time.

To move a dialing policy:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Dialing Policies**. The Auto Attendant Dialing Policies window appears with a list of the configured dialing policies.
3. Select a dialing policy to move. You can select several dialing policies to move up or down within the list at one time. The order of the selected dialing policies will be maintained when moving multiple policies at a time.
4. Click either **Move Up** or **Move Down** to move the dialing policies in the desired manner. The selected policies will then move up or down by one line in the list.

Note:
The change in the dialing policy order does not take effect until you click **Save**.

Test a Dialing Policy

It is recommended that you test the dialing policies you have configured before making them effective.

To test the configured dialing policies:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Dialing Policies**. The Auto Attendant Dialing Policies window appears with a list of the configured dialing policies.

3. In the **Enter a Phone No to test** field, enter a test telephone number to dial.
4. Click **Simulate**. The telephone number is matched against the configured dialing policies and the result (the call type and the resulting number that would be dialed) is displayed in the Results field.

Note:
When you are satisfied with the configured dialing policies, click **Save** to enable them on the system. A confirmation dialog appears to confirm the changes.

26.115 About Miscellaneous Parameters

Speech Auto Attendant configuration also includes the setting of various system-wide parameters. These parameters are used to configure and optimize the Speech Auto Attendant settings.

The following categories of miscellaneous parameters can be configured:

To configure these items:	Refer to this Category:
• Prompt language • Confidence thresholds • Barge-in • Output volume	Basic Speech Recognition Parameters
Determine which users can make which calls	Dialing Policy Parameters
Set up scheduled data source user list updates	User Data Source Parameters
Enable presence for internal/external callers; presence integration	Presence Feature Parameters
Admin password configuration	Administration Parameters

26.115.1 Basic Speech Recognition Parameters

The basic speech recognition parameters are used system-wide and are shared by all speech recognition applications hosted on the NuPoint UM system.

Note:
Some applications may overwrite these parameters and may, or may not, allow overwritten parameters to be configured. Refer to the documentation for the speech recognition application installed on your system for specific configuration details.

To configure basic speech recognition parameters:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Misc. Parameters**. The Auto Attendant Parameters window appears.
3. In the **Category** field, select **Basic Speech Recognition** from the drop-down menu.
4. Configure the following parameters (or click Use Default Valueto apply the default.)
5. **Primary Language**: By default, this value is set to the System Language. For Bilingual language systems, prompts are presented in this language first and then in the secondary language. You can switch primary and secondary languages to change the order of presentation.

Note:
NOTE: If you change Primary and Secondary language, you must perform activation.

- **Secondary Language**: For Bilingual language systems, select the secondary language, or select **Disable** to configure a unilingual system.
- **Low Recognition Confidence Level:** This value specifies the relative confidence level below which speech recognition results are rejected. The minimum value is 0 and the maximum value is 1, with a two-digit precision. The default value is 0.5.
- **High Recognition Confidence Level:** This value specifies the relative confidence level above which speech recognition results are implicitly confirmed. The minimum value is 0 and the maximum value is 1, with a two-digit precision. The default value is 0.8.
- **No Speech Timeout (in milliseconds):** This value specifies the length of silence that will trigger a help prompt to be played to the user. The minimum value is 0 and the maximum value is 60,000 milliseconds (60 seconds). The default value is 20,000 milliseconds (20 seconds).

Note:
You may need to change the default No Speech Timeout value to a higher value if external callers are consistently slow to respond. As a rule of thumb, the No Speech Timeout value should be about 5 to 8 seconds longer than the recorded external greeting.

- **Post-Speech Silence (in milliseconds):** This value specifies the length of silence that must follow an utterance before the speech recognition engine begins to process it as a complete sentence. The bigger this value is, the longer the pauses are allowed from the users. The minimum value is 0 and the maximum value is 60,000 milliseconds (60 seconds). The default value is 1000 milliseconds.
- **Output Volume:** This value specifies the linear volume that is applied to the output signal before prompts are played back to the users. You can use this parameter to adjust the volume when the

signal played to the users is too weak or too loud. The minimum value is 0.0 and the maximum value is 100.0. The default value is 100.0.

- **Speech vs. Accuracy:** This value specifies the relative priority of speech vs. accuracy. Using high accuracy algorithms requires more CPU resources and thus limits the number of concurrent speech recognition sessions. The minimum value is 0.0 and the maximum value is 1.0. Entering “0.0” places the emphasis on speed, while entering “1.0” places the emphasis on accuracy. The default value is 0.5.
- **Sensitivity:** This value allows you to configure the level between background noise and speech, and thus it controls the sensitivity of the speech detector. The minimum value is 0.00 and the maximum value is 1.00. Values approaching 1.00 improve the detection of speech but also increase the detection of background noise and thus utterances need to be spoken with a strong voice so as not to be mistaken with background noise. The default value is 0.5.
- **Barge-In:** This field allows you to enable or disable barge-in for the entire speech recognition engine (that is, the Speech Auto Attendant and every other installed speech recognition application). Barge-in is enabled by default.
- **Note:** Even if barge-in is enabled, speech recognition applications can choose to disable barge-in during portions of their dialogs. If barge-in is disabled, no application can use barge-in.
- **Prompt Normalization:** All greeting prompts recorded into the Speech Auto Attendant will be normalized to ensure good cohesion with the rest of the Auto Attendant prompts. Prompts will be normalized to the RMS value of 2200.
- **Prompt Trimming:** All greeting prompts recorded into the Speech Auto Attendant will be trimmed to ensure good cohesion with the rest of the Auto Attendant prompts. Prompt trimming will drop silence (signal below a power of 300) at the beginning and end of the prompts.

6. Click **Save**. The configured parameters will now be set to the selected values.

26.115.2 Confidence Thresholds

The system categorizes speech recognition with two confidence levels: low and high. Each utterance is analyzed and assigned a confidence value between 0.0 and 1.0, according to how well the system was able to match it with a word or name in its vocabulary.

When a confidence value meets or exceeds the "high" confidence level, the system recognizes the requested name, number, or department unambiguously and transfers the call to the appropriate destination.

When an utterance receives a confidence value below the "low" confidence level, the system does not recognize the requested name, number, or department and instructs the caller to repeat the call request.

When a confidence value falls between these levels, the system will seek explicit confirmation of its best match with the user before transferring the call.

The confidence thresholds can be adjusted using the configurable low/high confidence levels. **The default values are appropriate for most installations**. The following table outlines observed behavior and lists recommended actions:

Observation	Recommendation
Many calls result in confirmation requests with the expected name match. (Attendant says, "I heard <name>. Is that correct?")	Decreasing the high confidence level will allow more calls to be processed without explicit confirmation.
Many calls result in transfers to incorrect matches.	Increasing the high confidence level will ensure that more calls receive explicit confirmation before being transferred.
Many calls that are for valid names result in no match. (Attendant says, "I don't understand.")	Decreasing the low confidence level will allow more calls to be recognized, and receive explicit confirmation before being transferred.
Many calls result in confirmation requests with incorrect name matches. (Attendant says, "I heard <name>. Is that correct?")	Increasing the low confidence level will filter out more calls, requesting the caller to try again.

For confidence threshold configuration, refer to Basic Speech Recognition Parameters.

There are other adjustable parameters that affect speech recognition; we recommend that you leave these settings at their default values unless changes are requested by Mitel Product Support.

26.115.3 Dialing Policy Parameters

Dialing policy parameters allow you to determine which types of users are allowed to perform what types of calls.

To configure the dialing policy parameters:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Misc. Parameters**. The Auto Attendant Parameters window appears.
3. In the **Category** field, select **Dialing Policy** from the drop-down menu.
4. For each caller type field, you can choose one of the following four dialing permission options from the drop-down menu: “Extensions only”, “Extensions and local numbers”, “Extensions, local and long distance” and “Extensions, local, long distance and international calls”

   OR

   You can apply the default value for each of the parameters by clicking**Use Default Value**.

5. Configure the following parameters:

   - **Unknown (non-trusted) callers, external:** This field sets the dialing permissions for callers who place calls from outside the company's telephony network and the caller ID cannot be recognized as an Auto-Attendant user. The default value is "Extensions only."
   - **Unknown (non-trusted) callers, internal:** This field sets the dialing permissions for callers who place calls from inside the company's telephony network and the caller ID cannot be recognized as an Auto-Attendant user. The default value is "Extensions and local numbers."
   - **Known (trusted) callers, external:** This field sets the dialing permissions for callers who place calls from outside the company's telephony network and the caller ID is recognized as an Auto-Attendant user. The default value is "Extensions and local numbers."
   - **Known (trusted) callers, internal:** This field sets the dialing permissions for callers who place calls from inside the company's telephony network and the caller ID is recognized as an Auto-Attendant user. The default value is "Extensions and local numbers."
   - **Minimum Internal Number Length:** This field sets the minimum value for the length of the internal number that can be dialed by the user. The shortest value is 1 digit and the longest value is 11 digits. The default value for the minimum internal number length is 3 digits.
6. **Maximum Internal Number Length:** This field sets the maximum value for the length of the internal number that can be dialed by the user. The shortest value is 1 digit and the longest value is 11 digits. The default value for the maximum internal number length is 6 digits.

> **Note**:
> The maximum internal number length must be greater than or equal to the minimum internal number length.

7. Click **Save** to set the configured parameters to the selected values.

26.115.4 User Data Source Schedule Parameters

The user data source parameters allow you to schedule a specific time for the corporate list update. When these parameters are configured, the list of SAA users is automatically updated daily at the specified time.

To configure the user data source parameters:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Misc. Parameters**. The Auto Attendant Parameters window appears.
3. In the **Category** field, select **User Data Source** from the drop-down menu.
4. Configure the specific time for the corporate list update or click Use Default Value to apply the default. The value must be in the range of "0:00 AM" to "11:59 PM". The default value is "1:00 AM".
5. Click **Save**. The corporate user list will be updated daily at the configured time.

26.115.5 Presence Feature Parameters

Presence Feature parameters allow you to globally enable or disable the Presence feature for internal and external callers.

To configure the Presence feature parameters:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Misc. Parameters**. The Auto Attendant Parameters window appears.
3. In the **Category** field, select **Presence Feature** from the drop-down menu.
4. Configure the following parameters (or click Use Default Value to apply the default :
5. **Presence for Internal Callers:** This check box allows you to globally enable or disable the Presence feature for internal callers. The default value is “enabled”.

   - **Presence for External Callers:** This check box allows you to globally enable or disable the Presence feature for external callers. The default value is “enabled”.
   - Presence Integration: Select the type of server being used to provide Presence information.

     For Lotus Sametime servers, in theDefault Server Domain Namefield, enter the FQDN of the Sametime server (must contain the '.' character to be valid). Leave theSametime Server Name Attributefield blank (default value).
6. Click **Save**. The Presence feature will now be set to the configured parameters for both internal and external callers.

26.115.6 Administration Parameters

The administration parameters allow you to specify the PIN number for the administrator in order to perform configuration and administration tasks.

To configure the administration parameters:

1. In the navigation tree, click **Auto-Attendant**. The Auto-Attendant menu items appear.
2. Click **Misc. Parameters**. The Auto Attendant Parameters window appears.
3. In the Category field, select **Administration** from the drop-down menu.
4. In the **Administrator PIN** field, enter the digits that you would like to use for the administrator PIN. The PIN can contain from 4 to 10 digits only; any other characters are invalid, including star (*) and pound (#). The default value for the administrator PIN is “123456”.
5. Click **Save**. The administrator PIN is now saved and must be used to perform configuration and administration tasks.

26.116 Custom Pronunciations

Overview

The Custom Pronunciations tool allows administrators to add nicknames and to customize name pronunciation. For example, if a user named Michael also wants to be recognized as "Mick" or "Mickey" you can add these nicknames to the word "Michael". When a caller says either "Mick" or "Mickey", users named Michael are recognized. You can add multiple pronunciations for each SAA-registered user.

You can also add a phonetic representation of the user's name. For example, an English SAA system will have a better chance of matching the name "Benoit" when you add a phonetic pronunciation (like "benwah").

For systems that use a bilingual language configuration, you can also configure a pronunciation in the secondary language (for example, if French is configured as your secondary language, you can configure a secondary language entry of "maison" to be a pronunciation of the English "house". **Note**: If multiple SAA-registered users have a name that includes the word "house", they will also be recognized by the programmed pronunciation.

Conditions and Limitations

- There is no relationship between Custom Pronunciations and SAA names recorded by licensed users when they complete the SAA tutorial. As such, re-recording the SAA names has no impact on the recognition success rate for the Custom Pronunciations.
- Custom Pronunciations take effect immediately (without the need to click the Force Update button). For this reason, exercise care when adding or editing entries.

- It is recommended that a maximum of three Custom Pronunciation entries be added for any one user name.
- The Custom Pronunciation tool is available only to the SAA administrator, *not* to licensed users.
- The Custom Pronunciation tool does *not* replace the default system pronunciation engine.
- When implementing this feature, the SAA administrator should:
- • experiment with a single entry (e.g. a user's last name) to confirm that it can be recognized. If unsuccessful, re-do the entry. If successful, add more entries.
  - use default settings for the miscellaneous SAA parameters. Alternatively, contact Mitel product support before modifying the miscellaneous parameters.

Programming

Note:
If you change the SAA language at any time, your Custom Pronunciations may be inappropriate, and may even have a detrimental impact on recognition performance. We recommend that you delete your existing pronunciations when changing SAA language. (You may also want to keep a record of them for future use.)

To add a Custom Pronunciation:

1. In the navigation tree, click **Auto Attendant**. The Auto Attendant menu appears.
2. Click **Custom Pronunciation**.
3. In the **Word** field, type the name for which you want to add a pronunciation (for example, "mouse").
4. In the **Pronunciations** field, type one or more pronunciations that you want to be recognized as synonyms for "mouse", entering each pronunciation on a new line.
5. Click **Add**.

To edit a Custom Pronunciation:

1. In the navigation tree, click **System Maintenance** and then click **Auto Attendant**. The Auto Attendant menu appears.
2. Click **Custom Pronunciation**.
3. Click the link of the word you want to edit.

   Note: If the word list is long, you can use the alphabet toolbar to click the first letter of the word and display only those words that begin with the same letter.
4. Make the required changes and then click **Save**.

To delete a Custom Pronunciation:

1. In the navigation tree, click **System Maintenance** and then click **Auto Attendant**. The Auto Attendant menu appears.
2. Click **Custom Pronunciation**.
3. Select the check box beside the word you want to delete and then click **Delete**. Click **OK** to confirm the deletion.

26.117 Troubleshooting SAA Name Recognition Problems

This topic provides instructions for troubleshooting problems encountered with the SAA name recognition engine. If you are unable to resolve a problem after following the guidelines below, contact your distributor or Mitel product support.

Cause of Name Recognition Problem	Corrective Action
Missing or inaccurate name entries.	Ensure that the spoken name is entered in the Speech Auto Attendant database and that callers are saying tha t exact name. For example, if the name is entered in the database as Ted Smith, ensure that callers aren't sayin g Edward Smith.
Background noise, hands-free operation, echo, and sp eakerphone quality.	If the caller is experiencing name recognition problems when calling from a speakerphone, get the caller to try the name from a handset.
Mispronunciation, poor annunciation and accents.	Determine if the caller's pronunciation is causing the r ecognition problem by checking if the system recogni zes the name when other callers try it.
High noise levels, high audio levels, or echo.	Determine if the problem is specific to the phone, that is, if the caller is not recognized when dialing in remotely , get them to try locally.

Cause of Name Recognition Problem	Corrective Action
Cell and internet calls sometimes introduce propagation delays. A bad trunk could exhibit noise, including cross talk, popping , static or audio level problems, which, in turn, could contribute to echo. If the remote caller experiences intermittent cases where low confidence forces the caller to repeat the spoken name, check the audio quality of the trunks or isolate whether only certain types of calls (for example, overseas calls) are affected.	If trunk audio quality is at fault, contact your carrier or service provider. If the source of the problem cannot be determined, advise the caller to use DTMF as an input to Speech Auto Attendant until it can be determined whether other remote callers are also experiencing remote access recognition issues.
The dictionary contains most of the common North American English names. A pronunciation for an unusual name may not be programmed in the dictionary.	If multiple callers are speaking a specific name that is not recognized, use the pronounce tool.
Speech recognition is poor.	For individual names, use the pronounce tool to instruct the Speech Auto Attendant how to pronounce individual words.

26.11.8 Install Active Directory (AD) Snap-in

The optional AD Snap-In allows the NuPoint UM server to import user configuration from an Active Directory server. The AD Snap-In also adds a user property sheet to the AD User Interface for NuPoint attributes. NuPoint user properties can be modified and saved with this interface. When the properties are saved, the Snap-In pushes the changes to the NuPoint database.

The AD Snap-In comprises two components:

1. The snap-in configurator, which appears as an installed executable program on the Windows PC. Administrators use the configurator for the following functions:

- Associate Active Directory with a NuPoint system for the purpose of managing users on the NuPoint system.
- Where licensing allows, specify the data source for the NuPoint Speech Auto Attendant. The possible data sources are the associated NuPoint system, the Active Directory users, or the MiCollab. If the data source is Active Directory, then several additional settings are required.

1. The snap-in itself, which appears as an additional property tab for users in Active Directory.

Administrators can add and delete NuPoint users from the snap-in and change some basic settings (for example, class of service, Unified Messaging settings, Speech Auto Attendant settings). In addition, the snap-in allows the administrator to associate Active Directory user accounts to NuPoint user accounts.

The AD Snap-in functions with Active Directory Services on Windows Server 2008 and 2012 R2. It is supported on 32-bit systems and can be used on 64-bit systems by running Active Directory Users And Computers in 32-bit mode (that is, starting the program with the /32 option). This is done with the following command or shortcut:

%SystemRoot%\system32\dsa.msc /32

Note:

- The AD Snap-In does not extend the schema on the server but the user does need schema rights.
- The AD Snap-In is not supported for Lotus or Google implementations.

The AD Snap-In is provided in the form of a Windows installer that you can run on any PC that has access to AD Users and Computers with schema rights. The executable will install the Snap-In and provide an icon on the desktop that will allow you to configure the Snap-In at a later time or re-configure it if there are changes to be made.

To install the AD Snap-In:

1. Insert the NuPoint UM DVD1 and navigate to the **ADSnapInSetUp.exe** file. Double-click to open.
2. At the Welcome screen, click **Next**.
3. Select a destination for the installation or click **Next** to accept the default. The software installs.
4. At the **Would you like to configure and register?** prompt, click **Yes**. The End User License Agreement appears.
5. Read the end user license and then, if you agree, select **I accept the terms in the license agreement**. The configuration screen appears.
6. Enter the following information:

   NuPoint Section:

   - **NPM Server FQDN or IP Address**: Enter the fully qualified domain name of the NuPoint Unified Messaging server. This information is necessary for the AD Snap-In to connect to the NuPoint Unified Messaging server. When using a NuPoint UM 640 platform, specify the Cluster Name in this field.
   - **NPM Admin Login Name**: Enter the account that the AD Snap-In will use to connect to the NuPoint Unified Messaging server. Use the "root" account.
   - **NPM Admin Password**: Enter the password for the root account.
   - Active Directory Section
   - **AD FQDN or IP Address**: Enter the fully qualified domain name of the Active Directory server. This information is necessary for the AD Snap-In to connect to the NuPoint Unified Messaging server.
   - **AD Admin Login**: Enter the account used to connect to the AD/LDAP repository. The account needs root privileges.
   - **Admin Container**: Enter a fully qualified container name where the "AD Admin Name" account is located in the AD hierarchy.
   - **AD Password**: Enter the password for the AD/LDAP account.
   - **AD Attribute**: Skip this setting.
7. Click **Next**.
8. If Speech Auto Attendant licenses are present, a Speech Data Source configuration screen appears. The attributes that you configured for Privacy, Auto-Attendant User, and Default Telephone Number are displayed. Click **Next**. AD Configuration is complete.

The AD Snap-In adds a customized NuPoint tab under the properties of a user. This tab allows you to add a new NuPoint mailbox to the repository, or to edit an existing NuPoint mailbox. You can also launch the

Web Console (by clicking the "View Web Profile" button) to modify additional fields that are not present in the NuPoint tab. The Snap-In establishes a connection to the NuPoint Unified Messaging server using a secure SOAP connection.

Note:
NuPoint properties on this screen are disabled when SAA is installed as a standalone application.

You need to enable the **NuPoint User** check box on a property page in order to make the fields and the drop-down menus active. The drop-down menus will be populated with the actual FCOS and LCOS information from the NuPoint Unified Messaging server. Configuring the parameters on the NuPoint tab links the AD user with the NP-UM mailbox.

After the AD user and the mailbox have been linked, the **Advanced UM Email Alias** for the linked mailbox is also updated with the mailbox nickname. System users see the populated Advanced UM Email User Name field in the Web Console, in Web View and in the Text Console.

Note:
Only those FCOS that contain LCOS values that have names will be populated. All other FCOS, and any unnamed LCOS, cannot be populated to the AD Snap-In. If you encounter an unnamed COS, use the Text console to name it.

26.119 Presence Overview

The Speech Auto Attendant feature provides the ability to optionally play back the current presence state of the matched person prior to transferring the caller. A caller hears the user's current presence state, spoken by the Speech Auto Attendant, before being transferred to the user's phone. For example, SAA might say, "Alice Brown is currently Away." before transferring the call to Alice Brown's phone.

Note: The Presence feature is only supported with installations that use Active Directory as their user repository. See User Data Sources for more information.

Presence status information is for reference only, so a call will be transferred regardless of presence status. Standard universal barge-in commands such as "cancel" and "help" during a call transfer are supported.

The presence status information is optional. It is enabled by default for both internal and external callers, and is independent of whether the caller is trusted or non-trusted. It can be turned off using the **Presence for Internal Callers** and **Presence for External Callers** check boxes in the Miscellaneous Parameters menu of the Web Console.

Server Support

The presence feature in Release 4.0 and later supports the Microsoft Live Communication server (LCS 2005 SP2), Office Communications server 2007, Lotus Sametime 8.0, and Mitel MiCollab Client Service .

Licensing

This feature is licensed as a single license, “NuPoint Messenger: Enable Presence (Speech AA)”, which enables Presence on the system. The license can be activated at any time and becomes available within one minute of activation. No reboot or restart is necessary.

Installation

Presence information is supplied to the Speech Auto Attendant by the Presence Proxy service. The Presence Proxy is part of the NuPoint Unified Messaging system, and is installed using the “NPMPresence” blade. See Presence Installation for more information.

26.119.1 Presence Installation

The Presence Proxy is packaged as an MSL Blade called **NPMPresence**. It provides basic presence information to the Speech Auto Attendant and is installed as part of the NuPoint UM system. The Presence proxy service remains dormant until a Presence license is purchased. Once licensed, the Presence proxy service becomes fully functional within minutes of being activated on the NuPoint UM server.

See Optional Feature Installation for blade installation instructions.

The Presence Proxy itself requires no configuration, however, configuration is required on the presence server, in Active Directory, and possibly to DNS. See the following topics for detailed configuration instructions:

- LCS Configuration
- OCS Configuration
- Sametime Configuration
- Mitel MiCollab Client Service Configuration

26.119.2 LCS Configuration

The configuration steps required to set up the Presence Proxy for the Speech Auto Attendant (SAA) with LCS 2005 are as follows:

Note:
The Speech Auto Attendant must be installed and configured to use Active Directory as the user data source before the Presence Proxy can be configured. (See step 6 below.)

1. Create the Active Directory/LCS accounts for the NP-UM Presence Proxy
2. Add all NP-UM Presence Proxy accounts to the Allow list of every SAA user
3. Trust the NP-UM Server in LCS 2005
4. Verify that the LCS service entry exists in the Corporate DNS server
5. Configure DNS on the NP-UM server so that it can find the LCS service SRV record
6. Install and configure SAA on the NP-UM server
7. Purchase the SAA Presence license for the NP-UM server

8. Verify the installation

1 - Create the Active Directory/LCS accounts for the NP-UM Presence Proxy

For every 145 Speech Auto Attendant users that have their presence state monitored, it is necessary to create one account for use by the Presence Proxy. For example, to monitor 2000 SAA users, you need to create 14 Presence Proxy user accounts in the LCS Server. For the maximum supported 5000 presence users, it is necessary to create 35 Presence Proxy user accounts in LCS.

Create the Active Directory user accounts using the following names and SIP URIs in the same domain as the other LCS users (in particular, the domain used by the SAA users in NP-UM):

First Name	Last Name	Account	SIP URI
Mitel	Presence	mitelpresence@xyz.com	sip:mitelpresence@xyz.com
Mitel	Presence	mitelpresence2@xyz.com	sip:mitelpresence2@xyz.com
Mitel	Presence	mitelpresence3@xyz.com	sip:mitelpresence3@xyz.com
Mitel	Presence	mitelpresence4@xyz.com	sip:mitelpresence4@xyz.com
Mitel	Presence	mitelpresence5@xyz.com	sip:mitelpresence5@xyz.com
Mitel	Presence	mitelpresence6@xyz.com	sip:mitelpresence6@xyz.com
Mitel	Presence	mitelpresence7@xyz.com	sip:mitelpresence7@xyz.com
Mitel	Presence	mitelpresence8@xyz.com	sip:mitelpresence8@xyz.com
Mitel	Presence	mitelpresence9@xyz.com	sip:mitelpresence9@xyz.com
Mitel	Presence	mitelpresence10@xyz.com	sip:mitelpresence10@xyz.com
etc.	etc.	etc.	etc.

To create a user in the "Active Directory Users and Computers" management console on the Domain Controller:

1. Expand the domain holding the LCS users.
2. Right-click on **Users**, and then select **New->Users**.
3. Enter 'Mitel' for the **First name**, 'Presence' for the **Last name**, and 'mitelpresence99' for the **User logon name**, where 99 is blank for the first user, ’2’ is entered for the second user, ’3’ is entered for the third user, and so on for the remaining users (see table above).
4. Click **Next**.
5. Enter a password. For increased security, make the password as long as possible (at least 7 characters) and use a mix of numbers and letters in upper and lowercase.
6. Select the **Password never expires** check box. Leave all other check boxes empty.
7. Click **Next**.

8. Review the values entered for accuracy, and then click **Finish**.

The ’mitelpresence’ user will appear in the list of users in the right pane. Add as many ’mitelpresence’ users as is necessary based on the number of SAA users to have presence.

Next, enable the mitelpresence users for LCS by doing the following steps for every ’mitelpresence’ user in the right pane:

1. Right-click on the ’mitelpresence’ user, and select **Properties**.
2. In the **Properties** window, select the **Live Communications** tab.
3. Select the **Enable Live Communications for this user** checkbox.
4. In the **SIP URI** box, enter 'sip:mitelpresence99@xyz.com' where xyz.com is replaced with the proper domain and 99 is replaced with the number matching this mitelpresence user (refer to the table above).
5. Select the LCS server from the **Server or pool** list.
6. Click **OK**.
7. Repeat the steps above for all other ’mitelpresence’ users.

Note:

- It will take several minutes for these Active Directory changes to propagate and come into effect.
- Scripting (e.g., VB Script) can be used to automate the creation of accounts.

2 - Add all NP-UM Presence Proxy accounts to the Allow list of every SAA user in LCS

To allow the Presence Proxy to monitor the presence state of SAA users without becoming a member of each user's Contact or Buddy list, it is necessary to add all Presence Proxy user accounts to the Allow list of every SAA user.

In the LCS management console:

1. Right-click on an SAA LCS user, and then select **Properties**.
2. In the **Live Communications** tab, click the **View/Edit** button beside the **Allow and block list:** label.
3. In the **User Allow and Block List** window, click **Add**.
4. In the **Type** list, select **User**.
5. In the **Mask** box, enter the SIP URI of a Presence Proxy's account—for example, 'sip:mitelpresence99@xyz.com' where 'xyz.com' is the LCS domain name and 99 is replaced with the number of the ’mitelpresence’ user.
6. Select **Allow subscriptions and invitations**.
7. Click **OK** for each window that appears to save the changes.
8. Repeat the steps above for every ’mitelpresence’ user account.

The Presence Proxy user accounts can also be added to the Allow list of every SAA user through Microsoft Office Communicator when logged in as an SAA user:

1. Select **Actions > Options**.
2. Select the **Permissions** tab.
3. Click **New**.
4. In the **Type** list, select **User**.
5. In the **Account name** box, enter the SIP URI of the Presence Proxy's account—for example, 'sip:mitelpresence99@xyz.com' where 'xyz.com' is the LCS domain name and 99 is replaced with the number of the ’mitelpresence’ user.
6. In the **Permission** list, select **Allow**.
7. Click **OK**.

If the Presence Proxy user is missing from a user's Allow list, attempts by the Presence Proxy to subscribe to that user's presence may fail. The SAA user will be prompted by Office Communicator to add the Presence Proxy to their buddy list. Unless the Presence Proxy is in the user’s buddy list, it will not be able to receive the user's presence status.

Note: The above procedure is practical for a small number of users. For larger numbers, scripting (for example, VB Script) can be used instead. The Microsoft LCS 2005 Resource Kit provides sample scripts that you can use as a starting point. To obtain the scripts, download the kit from the Microsoft website and install it on the LCS 2005 server.

3 - Trust the NP-UM Server in LCS 2005

In the LCS Management Console, add the NP-UM server as an Authorized Host:

Note: For NuPoint UM 640, trust the cluster IP address and all the server IP addresses.

1. Right-click the server under **Live Communications servers and pools**.
2. Select **Properties**.
3. Select the **Host Authorization** tab.
4. Click **Add...**.
5. Enter the **IP address** of the NP-UM server.
6. Select the **Treat as Authenticated** check box.
7. Click **OK**.

4 - Verify that the LCS service entry exists in the Corporate DNS server

Ensure that the corporate DNS server (it may be running on the Windows Domain Controller or other Windows server) has been configured following the recommendations in the LCS Deployment Guide. This means there must be an SRV record for '_sip._tcp.xyz.com' where 'xyz.com' is the domain that LCS is in.

One way to verify the setup is to view the corporate DNS configuration directly. Another way is by using the Microsoft Office Communicator client. If it works using 'Automatic configuration', then DNS is correctly set up, assuming that the DNS servicing the Communicator Client PC is the same DNS in effect for the NP-UM Server that the Presence Proxy is running on.

In a working Office Communicator application:

1. Select **Actions->Options**.
2. Select the **Accounts** tab.
3. Click the **Advanced** button beside the **Sign-in name** box.

If **Automatic configuration** is selected, then the Communicator client is using DNS to locate the OCS server in the same way that the NP-UM Presence Proxy does. This means that DNS is already configured for OCS.

If **Manual configuration** is selected, try changing it to **Automatic configuration** as described below:

1. Select **Automatic configuration**.
2. Click **OK** to save the change.
3. Click **OK** again to exit the **Options** window.
4. Log out of Office Communicator (select **Connect > Sign Out**), and then log in again.
5. Click **Sign In**.
6. If prompted, log in as the same user.

If the login succeeds, DNS is correctly set up.

5 - Configure DNS on the NP-UM server so that it can find the LCS service SRV record

Ensure that the NP-UM server has its DNS set up so that DNS queries are forwarded to the Windows DNS server, often on the Domain Controller.

Many working DNS configurations are possible. The requirement is that the Presence Proxy running on the NP-UM server is able to use DNS to resolve the '_sip._tcp.xyz.com' service name (where xyz.com is the domain that LCS is in).

To test this, from a command line on the NP-UM system, enter the following command and verify that it returns the information for the LCS server:

dig _sip._tcp.xyz.com SRV +short

where "`xyz.com`" is replaced with the domain of LCS. The result should look similar to this:

0 0 5060 mylcs.xyz.com

where `mylcs.xyz.com` is the hostname of the LCS server and `5060` is the port used to connect to LCS. If the result is nothing or a blank line, DNS is incorrectly configured, or DNS on the NP-UM server is not configured correctly to use the corporate DNS server(s).

6 - Install and configure SAA on the NP-UM server

See Speech Auto Attendant Installation and Configuration for installation instructions. The Speech Auto Attendant must be set up to use Active Directory as the user repository. See Define an Active Directory Data Source.

7 - Purchase the Presence license for the NP-UM server

The "NuPoint Messenger: Enable Presence (Speech AA)" license must be purchased. Once that license becomes effective for the NP-UM server, no further actions are required. The Presence Proxy is always running when NP-UM is running and it will detect that the license has been purchased and will automatically start up within a minute of enabling the license.

8 - Verify installation

To verify the installation, check that the Speech Auto Attendant can retrieve the presence state of a user. Call the SAA main number and speak the name of an SAA user who is also an LCS-enabled user. SAA should speak the current presence state of the user before forwarding the call. Change the presence state of the SAA user (e.g., from Online to Busy or Be Right Back) and make another call through SAA to that user. The presence state spoken by SAA should be the new state.

26.119.3 OCS Configuration

The configuration steps required to set up the Presence Proxy for the Speech Auto Attendant (SAA) with OCS 2007 are as follows:

Note:
The Speech Auto Attendant must be installed and configured to use Active Directory as the user data source before the Presence Proxy can be configured. (See step 7 below.)

1. Create the Active Directory/OCS accounts for the NP-UM Presence Proxy
2. Add all NP-UM Presence Proxy accounts to the Allow list of every SAA user
3. Add all NP-UM Presence Proxy accounts as a PromptedSubscriber for every SAA user in the OCS database
4. Trust the NP-UM Server in OCS 2007
5. Verify that the OCS service entry exists in the Corporate DNS server
6. Configure DNS on the NP-UM server so that it can find the OCS service SRV record
7. Install and configure SAA on the NP-UM server
8. Purchase the SAA Presence license for the NP-UM server
9. Verify the installation

1 - Create the Active Directory/OCS accounts for the NP-UM Presence Proxy

For every 145 Speech Auto Attendant users that have their presence state monitored, it is necessary to create one account for use by the Presence Proxy. For example, to monitor 2000 SAA users, you need to create 14 Presence Proxy user accounts in the OCS Server. For the maximum supported 5000 presence users, it is necessary to create 35 Presence Proxy user accounts in OCS.

Create the Active Directory user accounts using the following names and SIP URIs in the same domain as the other OCS users (in particular, the domain used by the SAA users in NP-UM):

First Name	Last Name	Account	SIP URI
Mitel	Presence	mitelpresence@xyz.com	sip:mitelpresence@xyz.com
Mitel	Presence	mitelpresence2@xyz.com	sip:mitelpresence2@xyz.com
Mitel	Presence	mitelpresence3@xyz.com	sip:mitelpresence3@xyz.com
Mitel	Presence	mitelpresence4@xyz.com	sip:mitelpresence4@xyz.com
Mitel	Presence	mitelpresence5@xyz.com	sip:mitelpresence5@xyz.com
Mitel	Presence	mitelpresence6@xyz.com	sip:mitelpresence6@xyz.com
Mitel	Presence	mitelpresence7@xyz.com	sip:mitelpresence7@xyz.com
Mitel	Presence	mitelpresence8@xyz.com	sip:mitelpresence8@xyz.com
Mitel	Presence	mitelpresence9@xyz.com	sip:mitelpresence9@xyz.com
Mitel	Presence	mitelpresence10@xyz.com	sip:mitelpresence10@xyz.com
etc.	etc.	etc.	etc.

To create a user in the "Active Directory Users and Computers" management console on the Domain Controller:

1. Expand the domain holding the OCS users.
2. Right-click on **Users**, and then select **New->Users**.
3. Enter 'Mitel' for the **First name**, 'Presence' for the **Last name**, and 'mitelpresence99' for the **User logon name**, where 99 is blank for the first user, ’2’ is entered for the second user, ’3’ is entered for the third user, and so on for the remaining users (see table above).
4. Click **Next**.
5. Enter a password. For increased security, make the password as long as possible (at least 7 characters) and use a mix of numbers and letters in upper and lowercase.
6. Select the **Password never expires** check box. Leave all other check boxes empty.
7. Click **Next**.
8. Review the values entered for accuracy, and then click **Finish**.
9. The ’mitelpresence’ user will appear in the list of users in the right pane. Add as many ’mitelpresence’ users as is necessary based on the number of SAA users to have presence.

Next, enable the mitelpresence users for OCS by doing the following for every ’mitelpresence’ user in the right pane:

1. Right-click on the ’mitelpresence’ user, and the select **Properties**.
2. In the Properties window, select the **Communications** tab.
3. Select the **Enable user for Office Communications Server** checkbox.

4. In the **Sign in Name** field, enter 'sip:mitelpresence99' and select @xyz.com from the drop-down list, where xyz.com is replaced with the proper domain and 99 is replaced with the number matching this mitelpresence user (refer to the table above).
5. Select the OCS server from the **Server or pool** list.
6. Click **OK**.
7. Repeat the steps above for all other 'mitelpresence' users.

Note:

- It will take several minutes for these Active Directory changes to propagate and come into effect.
- Scripting (e.g., VB Script) can be used to automate the creation of accounts.

2 - Add all NP-UM Presence Proxy accounts to the Allow list of every SAA user in OCS

To add the mitelpresence as "Allowed" to each SAA user in OCS 2007, it is necessary to use a script. The user interface for modifying a user's Allow list that existed in LCS 2005 has been removed from OCS 2007 for both the OCS 2007 server and the Office Communicator client.

Sample scripts are included in the Microsoft Office Communications Server 2007 Resource Kit Tools. The Resource Kits are free and available for download from the Microsoft website. The resource kit is installed on the OCS 2007 server, default location C:\Program Files\Microsoft Office Communications Server 2007\ResKit\WMI Samples. The sample script of interest is LCSAddACEs.wsf. Instructions for using the script can be found in the included document OCS_ResourceKitTools_ReadMe.doc in the ResKit directory.

If the Presence Proxy user is missing from a user's Allow list, attempts by the Presence Proxy to subscribe to that user's presence may fail. The SAA user will be prompted by Office Communicator to add the Presence Proxy to their buddy list. Unless the Presence Proxy is in the user's allow list, it will not be able to receive the user's presence status. If the Presence Proxy is added to their allow list properly, there will be no popup for the user and the Presence Proxy will never appear in their Buddy list in Communicator.

3 - Add all NP-UM Presence Proxy accounts as a PromptedSubscriber for every SAA user in the OCS database

This step is required to prevent every SAA OCS user from seeing popup windows in Office Communicator 2007 notifying them that a mitelpresence user has added them as a contact. The only way to prevent the popups is to modify the OCS database directly. The OCS server does not need to be stopped while performing this modification.

Follow the steps below to modify the OCS database:

1. Log into the OCS Server using an account with Administrative privileges.
2. Create a file named PresProxySub.sql containing the following text:

```
USE [rtc]

GO

delete dbo.PromptedSubscriber

from dbo.PromptedSubscriber ps

inner join dbo.Resource r

on ps.SubscriberId = r.ResourceId

where r.UserAtHost like 'mitelpresence%'

GO

insert into dbo.PromptedSubscriber

select distinct c.PublisherId,

r.ResourceId,

'True',

1,

'True',

0,

NULL,

NULL

from dbo.Container c,dbo.Resource r

where r.UserAtHost Like 'mitelpresence%'

order by c.PublisherId, r.ResourceId

GO
```

1. Then run the following command at the command prompt (cmd.exe):

```
sqlcmd -S (local)\rtc -d rtc -E -i PresProxySub.sql
```

This command can be run more than once as it first cleans up the PresenceProxy-related records already in the database (it will not create duplicate records).

In fact, this command should be re-run each time new OCS users (who are also SAA users) are added to prevent those new users from seeing the client contact list notification popup window.

4 - Trust the NP-UM Server in OCS 2007

In the OCS Management Console, add the NP-UM server as an Authorized Host:

Note: For NuPoint UM 640, trust the cluster IP address and all the server IP addresses.

1. Right-click on the server under **Standard Edition Servers**.
2. Select **Properties -> Front End Properties**
3. Select the **Host Authorization** tab.
4. Click **Add...**.
5. Enter the NP-UM server's IP address or FQDN (select the appropriate radio button)
6. Select the **Treat as Authenticated** check box.
7. Click **OK**.
8. Click the next **OK** button.

5 - Verify that the OCS service entry exists in the Corporate DNS server

Ensure that the corporate DNS server (it may be running on the Windows Domain Controller or other Windows server) has been configured following the recommendations in the OCS Deployment Guide. This means there must be an SRV record for '_sip._tcp.xyz.com' where 'xyz.com' is the domain that OCS is in.

One way to verify the setup is to view the corporate DNS configuration directly. Another way is by using the Microsoft Office Communicator client. If it works using 'Automatic configuration', then DNS is correctly set up, assuming that the DNS servicing the Communicator Client PC is the same DNS in effect for the NP-UM Server that the Presence Proxy is running on.

In a working Office Communicator application:

1. Select **Actions->Options**.
2. Select the **Accounts** tab.
3. Click the **Advanced** button beside the **Sign-in name** box.

If **Automatic configuration** is selected, then the Communicator client is using DNS to locate the OCS server in the same way that the NP-UM Presence Proxy does. This means that DNS is already configured for OCS.

If **Manual configuration** is selected, try changing it to **Automatic configuration** as described below:

1. Select **Automatic configuration**.
2. Click **OK** to save the change.
3. Click **OK** again to exit the **Options** window.
4. Log out of Office Communicator (select **Connect->Sign Out**), and then log in again.
5. Click **Sign In**.
6. If prompted, log in as the same user.

If the login succeeds, DNS is correctly set up.

6 - Configure DNS on the NP-UM server so that it can find the OCS service SRV record

Ensure that the NP-UM server has its DNS set up so that DNS queries are forwarded to the Windows DNS server, often on the Domain Controller.

Many working DNS configurations are possible. The requirement is that the Presence Proxy running on the NP-UM server is able to use DNS to resolve the '_sip._tcp.xyz.com' service name (where xyz.com is the domain that OCS is in).

To test this, from a command line on the NP-UM system, enter the following command and verify that it returns the information for the OCS server:

dig _sip._tcp.xyz.com SRV +short

where "xyz.com" is replaced with the domain of OCS. The result should look similar to this:

0 0 5060 mylcs.xyz.com

where mylcs.xyz.com is the hostname of the OCS server and 5060 is the port used to connect to OCS. If the result is nothing or a blank line, DNS is incorrectly configured, or DNS on the NP-UM server is not configured correctly to use the corporate DNS server(s).

7 - Install and configure SAA on the NP-UM server

See Speech Auto Attendant Installation and Configuration for installation instructions. The Speech Auto Attendant must be set up to use Active Directory as the user repository. See Define an Active Directory Data Source.

8 - Purchase the Presence license for the NP-UM server

The "NuPoint Messenger: Enable Presence (Speech AA)" license must be purchased. Once that license becomes effective for the NP-UM server, no further actions are required. The Presence Proxy is always running when NP-UM is running and it will detect that the license has been purchased and will automatically start up within a minute of enabling the license.

9 - Verify installation

To verify the installation, check that the Speech Auto Attendant can retrieve the presence state of a user. Call the SAA main number and speak the name of an SAA user who is also an OCS-enabled user. SAA should speak the current presence state of the user before forwarding the call. Change the presence state of the SAA user (e.g., from Online to Busy or Be Right Back) and make another call through SAA to that user. The presence state spoken by SAA should be the new state.

26.119.4 Lotus Sametime Configuration

Conditions

The Speech Auto Attendant must be installed and configured to use Active Directory as the user data source before the Presence Proxy can be configured. (See step 2 below.)

An IBM Technote specifies that when using AD as the user repository for Sametime, it is necessary to configure Sametime to use the **DistinguishedName** Active Directory attribute of the user by entering it in the "Attribute of a person entry that defines the internal ID of the Sametime user" field of the Sametime configuration. Refer to this web page above for more information: http://www-1.ibm.com/support/docview.wss?rs=203&uid=swg21161658

Procedure

The configuration steps required to set up the Presence Proxy for the Speech Auto Attendant (SAA) with Lotus Sametime are as follows:

1. Trust the Presence Proxy server in Sametime
2. Install and configure SAA on the NP-UM server
3. Purchase the SAA Presence license for the NP-UM server
4. Verify the installation

1 - Trust the Presence Proxy server in Sametime

By default Sametime restricts what IP addresses are allowed to connect to it as a server. To allow the Presence Proxy to connect it is necessary to perform the following actions:

1. Determine the IP address of the system the Presence Proxy is running on. It must be the IP address, not the server hostname.
2. On the Lotus Sametime server, use a Lotus Notes client to open the `Stconfig.nsf` database. This can be accomplished from a system with Lotus Notes installed by navigating to the Lotus Domino data directory on the Lotus Sametime server (for example, C:\Program Files\Lotus\Domino\data) using File Explorer and open the file stconfig.nsf.
3. Edit the **CommunityConnectivity** document.
4. In the **CommunityTrustedIPS** field, enter the IP address of the NP-UM (Presence Proxy) server. If there are multiple IP addresses they must be separated by either a comma or a semicolon.
5. Save the document and restart the Lotus Sametime server.

2 - Install and configure SAA on the NP-UM server

See Speech Auto Attendant Installation and Configuration for installation instructions. The Speech Auto Attendant must be set up to use Active Directory as the user repository. See Define an Active Directory Data Source.

3 - Purchase the Presence license for the NP-UM server

The "NuPoint Messenger: Enable Presence (Speech AA)" license must be purchased. Once that license becomes effective for the NP-UM server, no further actions are required. The Presence Proxy is always running when NP-UM is running and it will detect that the license has been purchased and will automatically start up within a minute of enabling the license.

4 - Verify installation

To verify the installation, check that the Speech Auto Attendant can retrieve the presence state of a user. Call the SAA main number and speak the name of an SAA user who is also a Sametime-enabled user. SAA should speak the current presence state of the user before forwarding the call. Change the presence

state of the SAA user (e.g., from Online to Busy or Be Right Back) and make another call through the SAA to that user. The presence state spoken by the SAA should be the new state.

26.119.5 Unified Communications Server Configuration

The configuration steps required to set up the Presence Proxy for the Speech Auto Attendant (SAA) with the Mitel MiCollab Client Service are as follows:

1. Trust the NP-UM Server in the Mitel MiCollab Client Service
2. Verify that the Mitel MiCollab Client Service service entry exists in the Corporate DNS server
3. Configure DNS on the NP-UM server so that it can find the Mitel MiCollab Client Service service SRV record
4. Install and configure SAA on the NP-UM server
5. Purchase the SAA Presence license for the NP-UM server
6. Verify the installation

Trust the NP-UM Server in the Mitel MiCollab Client Service

Note:
For NuPoint UM 640, trust the cluster IP address and all the server IP addresses.

1. In the MSL admin web interface, under **Applications**, select **Unified Communications Server**.
2. Click the **Configure Mitel UC Server** button.
3. Select the **Enterprise** tab, if it is not the active tab.
4. Click **Trusted Presence Proxies** to expand the section.
5. Click **Add Proxy**.
6. In the new line just added, double click **Add description** to add a meaningful description, for example the hostname of the NP-UM server.
7. In the new line, double click **Add IP address** to enter the IP address to be trusted.
8. Click **Apply** at the bottom of the web page.

Verify that the Mitel MiCollab Client Service service entry exists in the Corporate DNS server

Ensure that the corporate DNS server (it may be running on the Windows Domain Controller or other Windows server) has been configured with an SRV record for '**_sip._udp.xyz.com**' where 'xyz.com' is the domain that the Mitel MiCollab Client Service is in. The SRV record should point to the Mitel UC Server hostname and port (typically 18100).

Configure DNS on the NP-UM server so that it can find the Mitel MiCollab Client Service service SRV record

Ensure that the NP-UM server has its DNS set up so that DNS queries are forwarded to the Windows DNS server, often on the Domain Controller.

Many working DNS configurations are possible. The requirement is that the Presence Proxy running on the NP-UM server is able to use DNS to resolve the '_sip._udp.xyz.com' service name (where xyz.com is the domain that Mitel MiCollab Client Service is in).

To test this, from a command line on the NP-UM system, enter the following command and verify that it returns the information for the Mitel MiCollab Client Service :

dig _sip._udp.xyz.com SRV +short

where "xyz.com" is replaced with the domain of OCS.

The result should look similar to this:

0 0 18100 myucserver.xyz.com

where "myucserver.xyz.com" is the hostname of the Mitel UC Server and 18100 is the port used to connect to the Mitel MiCollab Client Service. If the result is nothing or a blank line, DNS is incorrectly configured, or DNS on the NP-UM server is not configured correctly to use the corporate DNS server(s).

Install and configure SAA on the NP-UM server

See Speech Auto Attendant Installation and Configuration for installation instructions.

Purchase the Presence license for the NP-UM server

The "NuPoint Messenger: Enable Presence (Speech AA)" license must be purchased. Once that license becomes effective for the NP-UM server, no further actions are required. The Presence Proxy is always running when NP-UM is running and it will detect that the license has been purchased and will automatically start up within a minute of enabling the license.

Verify installation

To verify the installation, check that the Speech Auto Attendant can retrieve the presence state of a user. Call the SAA main number and speak the name of an SAA user who is also a user of the Mitel MiCollab Client Service. SAA should speak the current presence state of the user before forwarding the call. Change the presence state of the SAA user (for example, from Available to Unavailable or Gone Home) and make another call through SAA to that user. The presence state spoken by SAA should be the new state.

26.120 SAA Backup and Restore

Speech Auto Attendant user data source configuration, departments, dialing policies, miscellaneous parameters, and line group configuration are backed up automatically by the current NuPoint UM backup procedures.

On Standalone SAA systems, you can perform backups using the instructions in the Backup section of the *NuPoint Unified Messaging Technician's Handbook*.

Note:

- When SAA is configured to use Active Directory or MiCollab as its user data source, the backup function will not back up (or restore) information stored in Active Directory. **Failure to back up Active Directory properly could result in data being lost**.
- Options to back up/restore messages and fax cover pages are not available on standalone SAA systems.
- If you choose to back up or restore "Names and Greetings" in any of the backup menus, then every prompt recorded for SAA (recorded names, departments, as well as customized auto-attendant system prompts) will be backed up (or restored).

26.12 Troubleshooting

Common Problems

SAA is not stating any SAA user's presence

This is the end result of most configuration errors. To isolate the cause, check the Presence Proxy logs on the NuPoint server.

If there is no log indicating the cause of the problem, the entire configuration will need to be checked. Below is the suggested order. For details on how to perform these checks, refer to the Presence configuration instructions.

1. Confirm that the NPM Presence license is purchased on the NuPoint server.
2. On the NuPoint UM server, check the DNS configuration using the `dig` command detailed in the Setup instructions. If the `dig` command does not provide the correct response, the DNS setup for the NuPoint system and the corporate DNS server must be corrected.
3. On the LCS or OCS Server, verify that the correct IP address of the NuPoint server has been added as an authorized host.
4. In Active Directory for the domain that the LCS/OCS/SAA users belong to, verify that the "mitelpresence" users have been created.
5. In Active Directory, verify that the "mitelpresence" users have been enabled as LCS/OCS users.
6. In Active Directory, verify that the "mitelpresence" users have the **Password never expires** checkbox selected.
7. In LCS/OCS, check the **Allow and block list** of the SAA users to ensure that all the "mitelpresence" users have been added as Allowed.

SAA is not stating the presence state of some users

If the presence status is supplied in SAA for some users and not for others, it is likely that the **Allow and block list** of the users was incorrectly modified.

Check the users and make sure that all the ”mitelpresence” users have been added as "Allowed".

Also check that all the ”mitelpresence” users have **Password never expires** selected in Active Directory. If not selected, the password may have expired and the account could be suspended, which means the Presence Proxy will fail to get presence updates for some users.

An SAA user’s presence state is incorrect

The SAA user in question may be logged in to more than one session. In LCS /OCS, a user can be logged into more than one session at the same time, for instance using Office Communicator on more than one PC. The server aggregates the presence state from all active sessions, and it is this aggregate presence state that is used by the Presence Proxy. If the user is online in one session and offline in the other, the Presence Proxy will reflect the online state.

Try logging in as a different user who has the problem user as a buddy, and see if the state shown there matches the one that is provided by SAA Presence.

An SAA user is being notified in Office Communicator 2007 that a mitelpresence user has added them as a contact

This means that the user's allow list was not properly modified by the script that was run in step 2 of OCS Configuration. Try running the script again.

26.12 Speech to Text - Description

Speech to Text is an optional, licensed feature of NuPoint UM that converts voice mail messages to text, allowing users to discreetly access voice messages in a text format. This feature uses a third-party transcription service that requires Internet connectivity. Your DNS configuration must allow for transcription requests being sent to the Speech to Text provider, Nuance Communications.

Speech to Text service allows you to:

- **Discretely check voice messages**

  When in meetings or in social settings, it is simply awkward to listen to voice messages. This situation is especially frustrating if an important message is expected. The STT feature allows you to "read" new voice messages virtually anywhere.
- **Quickly find important voice messages**

  In most cases, you can scan a transcribed message faster than you can listen to the original voice message. After performing this quick review, you can listen to the voice message to catch nuances of expressions and confirm key details.

- **Easily respond to voice message with an email**

  After reading a transcribed message, you can “reply” to it by forwarding it to email. This eliminates the need to "re-cap" the voice message by typing it into the email message.

Note:

- Administrators and users must agree to the terms of the transcription service provider's licensing agreement. Part of this agreement specifies that the transcription process may involve human beings listening to your recorded audio messages.
- The Speech to Text feature must be configured using the **Web Console**. (Exception: The Text Console can be used to configure STT for UM Standard.)

Conditions and Limitations

Speech to Text Provider (Nuance)

1. Although the transcription process is fully automated, voice messages are kept for 24 hours during which random spot checks are performed to assess quality. All data (voice message and transcriptions) are then electronically "shredded" and retained in a library for research purposes. This is analogous to a physical paper shredding process—audio and transcriptions from all sources are "cut up" and mixed up together so that a message cannot be pieced together again.
2. If an account balance lapses, transcription requests are denied and alarms are raised. NuPoint UM disables the Speech to Text feature until the administrator corrects the account balance and activates the feature again.
3. There may be limitations on the type and/or length of messages being transcribed. If transcription cannot be performed, an alternative email is sent to notify the user.
4. There may be a limit on the number of concurrent requests that can be sent at any given time, and on the number of transcriptions performed in a specific time period. Volumes higher than this limit may be queued.
5. Nuance does not provide language detection and/or translation services. For this release, messages received in languages other than North American English will not be transcribed.
6. The maximum message length is 60 seconds. For longer messages, users can dial in and listen to the entire original voice mail. (If necessary, your Mitel reseller can contact the transcription service provider to extend the maximum message length for your account.)
7. The Speech to Text service uses a complex computer model to transcribe spoken words into text. While transcription accuracy can be very good, there may be instances when the transcription does not accurately represent the spoken message. If in doubt, please listen to the original voice message.
8. If the system cannot understand the message, it will not transcribe it. Instead, the user will receive an email notification. Typically, about 15% of messages are deemed "untranscribable" due to non-English accents or language, jargon, background noise or other issues.

NuPoint UM

1. When Speech to Text is enabled, users receive a text transcription email for each of their voice mail messages. You can add a copy of the audio file by enabling "Include audio attachments with email messages" in the system-wide settings.
2. For Advanced UM, only email messages containing audio attachments are synchronized with the user's voice mailbox. Emails containing text transcriptions are not synchronized and do not affect the status of the original voice mail or MWI.
3. A message number (ID) is contained within the body of email messages. When two emails are generated for a single voice mail, they will have the same message number.
4. Speech to Text is supported in International English only, and in North America only.
5. Confidential, Record-a-Call, and Fax messages are not transcribed.
6. Text transcription emails can be handled like other emails (mark as read, forward, reply, etc.) but operations performed on them are not synchronized with the user's NuPoint voice mailbox.
7. Users must accept the Speech to Text license agreement in Web View before the feature can be used. Administrators cannot accept the license on the user's behalf.

About Nuance Transcription

The transcription service provider is Nuance Communications, Incorporated.

You must contact your Authorized Mitel Reseller in order to set up an account and purchase conversion credits from Nuance. When the credits run low or are depleted, NuPoint UM will begin generating alarm messages. You must then purchase more conversion credits from your reseller.

Transcription Performance

Because it takes time for the system to transcribe voice messages to text, email with text transcriptions will arrive after emails with audio attachments. Delays of 10 minutes or more can be encountered depending on the length of the voice messages and the number of transcription requests the system is currently processing. Internal corporate mail routing delays may also affect delivery time. The transcription process rarely takes less than two minutes.

Transcription Message Contents

Standard Messages

A typical transcribed message looks like this:

"Hi there. I was just returning your call about dinner at the weekend. Not very sure. I'll let you know by tomorrow what it’s looking like. Bye."

Spoken through Nuance.

The quotation marks delineate the contents of the original voice mail message.

Messages with Special Characters

Special characters contained in the body of the message indicate the following:

- **Question Mark**: Indicates that the service cannot understand the complete word. It therefore spells the word phonetically. For example, "Hi Ashby(?), are you still working? Bye."
- **Underscore**: Indicates that the service cannot understand any part of the word. It therefore replaces the word with an underscore. for example, "Hi _. My number is 777777777. I repeat 777777777. Thank you."

Unconverted Messages

The transcription service will not convert messages for the following reasons:

- Too much background noise
- Speaker's accent not understood
- Message was recorded in a language other than English
- Message spoken too fast
- Message contains too many special characters indicating that text has been replaced or spelled phonetically
- Message is a fax
- Message is marked "confidential"

If any of these conditions occur, NuPoint UM users will receive an email instructing them to call the voicemail system to check the original message.

26.122.1 Speech to Text - Installation

NuPoint UM

The Speech to Text feature requires a single system-wide license and an AMC synchronization. The feature does not require installation as it is bundled with the NuPoint UM base software and is automatically installed by the Master Installer blade.

Note: If you are installing the STT feature after the initial NuPoint UM installation, you must install the STT blade. See Installing an Optional Feature.

Speech to Text Provider (Nuance)

Administrators are required to contact their Authorized Mitel Reseller in order to set up an account and purchase conversion credits from the transcription service provider, Nuance Communications. When your credits run low, you will be alerted through the NuPoint alarm mechanism. You must then purchase additional credits through your reseller in order to retain the service.

26.122.2 Speech to Text Configuration

Configuration of the Speech to Text feature consists of the following steps, detailed below:

- Obtain a Nuance speech transcription account and conversion credits
- Configure system-wide Speech to Text settings
- Enable the Speech to Text feature
- Configure Speech to Text for users

Obtaining a Nuance Account and Conversion Credits

Nuance Communications is responsible for transcribing voice messages to text. To access this service, you require a user account and conversion credits, which you can obtain through your Authorized Mitel Reseller.

Note:
Purchase the NuPoint UM Speech to Text "enablement" license before you set up your Nuance account and obtain conversion credits.

1. Contact your Authorized Mitel Reseller and provide the following:

   - **User Name**: Name of your NuPoint UM system.
   - **System ID**: Application Record ID, or ARID, of the NuPoint UM system.
   - **Conversion credit quantity**: Mitel sells conversion credits in prepackaged quantities.
   - **Confirmation email addressess**: Nuance sends a confirmation email to these addresses when conversion credits are purchased.
2. The information is sent to Nuance, which sets up your user account, assigns conversion credits, and sends you an email containing the following:

   - **User Name**: Same as above.
   - **Password**: Your unique account password, provided by Nuance.
   - **Account ID**: Your unique account ID number, provided by Nuance.
   - **Application ID**: Your unique application ID name, provided by Nuance.
3. Complete the next procedure, Configuring System-wide Speech to Text Settings.

These same credentials are used for account renewals. NuPoint UM does not know or report the state of your Nuance subscription. If your account is running low, Nuance notifies the NuPoint UM server, which in turn issues warning alarm messages. If your account is empty, the Speech to Text transcription service is terminated. You will need to purchase additional credits through your Authorized Mitel Reseller and then Activate Text to Speech.

Configuring the System-wide Settings

In the NuPoint UM Web Console:

1. From the navigation tree, click **Unified Messaging > STT Configuration**. If properly licensed, the Speech to Text configuration page is displayed.
2. Enter the following:

   - **Username**: Name of your NuPoint UM system.
   - **Password**: Your unique account password, provided by Nuance.
   - **Account ID**: Your unique account ID number, provided by Nuance.
   - **Application ID**: Your unique application ID name, provided by Nuance.

3. To include the original audio attachment of the voice message in the transcription emails for all users, select **Include audio attachments with email messages**.
4. Click **Save**.

Customizing the Class of Service

1. Customize an FCOS to include the following feature bits:

   - **285** (Enable Speech to Text) and assign it to mailboxes that will use this feature.
   - **295** (and an Advanced UM license) OR **304** (and a UM Standard license) OR **289** (and a UM-SMTP license).
   - **290** to view and/or save a text transcription of a voice mail message in the Web View.
2. Customize an LCOS with a Minimum Message Length greater than zero (0).

> **Note**:
> If you fail to set a minimum message length, brief messages (such as when a caller immediately hangs up) will be transcribed and cause a conversion credit to be consumed.

3. Apply FCOS and LCOS to the STT mailboxes.

Configuring Users

> **Note**:
>
> - To include the original audio attachment of the voice message with the text transcription email for all users, enable the Include Audio Attachments system-wide settings.
> - All users must accept the End User License Agreement before they can use the Speech to Text feature. (Administrators cannot accept on behalf of users.)
> - The appropriate feature bits must be assigned to the FCOS of the user's mailbox before the Speech to Text configuration fields are displayed in the Web Console.
> - Users should record a voice mail greeting to encourage callers to speak clearly. For example: "Please speak clearly as your voice message will be transcribed and sent to me in an email."

To configure STT for users:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.

3. Select a mailbox in the list, and then click Edit > Selected. The Mailbox data view is displayed (Basic view), populated with data for the selected mailbox.

   - For UM-SMTP Users:
     - Enter a valid email address in the **UM-SMTP Email Address** field.
     - From the delivery option list beside the Email Address field, select **Speech-to-Text**. All incoming voice mail messages (except Confidential, Record-a-Call, and Fax messages) are transcribed into text and sent as email messages to the specified email address.
     - Click **Save**.
   - For UM Standard Users:
     - Enter a valid email address in at least one of the **Standard UM Email Address** fields.
     - From the delivery option list beside the appropriate Email Address field, select **Speech-to-Text**. All incoming voice mail messages (except Confidential, Record-a-Call, and Fax messages) are transcribed into text and sent as separate email messages to the specified email address.
     - Click **Save**.

   Note:
   For UM Standard Users, it is possible to configure Speech to Text using the Text Console (see the *NuPoint Unified Messaging System Administration* online help, available at Mitel OnLine).

   - For UM Advanced Users:

   Note:
   Prior to using STT for UM Advanced users, you must program the smart host in the MSL Server Manager on the E-Mail settings screen. The smart host can be entered as IP address or a FQDN.

     - Enter a valid **Advanced UM Email Alias / Full Name / Address**and**Advanced UM Email Password** .
     - Select the **Enable Speech-to-Text Transcription** check box. All incoming voice messages are automatically transcribed and sent as email messages to the user's account. **Note**: The transcriptions are sent as separate emails and are not synchronized. (Only the original voice message with audio attachment is synchronized with the user's Inbox and/or MWI.)
     - Click **Save**.

Note:
To take advantage of Secure IMAP, you must enter the correct authentication settings in the Exchange Server.

Alert Users of the Following:

- The STT feature is *not* a dictation service. While transcription accuracy can be very good, there may be instances when the transcription does not accurately represent the spoken message. If in doubt, listen to the original voice message.
- Most callers do not speak in full and complete sentences; the transcription service will attempt to reflect this with spaces and punctuation.
- Transcription quality depends on the clarity of the original voice message. For example, if the person has a heavy accent or does not speak clearly, or is speaking from a noisy from a noisy environment, then the message will not be transcribed correctly.
- If the system cannot understand a voice message, it will not transcribe it. Instead, the user will receive an email notification. Typically, about 15% of messages are deemed "untranscribable."
- The system is "tuned" to transcribe typical English conversation. In many businesses however, messages may contain jargon, phrases and acronyms that are difficult to transcribe.
- The service is available in North American English only. For this reason, users who receive a significant number of voice messages in a different language should not be enabled for STT.
- The maximum message length is 60 seconds. For longer messages, users can dial in and listen to the entire original voice mail.

26.122.3 Activating or Terminating Speech to Text

Activate the Speech to Text Feature After Account Renewal

If your Nuance account credits become depleted, no further transcription is done. NuPoint UM disables the Speech to Text feature until you have corrected the account balance and re-activated the feature.

Note: Voice messages that are left while the Speech to Text feature is disabled will not be transcribed.

To re-activate Speech to Text:

1. From the navigation tree, click **Unified Messaging > STT Configuration**.
2. Click **Activate**.

Note:
The Activate button only appears when the feature has been disabled due to Nuance credit depletion. If you click Activate without correcting your account balance, NuPoint UM will disable the feature again.

Terminate the Contract and Disable Speech to Text

- Contact the your Authorized Reseller and cancel your Nuance account. NuPoint UM disables the service and displays alarms.

To clear the alarms:

1. From the navigation tree, click **Unified Messaging > STT Configuration.**
2. Clear the **User name**, **Password**, **Account ID**, **and Application ID** fields and then click **Save**.
3. Remove the Speech to Text feature bit (285) from the FCOS of all user mailboxes.

26.122.4 Speech to Text Alarms

NuPoint UM

When an error is detected in the process of transcribing a voice message, an alarm is raised. You can view alarms using the Web Console, Text Console, or email and SNMP clients. See Alarm Manager for more information about handling/clearing alarms.

Speech to Text Provider (Nuance)

The following types of error may arise as part of the interaction with the Nuance Speech to text service:

- Problem with the Speech to Text account (invalid username or password, limited or disabled account, etc.)
- Conversion credits nearing depletion.
- Conversion credits depleted.

Conversion Credit Alarms

Nuance informs NuPoint UM concerning the status of the conversion credits, which in turn result in alarms. It is the responsibility of the administrator to configure NuPoint to issue email notifications of these alarms. See Alarm Manager for more information.

The alarm behavior is as follows:

- When only 20% of the conversion credits are remaining, a Warning-level alarm is issued with the following message: "Your system currently has XXX credits remaining. Please buy additional credits."
- After seven daily Warning alarms are issued, the alarm level is raised to Minor.

- After seven daily Minor alarms are issued, the alarm level is raised to Major with the following message: "Your system currently has XXX credits remaining. Please buy additional credits. The Speech to Text service will stop working if your system runs out of credits."
- If the credits run out completely a final alarm will be provided indicating that Speech to Text is no longer working and NuPoint will disable the feature. The alarm message is: "Your NuPoint System has run out of speech to text credits. Transcriptions will no longer be provided to users. Please contact Mitel to purchase more credits."

If you purchase additional credits before running out, the alarms will cease and no further action is necessary. If, however, you purchase credits after allowing them to run out, you must then reactivate the Speech to Text feature in order to communicate with Nuance again. For details, see Activating the STT Feature after Account Renewal.

26.123 Speech Navigation - Description

Speech Navigation is an optional, licensed feature of NuPoint UM that enables users to manage their mailboxes using voice commands. Instead of struggling to find and press a button on their telephone dial, they can simply “say the command." This is particularly helpful for drivers who wish to use their cell phones in hands-free mode.

Features

Speech Navigation offers the following features:

- **Tutorial**

  A brief tutorial explaining the basic operation of Speech Navigation is played when a user logs in for the first time. The tutorial explains the available commands as well as the submenus that are not fully voice-enabled.
- Help

When a user asks for help, the system will list the commands that are available with Speech Navigation and with the telephone user interface.

- **Multiple Command Options**

  Speech navigation supports the concept of aliases so that up to two different phrases can be used to accomplish the same task. For example, users can say, “Delete Message” or “Discard Message” to delete a voice message.
- Barge-In

This feature allows users to interrupt a system prompt with a speech or keystroke command. The system stops playing the prompt and responds to the command. Barge-in allows experienced system users to skip quickly through the prompts.

- Error Handling

Speech Navigation responds to an error by instructing the user to retry the command. After three recognition errors, the system will play the prompt, "I do not understand that command. Please call again," and then disconnect the call.

- Mailbox Extensions

When Speech Navigation is enabled for a mailbox, it applies all of the user's extensions, including alternate extensions such as teleworker and cell phones. The enables users to call the message center from remote locations and immediately begin using Speech Navigation commands.

- Commands

The following commands can be invoked with Speech Navigation: Play Message, Keep/Save Message, Delete/Discard Message, Answer/Reply To Message, Forward/Give Message, Next Message, Make Message, User Options, Operator, and the digits zero to nine. In addition, users can leave the system by saying one of the following commands: Bye, Goodbye, Hang-up, or Quit. For detailed usage instructions, see the *NuPoint Unified Messaging User Guide*.

Conditions and Limitations

- You must purchase a license that specifies the total number of mailboxes that may use the Speech Navigation feature. Individual licenses are allocated to mailboxes on a per-user basis from this amount.
- Individual user licenses are assigned in numerical order. For example, if you purchase a Speech Navigation license for forty users and then activate the feature on fifty mailboxes (by assigning feature bit 99 to them), only the first forty mailboxes owners will be able use the feature.
- Speech Navigation users can be issue commands in North American English only. In a later release, users will be able to issue commands in either of two different languages from a selection of up to 50 languages.
- Some Speech Navigation commands, such as Make Message and Answer/Reply to Message, take the user to a menu that requires keystroke inputs on the telephone user interface.
- Up to 120 users (on a 120 port system) can simultaneously use speech navigation.
- Speech Navigation commands are not supported with the Competitive Telephone User Interface (TUI).

26.123.1 Speech Navigation Installation

The Speech Navigation feature requires a single system-wide license and an AMC synchronization. The basic software components (NuPoint UM Speech Recognition Prerequisites and NuPoint UM Speech Navigation) are bundled with the NuPoint UM base software and are automatically installed by the Master Installer blade.

To complete the installation, the administrator must manually install the following:

- NuPoint UM Speech Recognition American English prompts (DVD 2)

See Installing an Optional Feature for software blade installation instructions.

26.123.2 Speech Navigation Configuration

Configuration of the Speech Navigation feature consists of the following steps, detailed below:

- Assign the Speech Navigation Feature Bit to Mailboxes
- Manage Speech Navigation Licenses
- Configure Speech Navigation for Users (Administrative and User procedures)

Assigning the Speech Navigation Feature Bit to Mailboxes

Use this procedure to create a customized FCOS containing the Speech Navigation feature bit (99), and then assign that FCOS to mailboxes.

Provided that the number of mailboxes you program does not exceed the user license count, then all of the mailboxes can use the feature. However, if the number of mailboxes you program exceeds the user license count, then the license limit is applied to the mailboxes in numerical order. For example, if you assign feature bit 99 to five mailboxes but have only two user licenses, then the first two mailboxes (1111 and 1112) will be able to use the feature while the last three mailboxes (1113, 1114 and 1115) will be prevented from using it. If you then purchase two more user licenses, two more mailboxes (1113 and 1114) will be able to use the feature.

To assign the Speech Navigation feature bit to mailboxes:

1. Customize an FCOS to include feature bit 99 (Speech Navigation).
2. Apply the custom FCOS to the mailboxes you wish to make eligible for Speech Navigation.

Managing Speech Navigation Licensing

Use this procedure to determine the number of Speech Navigation licenses purchased, used and available, check whether a particular user is licensed, and export the list of licensed users.

Viewing the Speech Navigation License Counts

To view the Speech Navigation license totals:

1. Click **Speech Navigation > Licensing**.
2. View the license counts at the bottom of the screen:

- **Total Licenses** - the number of licenses that have been purchased.
- **Used Licenses** - the number of licenses that have feature bit 99 and have been assigned a license by the system.
- **Unused Licenses** - the number of licenses that remain available to be assigned to mailboxes.

Note: The number of used licenses will always be equal to or less than the Speech Navigation license limit. The number of unused licenses will decrease when you assign feature bit 99 to new mailboxes.

Searching for a Licensed User

To search for a licensed user:

1. Click **Speech Navigation > Licensing**.
2. In the **Find** field, enter a user's mailbox number or first/last name. If entering a name, a partial string is acceptable.
3. Click **Search**.
4. If you are unable to locate the user, click **Show All** and page through the complete user list by clicking **Next**.

Searching for a Licensed User File

To export for a licensed user file:

1. Click **Speech Navigation** > **Licensing**.
2. Click **Export**. The File Download window appears.
3. Click **Save** and select a location for the file. Rename the file if you want.
4. Click **Save**. The file is saved to the specified location in .CSV format.

Note:

1. The export function always exports the full list of licensed users, no matter what search may have been performed before. The exported user list is sorted alphabetically.
2. By default, Microsoft Excel does not display UTF-8 characters properly. To export a file with UTF-8 characters successfully, open the file in Notepad, click Save As and save the file without any changes.

Configuring Users

Administrator

The administrator is responsible to enable Speech Navigation for each user's mailbox. If the user has alternate extensions, such as cell phones, they may be configured at this time.

To enable Speech Navigation for the extensions on a user mailbox:

1. From the navigation tree, click Mailbox Maintenance, and then click Mailboxes.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Select a mailbox in the list, and then click **Edit** > **Selected**. The Mailbox data view is displayed, populated with data for the selected mailbox.
4. Optionally, click **Advanced** and enter up to four Alternate Extension numbers for internal or external phones (such teleworker or cell phones) that will share this mailbox.
5. On the **Misc** tab, select **Enable Speech Navigation**.
6. Click **Save**.

Speech Navigation is enabled for all configured extensions of the mailbox.

Mailbox Owner

The mailbox owner is responsible to enable Speech Navigation on the mailbox itself. This "turns on" the feature.

1. Open the Web View interface in a web browser.
2. Enter your Mailbox number and Passcode, and then click **Submit**.
3. Select the **Speech Navigation** tab.
4. Click **Enable Speech Navigation**.

Speech Navigation is "turned on" for the mailbox.

Alert Users of the Following:

- When Speech Navigation users call the message center, the system will prompt them to "say" their password in order to access their mailboxes.
- Users must say commands in North American English only.
- If a NuPoint system has foreign-language prompts installed, users must set their voice mailbox language to "English" in order to use Speech Navigation.
- The responsiveness of the system depends on the clarity and accuracy of the spoken command. For example, if the user has a heavy accent or does not speak clearly, or is speaking from a noisy from a noisy environment, then the system will not understand the command and prompt the user to repeat it. After a total three failed attempts, the system will play the prompt, "I do not understand that command. Please call again." The system will then disconnect the call.
- Users can "barge in" and say a command before the system finishes playing a prompt or message. For example, while the system is in the midst of playing a voice mail message, the user can say, "Next," and the system will skip to the next message. Or while the system is listing menu options, the user can say one of the options and the system will respond immediately.
- When a Speech Navigation user calls the message center from one of her extensions, she will receive a prompt asking her to "say" her mailbox password. When a Speech Navigation user calls the message center from an external number (not from one of her extensions), she will be prompted to log in by entering keystrokes for mailbox number and password. After logging in, she will be able to use Speech Navigation commands.
- If Speech Navigation is enabled for mailbox, the mailbox owner will receive prompts only for North American English. If the mailbox is configured to use non-English prompts, Speech Navigation prompt will not be played.
- The following commands can be invoked with Speech Navigation: Play Message, Keep/Save Message, Delete/Discard Message, Answer/Reply To Message, Forward/Give Message, Next Message, Make Message, User Options, Operator, and the digits zero to nine. For detailed usage instructions, see the *NuPoint Unified Messaging User Guide*.
- Users can exit the system by saying any of the following commands: Bye, Goodbye, Hang up, Quit.
- Users can go up one menu in the menu structure by saying, "Exit."
- If users are employing the Competitive TUI emulation feature, Speech Navigation commands are not supported.
- Users can hear help information about the Speech Navigation feature by saying "Help." The command causes the system to enumerate the commands the user can say using Speech Navigation and the keys the user may press using the TUI.
- If you enable Speech Navigation, the soft keys for the user's primary extension will be disabled.

26.124 Unified Messaging - Description

Unified Messaging (UM) allows you to integrate your NuPoint Unified Messaging voice mail system with your e-mail client for increased access to messages.

The following features are available with Unified Messaging:

- Basic Unified Messaging Features (SMTP Forwarding and Web View)
- Optional Unified Messaging Features (Standard UM and Advanced UM)

26.12.5 Basic Unified Messaging Features

The following Unified Messaging features are installed without charge as part of the "base package" in every NuPoint UM system.

SMTP Forwarding

The SMTP Forwarding (or "UM-SMTP") is enabled on a system-wide basis and can be deployed to all system users. It facilitates forwarding of voice mail and fax messages from NuPoint to e-mail addresses. Communication occurs in one direction, from NuPoint to the email server. Since there is no communication from the email server back to NuPoint, message waiting indication (MWI) synchronization is not supported.

To set up SMTP Forwarding, the system administrator configures each user's mailbox with an email address. Whenever a user receives a voice or fax message, a copy is forwarded to the specified email address. For voice messages, the email message includes an audio file (.wav) attachment that the user can listen to on a PC or smartphone.

A copy of the original voice or fax message is retained on the NuPoint UM system. As a result, the MWI on the user's telephone will remain even after the user has deleted the message from an email client. The MWI is extinguished only when the message is accessed via the telephone user interface (TUI). To minimize confusion, the system administrator may choose to disable MWI for users who prefer using an email client rather than a telephone to access their messages.

Web View

Web View is available to users on a system-wide basis. It enables them to access a visual representation of their NuPoint mailboxes through a URL and to manage their NuPoint mailboxes through a GUI instead of the TUI. It supports MWI synchronization. In other words, when a user listens to a message in Web View, the MWI lamp will turn off, just as it would after listening to the message through the TUI.

Web View allows users to perform actions that blur the boundary between voice, fax, and email messaging:

- Access voice and fax messages from Web View.
- Access voice, fax, and Record-A-Call (RAC) messages from the telephone user interface (TUI).
- Reply to voice or fax messages by email to other Web View users; forward voice or fax messages via email by entering the recipient’s email address
- Save voice or fax messages to an email mailbox for archiving as a .WAV file.

In addition, all Unified Messaging users can configure the encoding format for their audio files on the Settings tab of the Web View interface.

Web View supports the following number of simultaneous sessions:

- NuPoint 60: 50 simultaneous sessions
- NuPoint 120: 60 simultaneous sessions

- Virtual NuPoint: 60 simultaneous sessions

See the *Web View Online Help* for information about Web View settings.

26.12.6 Optional Unified Messaging Features

In addition to the base features, SMTP Forwarding and Web View, NuPoint UM offers two other Unified Messaging features:

- Standard UM
- Advanced UM

Standard UM and Advanced UM are optional applications that require extra licensing and software blade installation. They provide the following benefits:

- Easier and faster message management. NuPoint UM displays voice and fax messages visually in the users' e-mail clients, enabling them to see the following at a glance:
- A listing of voice and fax messages.
- Message caller ID information. This enables smart phone users to return the call simply by clicking on the number contained in the message.
- Message date and time.
- Status. Urgent messages are flagged with an exclamation point, confidential messages with a lock (if the email client supports these indicators).
- Users can click on the message to hear it through a media player on their device.
- Users can save messages. For users accessing their voice messages using Standard UM, the Save function automatically copies selected messages to their default email address. These messages then appear in the user’s email inbox as an email message with a WAV file attachment. The messages can be moved to a folder, archived, or sent via e-mail to users outside the NuPoint system.

Standard Unified Messaging

Standard UM provides users with numerous options to manage their messages. Using the Settings tab in Web View, users can set parameters associated with the consolidation of their voice, fax, and email messages.

When a voice mail is received, NuPoint sends a message to the mailbox owner’s email account via the SMTP service. The subject of the message includes the original sender’s telephone number, a time/date stamp and a subject line that adheres to this format:

"Voice Message from <Name/CLID/Mailbox Number/Unknown Caller> MB:<To Mailbox Number>".

The body of the message can include:

- A simple text notification that a new voice message has arrived. The voice message is stored only in NuPoint.
- An audio attachment (.wav or .mp3 file). Listening to the attachment does not update the MWI. The voice message is stored in NuPoint and the email server.

- A hyperlink to Web View. The user can log into Web View and manage the message from the Web View messages tab. Actions taken within Web View will update the MWI. The voice message is stored only in NuPoint.

Note:

Record-A-Call messages appear in the Web View screen but are not sent to the user's e-mail inbox.

- An Audio Link to the specific message. The user can listen to the (new) message by clicking on the hyperlink. This will update the MWI. The voice message is stored only on NuPoint.

In most situations, there is no synchronization between the voice mails stored on NuPoint Unified Messaging system and the voice mails in the users' e-mail account or with the message waiting indicator (MWI) on their phone. The only exception occurs when the e-mail includes a link to the voice mail as an audio file. Listening to the file will mark the message as played in the NuPoint voice mail box; however, playing a message in the voice mail box will not mark the e-mail as read on the e-mail server.

Standard UM supports connections to SMTP email servers, including relay servers such as Microsoft 365 and Google.

Note:

- The "link to the message in Web View" option requires that your server translate the FQDN. If you have a corporate DNS server, ensure that the FQDN is associated with the appropriate IP address. If you do not have a DNS server, you need to use a text editor (like Notepad) to make an IP/FQDN equivalency entry in the system HOSTS file of the client PC (C:\WINDOWS\SYSTEM32\DRIVERS\ETC).
- For voice mail that is received as "Confidential" (forwarding not allowed) the NuPoint Unified Messaging system creates an e-mail message without a voice attachment and sends it to the user. In the body of the e-mail message, the user is directed to listen to the message over the phone.
- For NuPoint deployments that are configured with the Web Proxy service of the MiVoice Border Gateway , the audio file links are valid both inside and outside the corporate network provided that DNS is configured correctly. An external DNS server should resolve your Virtual Host name (for example, "MAS1.mitel.com") to the corporate firewall, and your internal DNS server should resolve the LAN host name (also "MAS1.mitel.com") to the actual server on the LAN.

Advanced Unified Messaging

With Advanced Unified Messaging, users can receive all their voice, fax, and emails through a single interface—whether it’s the TUI or the email client. Actions taken on one interface are reflected on the other.

Advanced UM provides the following features:

- Voicemail and fax messages are duplicated in the user's email account—and therefore on the email server.
- Users can manage all voicemail, fax, and email messages from within a supported email client.
- NuPoint and the email server are synchronized so that actions taken on one system are reflected on the other. An email message (with audio attachment) is created for each voice message. For example:
    - When a user listens to a voice message through the TUI, the matching email message will be marked as "read" in the user's email inbox.
    - When a user clicks on an email message containing a voice or fax message using an email client, the message will be marked as "read" and the message waiting indicator (MWI) will turn off on the user's telephone. Note that the user may not have listened to the voice message in the attachment.
    - When a user deletes an email message containing an audio file using an email client, the matching voice message will be permanently deleted from the user's voice mailbox.
    - When a user deletes a voice or fax message using the TUI or Web View, the matching email message will be deleted in the user's email inbox. On most email systems, the email will be moved to the "deleted" folder (and, if necessary, may be recovered from there).

Advanced UM can be implemented on a NuPoint 60 platform with support for 1200 mailboxes, or a NuPoint 120 with 2500 mailboxes. One Advanced UM license is required per mailbox that employs the feature.

Advanced UM supports IMAP connections to Microsoft Exchange servers, or to hosted email services such as Microsoft Office 365 or Google Apps. For a list of supported configurations, see Mail Server Adapter Types.

Microsoft Exchange and Outlook Integration with NuPoint Voice

This option is based on an integration between the Microsoft Exchange server (e-mail server) and the NuPoint UM server (voice mail server). Emails on the Exchange server can be accessed by the NuPoint UM server so that voice mails and emails are accessible through both the Outlook client email and the NuPoint UM voice mailbox. The optional **Active Directory plug-in** provides LDAP-like directory services.

Also optional, users can install the **Outlook Client plug-in**, which provides a greater level of integration by installing:

- the Mitel Networks QuickPlayer in each Outlook client, which provides the ability to play voice messages over the PC speakers or using a Call Me/Meet Me session
- the Unified Messaging toolbar in the Outlook client so that users can reply to, create, and forward voice messages. The UM toolbar also enables users to launch Web View from Outlook.

Users who do not install the Outlook Client Plug-in:

- Will not have access to the UM toolbar (can use the default Windows media player to play voice messages)
- Will have voice mail messages displayed in Outlook with an email icon (rather than a speaker icon)

Microsoft Exchange integrations support IMAP protocol.

Google Apps with NuPoint Voice

This option is based on an integration between the Google Apps for Business hosted email server and the NuPoint UM server (voice mail server). The Google Apps integration uses IMAP (only) to synchronize with NuPoint Unified Messaging. The OAuth protocol is employed to provide access to email accounts in Google Apps, and eliminates the need for users to enter their email passwords on the NuPoint UM system.

26.126.1 Configuring UM-SMTP, UM-Web View and Standard UM

Overview

Configuring Standard UM consists of the following tasks:

- Ensure that you have purchased enough UM licenses and assigned them to the mailboxes you want to enable for UM
- Configure Standard UM parameters
- Configure Outbound SMTP Server (Smart Host) settings
- Configure the user mailbox
- Force a license update

These procedures can be performed using the Web Console (instructions below) or the Text Console (see the *NuPoint Unified Messaging System Administration* online help, available at Mitel OnLine).

Configure Parameters for UM-SMTP

1. From the navigation tree, click **Unified Messaging**, and then click**UM-SMTP**.
2. The **UM-SMTP Configuration** screen appears.
3. Enter the following configuration information:

    - In the **Queue Size** field, enter the size of the queue for messages sent using Reply and Forward in Web View. The default value is 200. Maximum value is 1000. Do not modify this value unless you are experiencing problems with lost messages or the queue becoming full.
    - In the**Corporate Callback Number**field, enter the callback number to be included in the body of Standard and Advanced email notifications. Enter the callback number in a format that can be recognized by mobile devices (valid characters are 0-9, +, -, #, *, space, parentheses, period, and comma).

Note:

The **Smart Host Domain Name** field contains the IP address or Fully Qualified Domain Name (FQDN) of the e-mail server, which you can configure in the MSL Server Manager on the E-Mail settings screen. If you use an FQDN, configure it with an MX record in the corporate DNS.

4. Click **Save**.

Configure Parameters for UM-Web View and UM Standard

Note:

All Web View user's messages are transferred via HTTPS.

1. From the navigation tree, click **Unified Messaging**, and then click **UM-Web View**.
2. The **UM-Web View Configuration** screen appears.
3. Enter the following configuration information:

- The **Add UM Web View Sessions** field shows the maximum number of Web View sessions allowed by your license. This field is read-only.
- In the **Queue Size** field, enter the size of the queue for messages sent using Reply and Forward in Web View. The default value is 200. Maximum value is 1000. Do not modify this value unless you are experiencing problems with lost messages or the queue becoming full.
- In the **Refresh Speed** field, enter the frequency, in minutes, at which the Web View GUI should refresh. **Note**: The smaller the number in this field (the more frequently the Web View GUI refreshes) the higher the network traffic the Web View GUI will generate.
- In the **Session Timeout** field, enter the length of time, in minutes, a session should remain active without any user activity. This field also determines how long the session will remain locked if a user closes the web browser without logging out.
- Select the **Transfer Media Files Over Secure HTTP** if you want Web View users' messages to be transferred over secure HTTP (HTTPS).

Note:

The **Smart Host Domain Name** field contains the IP address or Fully Qualified Domain Name (FQDN) of the e-mail server, which you can configure in the MSL Server Manager on the E-Mail settings screen. If you use an FQDN, configure it correctly in the corporate DNS.

4. Click **Save**.

Configure Outbound SMTP Server Settings

NuPoint UM can communicate with an outbound SMTP server using one of the following connections:

- Port 25 (standard SMTP)
- Port 465 (secure SSL SMTP)
- Port 587 (secure TLS SMTP)

If you employ a secure port (465 or 587) to connect with an outbound SMTP mail server, you will be required to enter authentication details (User ID and Password) and your account may be subject to usage limitations.

Note:

You must use the MSL Server Manager to configure the SMTP server settings. Once setup is complete, you can review the settings in the NuPoint Web Console (in the Offline Configuration under Unified TCP/IP) or in MSL.

To configure the outgoing SMTP relay server settings:

1. Log in to the MSL Server Manager as "admin."
2. From the navigation tree, click **Configuration**, and then click **E-Mail Settings**.
3. Click the **Change** button beside the setting you want to change.
4. Configure the settings as required and then click **Save.**

Note:

The Admin should always restart the NuPoint UM after changing the SMTP server.

Setting	Description
Server to use for outbound SMTP	The server can deliver outgoing messages via a corporate or Internet service provider's SMTP server, or can deliver messages directly to their destination (by looking up mail exchanger records in DNS). If using a specific SMTP server, specify its hostname or IP address. Otherwise leave this field blank. The server hostname is limited to 16 characters, maximum. **Note**: • If you are connecting directly to Google Apps, enter smtp.gmail.com as the outbound SMTP server hostname. Also, you must update the Google security settings as follows: 1. Open a web browser and navigate to the administrative console for your Gmail domain: admin.google.com 2. Navigate to **Security** > **Basic security settings** > **Less secure Apps**. 3. Select the **Enforce access to Less secure apps for all users** option. 4. Click **Save**.

Setting	Description
	• If you are connecting directly to Microsoft Exchange Online (Office 365), program the outbound SMTP server hostname as follows:
	1. Log in to the Microsoft Online Services Portal (https:// login.microsoftonline.com) 2. Access the account that is being used to send mail. 3. Under Outlook, click **Options**. 4. On the Account > My Account tab select **Settings for POP, IMAP, and SMTP access**. 5. Under SMTP access, locate the server name (for example, pod51010.outlook.com) and enter it as the SMTP server hostname.
Destination port for outbound SMTP	If you have specified a server to use for outbound SMTP, select the destination port for outbound SMTP messaging: • **Port 25** (use cleartext; default) • **Port 465** (SSL encryption) • **Port 587** (TLS encryption)
Mail Server User ID	If the SMTP server is using is using secure port 465 or 587, or port 25 with Google Gmail, enter the required user ID. This ID must be configured and licensed in the SMTP server.

Setting	Description
Mail Server Password	If the SMTP server is using is using secure port 465 or 587, or port 25 with Google Gmail, enter the required password. This password must be configured and licensed in the SMTP server. **Note**: Some SMTP relay servers that employ secure SMTP, such as Microsoft 365 and Yahoo, may require that messages contain a "From" address that matches the authorized account ID. See From Address Specification for configuration instructions.
SMTP e-mail injection restrictions	Controls which networks will be allowed to send mail through this server via SMTP. Choose from one of the following three settings: • **Localhost only** – accept e-mail only from applications installed on the server (default setting). • **Accept only from local networks** – accept e-mail from local networks that are directly connected to the LAN. (These networks are on the same subnet as the server's private interface.) • **Accept from anywhere** - accept all e-mail

Setting	Description
Forwarding address for administrative e-mail	By default, e-mail to the administrator is sent to the user " admin" at the domain name configured on the server. You can override the default by entering an e-mail address in this field. **Note**: RAID array event notifications are sent to this e-mail address. We recommend that you configure a valid address here.
E-mail sent for events:	Select the system events for which you want to receive e-mail notifications — Cleared, Indeterminate, Warning, Minor, Major, Critical. By default, Major and Critical are preselected. The e-mails are sent to the " admin" mailbox. To turn off e-mail notifications clear all the event boxes.

From Address Specification

By default, NuPoint includes the user's calling line ID (CLID) in the "From" address of email messages (e.g. CLID_6135922122@domain_name.com). However, SMTP relay servers such as Microsoft 365 and Google and some SPAM filters will not accept this format and instead require that all messages contain a "From" address that matches an authorized account ID. If your enterprise requires use of an authorized account ID, you must configure it in MSL as the Mail Server User ID (the user ID must be in the format of an email address), add it to your SMTP server or SPAM filter, and then employ the following procedure to select it for use.

To specify the "From" address format for NuPoint email messages:

1. From the navigation tree, click Unified Messaging > Smarthost Configuration.
2. In the **"From" address for all sent emails:** field, select one of the following options:

   - **Use the Mail Server User ID configured in the MSL server-manager** - NuPoint inserts the Mail Server User ID in all sent emails. Select this option if your environment includes an SMTP server that uses secure port 465 or 587, or a SPAM filter that requires a single authorized account ID. To complete the configuration, add the user ID to your SMTP server and/or SPAM filter. **Note**: In

Standard UM emails, the administrator email ID (the Mail Server User ID) will be displayed in the “from” field irrespective of whether the mailbox user’s email address is configured.

- **Let NuPoint determine the "From" address** - (default) NuPoint inserts each user's CLID or name in all sent emails. Select this option if your environment does not include an SMTP server that uses secure port 465 or 587, or a SPAM filter that requires a single authorized account ID.

Note:

For Google Apps implementations, when NuPoint receives a call from an external source, the system will insert the Mail Server User ID, in addition to the user's CLID or name, in the From header of sent emails. For more information on this limitation, see Google Apps Configuration Requirements and Usage Limits.

3. Click **Save**.

Note:

The **Smart Host Domain Name** field contains the IP address or Fully Qualified Domain Name (FQDN) of the e-mail server, which you can configure in the MSL Server Manager on the E-Mail settings screen. If you use an FQDN, configure it correctly in the corporate DNS.

Configuration Requirements if Connected Directly to Outbound SMTP Server

If NuPoint UM connects directly to a hosted SMTP mail server such as Google Apps or Microsoft Exchange Online (Office 365), it may be subject to particular configuration requirements and usage limitations.

Google Apps Configuration Requirements and Usage Limits

- The corporate DNS settings on the local server must be able to resolve to the Google Apps outgoing SMTP server hostname (smtp.gmail.com). DNS settings can be configured under "Domains" on the MSL Server Manager.
- Direct connections to the Google Apps SMTP server must be made through a secure SMTP Port (465 or 587) using a single, authenticated user account. As a result of this setup, Google's SMTP server delivers all email messages with the same "Reply To" email address. For example, if someone from extension 1120 leaves an email message for mailbox 4009, the message's From field will contain a unique name such as John Smith but a common email address such as admin@company.com. To alleviate this limitation, configure a Google Apps account that indicates the messages are originating from a NuPoint voicemail server. For example, use nupoint.voicemail@mitel.com rather than admin@mitel.com. Also enter this address in MSL as the Mail Server User ID.

- If you connect directly to the SMTP server using a single, authenticated user account, the account will be subject to sending limitations to prevent email spamming. For example, Google Apps has a sending limit of 2,000 email messages per day. Once that limit is reached, the account will be locked for 1 to 24 hours, preventing further emails from being sent. In addition, the account will also be locked if too many emails are sent during a short period of time. While the account is locked, Google rejects new email with a "Daily sending quota exceeded" error and the event is logged in / var/log/ qmail. (Note that Google controls the account lockout triggers and time periods, and does not publish the exact limits.) We strongly recommend that only customers with a small number of users (fewer than 80 mailboxes) use Google Apps directly instead of an SMTP relay server.
- Because sending limitations apply to all SMTP emails sent from your system (including emails generated by the alarm manager, and fax confirmation), direct connections to Google Apps should be implemented only by smaller organizations. A safe limit is 80 user mailboxes, based on typical call/port usage patterns.
- In some cases, Google Apps may treat email from NuPoint UM as spam. To correct this problem, you must add the NuPoint server to the email whitelist on the Google Apps domain as follows:

1. Log in to the Google Apps administrator control panel: https:// www.google.com/a/ cpanel/ yourdomainname
2. Click the **Settings** tab and select **Email**.
3. Locate the Email Whitelist section and enter the external IP address(es) of the NuPoint UM server.
4. Click **Save**.

Microsoft Exchange Online (Office 365) Configuration Requirements and Usage Limits

The limits on messages, mailboxes, recipients, and e-mail clients can be found online at this address: http://help.outlook.com/en-US/140/dd630704.aspx.

These limits are intended to protect Microsoft's servers from being used as a source for spam generation. Of note are the message rate limit of 30 messages per minute and the recipient rate limit of 1,500 recipients per day. Since the NuPoint is configured to send mail from a single authenticated user account, these limits apply system-wide.

Once a limit is exceeded, Microsoft's mail server will bounce any mail sent from the account until the time limit has expired. The Microsoft mail server will return one of two types of failures—temporary or permanent. In the case of a temporary failure, the message is resent by NuPoint. In the case of a permanent failure an alarm will be raised to the NuPoint system administrator indicating that a voice mail message has been returned with an error. Also, an email sending error will be logged in the /var/log/qmail logfiles directory.

Since the MSL outbound SMTP server setting applies to all SMTP mail sent from MSL, all applications running on MSL will then contribute towards the daily limit. This means alarm manager emails, fax confirmations, and any other application which sends SMTP email from MSL will contribute to the daily limit.

Accordingly, you should connect directly to the Microsoft Exchange Online (Office 365) only if you have small number of users (e.g. 60 mailboxes based on typical use patterns). If you have a large number of users, you should employ an outbound SMTP server without restrictive usage limits such one located in your enterprise network.

In its role as an SMTP relay server (smart host), Office 365 will only process messages containing a "From" address that matches the authorized account ID. To ensure that NuPoint provides this ID rather than unique CLIDs, program the From Address Specification.

Configure User Mailbox

1. From the navigation tree, click Mailbox Maintenance >Mailboxes.
2. Click **Add** to create a new mailbox, or search for an existing mailbox and click a mailbox number to edit it.
3. Select the **Class of Service** tab.
4. From the **Feature Class of Service** drop-down menu, select a Features class of service that includes the appropriate feature bits:

For this User:	Add these Feature Bits:
Standard-SMTP	289
Standard-Web View	250, 251, 252, and 290
Standard	304

5. Select the **General** tab and update parameters in the **Personal Information** and **Unified Messaging** sections.

Note:

- Enter the user's e-mail address, or addresses, in the **UM Email Address** fields. Users can add or change their e-mail addresses using Web View. For the UM-SMTP user type, no other Web View functions are available.
- For **UM Audio Encoding**, select **ADPCM**, **GSM 6.10**, or **MP3**. Since MP3 uses more processing resources, select it only if ADPCM and GSM 6.10 cannot be played on the user device or if the user is employing a hosted/ webmail web service such as Gmail.

6. Click **Save**.

Configure Unified Messaging Limits

Using Web Console, you can limit the use of hard drive space by specifying that voice mail messages be forwarded to email clients in text format only. To do so, you configure the Unified Messaging Limits feature using LCOS.

To specify voice mail messages be forwarded to email clients in text format only:

1. From the navigation tree, click **Class of Service >**Limits COS.
2. In the right pane, select **Default** (LCOS 1).
3. Select **Unified Messaging Limits** from the drop-down menu.
4. After **Allow All SMTP Delivery Formats**, select **No**.

   Selecting "No":

   - Limits all users to text notifications only. It limits both UM-SMTP and Standard UM, overriding all FCOS settings that relate to SMTP forwarding.
   - Completely disables FCOS bit 289
   - Overrides FCOS bit 304 and prevents notifications for email addresses for which a notification method other than Text Notification was selected
   - Limits FCOS bit 304 to Text Notification only for email addresses for which Text Notification was selected

Note:

- If you apply the Unified Messaging Limits LOCS, we recommend you do NOT use FCOS with bit "261 - Allow NP PWG View WEB access to messages".
- To prevent audio file leaks, you can limit user access to messages in Web View by removing FCOS 290.

Force a license update (not required for UM-SMTP or UM-Web View)

1. From the navigation tree, click **Unified Messaging**, and then click **UM User Licensing**.
2. Click **Update UM User Licensing**. Confirm the update. The Standard UM feature is now activated.

Note:

- For MiCollab deployments of Standard UM, you cannot force a license update by selecting the **Update UM User Licensing button**. Instead, you must access the MiCollab Users and Services application and enable **Standard Unified Messaging**.
- Updating UM User Licensing causes a scan of mailboxes that may take some time to complete and may place an extra load on the system.

26.126.2 Configuring UM-SMTP, UM-Web View and Standard UM

Overview

Configuring Standard UM consists of the following tasks:

- Ensure that you have purchased enough UM licenses and assigned them to the mailboxes that you want to enable for UM
- Configure Standard UM parameters
- Configure Smart Host settings
- Configure the user mailbox and force a license update

Configure parameters for UM-SMTP

1. Log in to the admin console as "root".
2. From the main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**.
3. In the Unified Messaging menu, select **(B) Standard UM-SMTP**.
4. To configure a **Corporate Callback Number** to be included in the body of Standard and Advanced email notifications, select **(C) Corporate Callback Number**. Enter the callback number in a format that can be recognized by mobile devices. Note: If your system does not have Speech Auto Attendant, you can configure a Line Group Call Flow to act as attendant.
5. Configure the queue size if required. (Do not modify this value unless you are experiencing problems with lost messages or the queue becoming full.)
6. Exit from the Text Console.

Configure parameters for UM-Web View

Note:
All Web View user's messages are transferred via HTTPS.

1. From the main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**.
2. In the Unified Messaging menu, select **(C) Standard UM – Web View.**

3. Configure the following parameters: [defaults are shown in brackets]

   - (**A**) Add UM Standard Web view Sessions [5]
   - (**R**) Refresh Speed [4]
   - (**T**) Session Timeout [5]
   - (**Q**) Queue Size [200] (Do not modify this value unless you are experiencing problems with lost messages or the queue becoming full.)
   - (**H**) Transfer Media Files Over Secure HTTP [n]. (Change this option to Y if you want Web View users' messages to be transferred via HTTPS.)
4. Exit from the text console.

Configure Standard UM Parameters

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**.
2. In the Unified Messaging menu, select **(E) Standard UM**.
3. Configure the queue size if required. (Do not modify this value unless you are experiencing problems with lost messages or the queue becoming full.)
4. Select **(U) Update Standard UM User License** to apply licenses to configured mailboxes.

Configure Outbound SMTP Server Settings

NuPoint UM can communicate with an outbound SMTP server using one of the following connections:

- Port 25 (standard SMTP)
- Port 465 (secure SSL SMTP)
- Port 587 (secure TLS SMTP)

Complete the configuration in the MSL Server Manager. For details, see Configure Outbound SMTP Server Settings.

Note:
You must use the MSL Server Manager to configure the SMTP server settings. Once setup is complete, you can review the settings in NuPoint or MSL.

Configure From Address Format

By default, NuPoint includes the user's calling line ID (CLID) in the "From" address of email messages (e.g. CLID_6135922122@domain_name.com). However, SMTP relay servers such as Microsoft 365 and Google and some SPAM filters will not accept this format and instead require that all messages contain a "From" address that matches an authorized account ID. If your enterprise requires use of an authorized account ID, you must configure it in MSL as the Mail Server User ID, add it to your SMTP server or SPAM filter, and then select it for use in the following procedure.

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**.
2. In the Unified Messaging menu, select **(S) Smarthost Configuration**.
3. For the **Email from address must match account name** parameter, select **(Y) Yes** or **(N) No**.
4. Exit from the text console.

Configure Smart Host Settings

To support the forwarding of emails to users who are not Advanced UM users, through the Outlook Client Plug-in you must configure the Smart Host. Emails are sent using SMTP forwarding through the NuPoint UM system, not the Outlook client.

To configure Smart Host settings for NuPoint UM:

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(G) Offline Menu**, **(B) Duplicate Active Configuration**, and **(U) Unified TCP/IP.**
2. In the Unified TCP/IP menu, select **(M) Configure a Module**.
3. In the Ethernet Card Configuration menu, select **(V) Smart Host Domain Name**. You are prompted to enter the fully qualified domain name (FQDN) of the smart host.
4. Enter the **FQDN or IP address** of the mail server (for example, mailserver.company.com).
5. Activate the configuration .

Configure User Mailbox

1. Program an FCOS for UM users:

   - Log in to the admin console as "root".
   - From the main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, and then **(F) Feature COS.**
   - Select **(C) Current FCOS** to modify and enter a number for this FCOS.
   - Select **(N) Name FCOS** and enter a name for this FCOS (for example, StdWebView).
   - Select **(A) Add Features** and add the following feature bits for each type of user:

For this User:	Add these Feature Bits:
Standard-SMTP	289
Standard-Web View	250, 251, 252, and 290
Standard	304

2. Modify the user's mailbox:

   - Assign the FCOS you programmed to the mailbox.
   - Enter the user's e-mail addresses in the **New UM Standard E-mail address** fields and select the delivery option for each.**Note**: If Audio Link is selected, messages that are played using a link in the email client will be marked as "Read" in the voice mailbox.
   - Select a **UM audio encoding** method:

Encoding Method	Description
ADPCM (default)	Microsoft audio encoding.
GSM 6.10	Audio encoding with wider support for mobile devices
MP3	Use MP3 only if ADPCM and GSM 6.10 cannot be played on the user device, or if the user is employing a hosted/webmail web service such as Gmail or Yahoo Mail.
MP3 may result in poorer sound quality than the other audio encoding methods. If your implementation includes the BlackBerry Enterprise Service 10 (BES 10), you may use MP3 or GSM 6.10 but not ADPCM.	

3. To update the User list for Standard UM after adding bit 304 to ensure user is added:

   - In the Unified Messaging menu, select **(E) Standard UM** and then select **(L) List Standard UM** User mailboxes.

Note:

Users can modify their email addresses from Web View.

Force Manual License Update

To force a manual license update: (not required for UM-SMTP or UM-Web View)

- From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**, and **(E) Standard UM**.
- In the Standard UM menu, select **(U) Update Standard UM User License**.

Note:

- For MiCollab deployments of Standard UM, you cannot force a license update by selecting the **Update Standard UM User License** option. Instead, you must access the MiCollab Users and Services application and enable **Standard Unified Messaging**.
- Updating UM User Licensing causes a scan of mailboxes that may take some time to complete and may place an extra load on the system.

Configure Unified Messaging Limits

Using Web Console, you can limit the use of hard drive space by specifying that voice mail messages be forwarded to email clients in text format only. To do so, you configure the Unified Messaging Limits feature using LCOS.

To specify voice mail messages be forwarded to email clients in text format only:

1. Access Web Console.
2. From the navigation tree, click **Class of Service >**Limits COS.
3. In the right pane, select **Default** (LCOS 1).
4. Select **Unified Messaging Limits** from the drop-down menu.
5. After **Allow All SMTP Delivery Formats**, select **No**.

   Selecting "No":

   - Limits all users to text notifications only. It limits both UM-SMTP and Standard UM, overriding all FCOS settings that relate to SMTP forwarding.
   - Completely disables FCOS bit 289
   - Overrides FCOS bit 304 and prevents notifications for email addresses for which a notification method other than Text Notification was selected
   - Limits FCOS bit 304 to Text Notification only for email addresses for which Text Notification was selected

Note:

If you apply the Unified Messaging Limits LOCS, we recommend you do NOT use FCOS with bit s "285 - Enable Speech-to-Text" or "261 - Allow NP PWG View WEB access to messages". It is important to prevent the Speech to Text option from being used and prevent users from saving voice mail messages to their PCs.

Note:

To prevent audio file leaks, you can limit user access to messages in Web View by removing FCOS 290.

Using Corporate Callback on Systems without Speech Auto Attendant

If Speech Auto Attendant is not enabled on your system, you can use Call Director to create a Line Group Call Flow to act as an attendant.

To create a Line Group Call Flow:

1. Create a Line Group for Call Director.
2. In the Call Director interface, create a call flow for Dial-back:

   - From the Call Flow list, select **Line Group** and enter the line group number.
   - Select the default action for New Call.
   - In the New Actions menu, select **Menu**.
   - In Menu Properties, enter a **name** for the call flow (for example, Call-back) and enter the **Max DTMF length** (extension number length).
   - In the Destination Action list, select the default action beside **Multi-key** and then select **Blind Transfer**.
   - In Blind Transfer Properties, in the **Transfer To** list, select **Gathered Digits**.

26.126.3 Mail Server Adapter Types

NuPoint Unified Messaging supports the IMAP messaging protocol as adapter types for connecting to email servers for voice mail synchronization and Text-to-Speech (TTS).

IMAP

The IMAP connector, which is deployed by default on NuPoint Unified Messaging, supports Microsoft Exchange Server 2016 and 2019, Microsoft Office 365 and Google Apps. The IMAP connector only supports one email server so it is targeted for small and medium-sized companies with one email server. Up to 1500 Advanced UM users are supported with Exchange and up to 750 Advanced UM users are supported with Office 365, and up to 2500 users are supported with Google Apps (Gmail).

To set up the email server for IMAP, see the following procedures:

- Configure IMAP for Exchange/Office 365
- Configure IMAP for Google Apps

Note:
In most cases, voice mail messages are sent immediately to the email server and then forwarded to the Advanced UM users. However, hosted email configurations such as Google Apps may experience slight delays due to virus scanning, anti-spam software, or routing delays caused by traffic volume. As a result, the timestamps of the original voice mail message and email audio attachment may not match.

When using IMAP with MS Exchange Server, you can create a superuser account (NPUMAdmin) for Advanced UM. Because *NPUMAdmin* has more privileges than the administrator account, it can access user accounts and inboxes in order to synchronize their voicemail and email messages.

26.126.4 Configuring Advanced UM

Task List

Configuring Advanced UM consists of the following tasks:

	Task List	Web Console Reference	Text Console Reference
1.	Verify that your NuPoint AMC license includes Advanced UM and a sufficient number of Advanced UM Mailbox licenses.	-	-

	Task List	Web Console Reference	Text Console Reference
2.	Print the Advanced Parameters worksheet and gather the required information.	-	-
3.	Configure the mail server:	If you are using an MS Exchange or MS Office 365 IMAP mail server, do the following: • configure IMAP • (optional) create a superuser account (for Exchange 2016/2019)	
		If you are using Google Apps IMAP mail server, do the following: • enable IMAP access • configure OAuth	
4.	Configure Advanced UM Parameters	Configure Advanced UM Parameters	Configure Advanced UM Parameters
5.	Enable Advanced UM for User Mailboxes (includes adding FCOS bits and forcing a license update)	Enable Advanced UM	Enable Advanced UM
6.	Configure Text-to-Speech and User dictionary as required	Configure Text-to-Speech	

The following optional steps are for Microsoft integrations only:

1. (Optional) Install Outlook Client Plug-in.
2. (Optional) Install Active Directory snap-in.

26.126.5 Advanced Parameters Worksheet

This worksheet provides parameters for both the Text Console and Web Console:

Web Console Tab	Parameter	Description	Your Value
NuPoint	(L) Administrator Login	The MSL administrator account needed to access NP-UM and examine mailboxes enabled for Advanced UM. Enter a string between 1 and 64 characters, without spaces.	
	(P) Administrator Password	Specify the password for the authoritative login name.	
	(I) Mailbox Poll Interval	The interval (in minutes or hours) when the system should poll for changes to the number of licensed users. The default setting is 60 minutes. Enter a value between one hour (60 minutes) and 24 hours (1440 minutes). **Note**: You must type the word "hours" or "minutes" as part of your input.	

Web Console Tab	Parameter	Description	Your Value
	(K) Permanent Delete (True/False)	Specify “true” to permanently delete replicated messages from the mail server when users delete messages using the TUI. Specify “false” to move replicated messages to the Deleted Items folder on the mail server when users delete messages using the TUI.	
	(V) Sender Domain [nupoint.com]:	The domain appended to the sender of Advanced UM e-mails. Enter a valid domain name that is between 1 and 64 characters.	
Mail Servers	(U) Unread Mail Poll Interval	Specify the interval (in seconds) when the system should poll the mail server for unread messages in the inbox to see if they have been read or deleted. The default setting is 5 seconds. Enter a value between 5 and 60 seconds.	
	(R) Read Mail Poll Interval	Specify the interval (in seconds) when the system should poll the mail server for any read messages in the inbox to see if they have been deleted. The default setting is 60 seconds. Enter a value between 10 and 60 seconds	

Web Console Tab	Parameter	Description	Your Value
	(E) Mail Server Timeout:	Specify the length of time (in seconds) to wait for a response from the mail server. Default is 30 seconds. Enter a value between 30 and 120 seconds.	
	(T) Maximum Concurrent Connections	Specify the maximum number of concurrent connections (CPU threads) available to connect to Mail servers and poll Advanced UM e-mail accounts. The default setting is 40 threads. Enter a value between 1 and 200.	
	(R) Mail Server Type	Specify Microsoft Exchange, Office 365, or Google Apps.	
	(T) Adapter type:	Specify the protocol to be used for message exchange (i for IMAP Gateway). The default setting is IMAP.	

Web Console Tab	Parameter	Description	Your Value
	(C) Secure IMAP (True/ False)	Specify "true" to enable a secure IMAP connection to a Microsoft Exchange Server (2016 or 2019). If the Server Type is Google Apps or Office 365, this setting is enabled by default. The connection uses SSL to encrypt the entire communication session, including passwords. The default setting is "false." **Notes**: • SSL requires a digital certificate on the mail server. For ease of setup, use the self-signed certificate provided with Microsoft Exchange. For enhanced security, generate a certificate signing request (CSR) on the mail server and provide it to a certificate authority (CA), which will then issue a third-party certificate. For details on managing SSL on Microsoft Exchange Server 2016 or 2019, see technet.microsoft.com. • To take advantage of Secure IMAP, you must enter the correct authentication settings in the Exchange Server. For details, see IMAP Setup for Exchange.	

Web Console Tab	Parameter	Description	Your Value
	(L) Superuser account name	Specify the IMAP superuser account name. If the Server Type is Google Apps, this setting is not available.	
	(P) Superuser password	Specify the IMAP superuser account password. If the Server Type is Google Apps, this setting is not available.	
	IP Address • (S) for IMAP	• For IMAP, specify the IP address or hostname of the IMAP mail server. This field defaults to "imap.gmail.com" if the Mail Server Type is Google Apps, and "outlook.office365.com" if the Mail Server Type is Office 365. Note that all hostnames, including pre-configured ones, must be resolvable by the corporate DNS server defined in MSL. **Note**: If an IMAP connection is being made to a Client Access Server (CAS), enter the address of the CAS in place of the mail server address. A load balancer or Exchange server can function as a CAS.	

Web Console Tab	Parameter	Description	Your Value
	Port No. / Hosted Exchange	If your implementation has a Microsoft Exchange server in a hosted environment, you can specify a non-default IMAP inbound connector port: 1. Select the **Hosted Exchange** box. 2. Enter a free, unreserved port number up to five digits in length as the **Port No**. 3. Configure the same port number on the MS Exchange server. **Note**: Google and Office 365 must use their default IMAP ports (993 or 143). To configure an IMAP port number in MS Exchange: 1. Access the Exchange server and log in as an administrator. 2. Launch the management shell. 3. Set the port number: • For SSL, enter: Set-ImapSettings -Server "server-name" -SSLBindings: IPaddress:Port • For TLS or no encryption, enter: Set-ImapSettings -Server "server-name" -UnencryptedOrTLSBindings IPaddress:Port	

Web Console Tab	Parameter	Description	Your Value
	(V) Verify Connection	Select to perform connection tests on all defined IP addresses/ hostnames. Note that this Verify function detects only one error at a time.	
LDAP Server	(A) LDAP Server Address	Specify the IP address of the LDAP server (i.e. Active Directory server). LDAP is not available for Google Apps.	
	(D) LDAP Administrator DN []:	An account for Active Directory specified in LDAP DN syntax. **Note**: • This account does not require administrative privileges. • This account is used to perform queries, not updates. As such, it only requires "read" access to the database. It does not require administrative rights with "read/write" access. • Get this value for from the Active Director administrator to ensure syntax compliance.	
	(P) LDAP Login Password []:	Specify the password for the LDAP administrator DN.	

Web Console Tab	Parameter	Description	Your Value
	(B) LDAP Search Base []:	Specify the path to users in Active Directory with Advanced UM mailboxes, in LDAP DN syntax.**Note**: Get this value for from the Active Directory administrator to ensure syntax compliance.	
	(V) Verify Connection	Select to perform connection tests on Active Directory server based on all LDAP parameters. Note that this Verify function detects only one error at a time.	

26.127 Configure IMAP Server Settings for Exchange or Office 365

The use of IMAP protocol and Microsoft Graph API protocol is as follows:

- Use IMAP protocol to connect the Microsoft Exchange and the NuPoint Unified Messaging server.
- Use IMAP protocol to connect the Office 365 email server and the NuPoint Unified Messaging server using basic authentication.
- Use Microsoft Graph API to connect the Office 365 email server and the NuPoint Unified Messaging server using OAuth 2.0 authentication.

Instructions are provided on this page to set up IMAP for:

- MS Exchange Server
- MS Office 365

Note:

- If you need to change your current authentication configuration from "Encrypted" to "Basic authentication" (password sent in clear text), or vice versa, then you must stop and restart the IMAP service for the change to take effect.
- If you need to change your current authentication configuration, then you must stop and restart the IMAP service for the change to take effect.
- For IMAP configurations of Microsoft servers, the Active Directory mail nickname attribute must be the same as the user logon name attribute.
- For Advanced UM with IMAP integration, no superuser account is required; however, NP-UM requires one account in Active Directory to query the Advanced UM user list. It is necessary to query to find each user's email address info and display name to deliver the voice mail to email.
- If your enterprise is using a Microsoft Exchange Server in secure IMAP mode, your Advanced UM users may experience a delay of up to ten minutes between the time they delete their voicemail messages in Outlook and the time the NuPoint database is updated. This occurs because of a known synchronization issue with Exchange Server and is described in the Microsoft technical forums.

Configuration Options

Advanced UM with IMAP can be configured in either of two ways, depending on whether you want users to access their mailboxes individually or using a superuser account:

- **Individual User Access**: With this setup, which is available for all server types, individual users must update their Advanced UM Email Passwords whenever they change their email client passwords. No superuser is required; however, NP-UM requires one account in Microsoft Active Directory.
- **Superuser Access**: With this setup, which is available for Exchange Server, a superuser account (NPUMAdmin) is used to access the individual user accounts and deliver the voice mail to email. This frees users from having to update their Advanced UM Email Passwords when they change their email client passwords.

Note:
If the IMAP service (Microsoft Exchange IMAP4) is already started, then you must restart the service after performing the configuration steps below in order for IMAP to function correctly. To restart the IMAP service, from the Services Console, select **Microsoft Exchange IMAP** and right-click to restart.

IMAP4 Setup for Exchange Server 2016 or 2019

The following procedure provides the basic steps. For additional information, refer to the Microsoft documentation at the links provided.

Note:
If your enterprise is using a Microsoft Exchange Server in a secure IMAP mode, your Advanced UM users may experience a delay of up to ten minutes between the time they delete their voicemail messages in OCP and the time the NuPoint database is updated. This occurs because of a known synchronization issue with Exchange Server and is described in the Microsoft technical forums.

1. Enable IMAP4 service on MS Exchange Server with Exchange Management Shell by entering the following commands:

```
Set-service
msExchangeIMAP4 -startuptype automatic
```

Start-service msExchangeIMAP4

See the following link for more details: http://technet.microsoft.com/en-us/library/bb124489(EXCHG.80).aspx

2. Enable IMAP4 access for a user with Exchange Management Shell:

```
Set-CASMailbox
-Identity CAS01 -ImapEnabled $true
```

Note:
The value "CAS01" in the command line above is only an example. You need to enter a valid exchange account that is specific to your system.

See the following link for more details: http://technet.microsoft.com/en-us/library/bb124783(EXCHG.80).aspx

3. Configure authentication for IMAP4 with Exchange Management Shell by entering *one* of the following commands:

```
Set-ImapSettings
–LoginType SecureLogin
```

(Secure IMAP enabled; encryption occurs before authentication)

```
Set-ImapSettings
```

```
-LoginType PlainTextAuthentication
```

(Secure IMAP enabled; encryption occurs after authentication)

```
Set-ImapSettings
-LoginType PlainTextLogin
```

(Secure IMAP disabled)

See the following link for more details: http://technet.microsoft.com/en-us/library/aa997188(EXCHG.80).aspx

4. Through **Administrative tools > Services**, right-click **Microsoft Exchange IMAP4** and select **Restart** (or "**Start**" if the service is not running.)
5. If you are using a Microsoft Exchange Server 2016/2019, start the IMAP4 service and the IMAP4 Backend service. (These services are disabled by default on Exchange 2016/2019.)
6. Proceed to the next step in the Configuring Advanced UM - Task List (Configure Advanced UM Parameters).

IMAP Setup for Office 365

If your enterprise is employing Microsoft Office 365 as its hosted mail server, you can use to the following summary instructions to configure NuPoint UM and confirm that the connection between the systems is operational.

Configuring the Connection to Office 365

To configure the connection to the Office 365 mail server:

1. From the Web View navigation tree, click **Unified Messaging**, and then click **Advanced UM**.
2. Select the Mail Servers tab and program the following:
3. Select **Office 365** for the **Mail Server Type**.
4. Enter **outlook.office365.com** for the **IP Address**.
5. Select Authentication Type as **OAuth 2.0** or **Basic**.

Note:

When the Authentication mode is selected as OAuth 2.0, the authentication is done with Microsoft Graph API, which is a recommended method. In the case of Basic Authentication mode, the authentication is done with IMAP secure.

6. To check connectivity with the Office 365 server, click the **Verify Mail Server IP Address** button.

Note:
For details concerning the mail server settings, see Configure Advanced UM Parameters.

Configuring Advanced UM Users

To configure an Advanced UM user mailbox:

1. From the navigation tree, click **Mailbox Maintenance**, and then click **Mailboxes**.
2. Search for a specific mailbox or click **Show All** to see a complete list of mailboxes.
3. Click a mailbox link or select a mailbox in the list, and then click **Edit > Selected**.
4. Edit the mailbox parameters as required:
   - Enter the email address (Microsoft) in the **Advanced UM Email Alias** field.
   - Enter the password for the email alias in the **Advanced UM Email Password** field.
5. Click **Save**.

Note:
For details concerning the Advanced UM user mailbox settings, see Enable Advanced UM for User Mailbox.

Configuring Office 365

No special configuration steps are required to support Office 365 IMAP connection to NuPoint UM or Advanced UM user mailboxes. Refer to the Microsoft documentation for more information.

NuPoint Advanced UM IMAP Configuration Settings on Exchange 2016 and Exchange 2019 Servers

The following steps provide basic information on how to configure IMAP settings on Exchange 2016, and 2019 servers for NuPoint Advanced Unified Messaging

Note:
For any assistance with making changes to the Exchange server, the site administrator can contact Microsoft. The administrator is responsible for all configuration changes made to the server.

1. Create the following registry keys in your machine using the following procedure:

   a. Click **Start**, click **Run**, type regedit in the Open box, and then click **OK**. The Registry Editor window opens.
   b. Navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS \ParametersSystem.*
   c. Right-click the **Parameters System**key. A pop-up menu opens.
   d. Point to **New** and choose **Key** from the drop-down menu. A new key value displays as **New Key #1**. Rename it as **Maximum Allowed Sessions Per User** by right-clicking it and choosing **Rename**.
   e. Double-click **Default** on the right pane and enter the value 2048 in the **Value Data** field.
   f. Similarly add another registry key with the name **Maximum Allowed Service Sessions Per User** and value 2048.
2. Create the following DWORDs in the registry key using the following procedure:

   a. Right-click the **Maximum Allowed Sessions Per User** key. A pop-up menu opens.
   b. Point to **New** and choose **DWORD Value** from the drop-down menu. A new DWORD value displays as **NewValue#1**. Rename it as **Maximum Allowed Sessions Per User** by right-clicking it and choosing **Rename**.
   c. Double-click **Maximum Allowed Sessions Per User**. Click the **Hexadecimal** radio button in the **Base** section. Enter the value 2048 in the **Value data** text field and click **OK**.
   d. Similarly add another DWORD with the name **Maximum Allowed Service Sessions Per User** and value 2048.
3. Close the Registry Editor window. Restart the Exchange server or restart the IMAP4 front-end and back-end services.
4. After the server restarts, launch the Exchange Management Shell and run the following command to prevent the Exchange Server from repeatedly prompting for authentication credentials and to restart your IMAP services on the Exchange Server:

Set-IMAPSettings -EnableGSSAPIAndNTLMAuth $false cmdlet

1. Enable IMAP logging and run the following command in the Exchange Management Shell to set the log file size allotment on server as 10MB:

Set-ImapSettings -Server <ServerName> -LogPerFileSizeQuota 10MB

1. Set the Maximum connections from a single user to 200000 from the default value of 16. Also make sure that all other connections are set to the default values. To make these changes, access the Exchange Admin Center (EAC) in the Exchange Server and follow the below mentioned steps:

    a. In the EAC, navigate to **Servers**>**Servers**.
    b. In the list of servers, select the Client Access server, and then click **Edit**.
    c. On the **Server Properties** page, click **IMAP4**.
    d. Scroll down and click **More options**.
    e. Under **Connection limits**, specify the following settings:

        i. **Maximum connections**: Specifies the total number of connections the specified server will accept. This includes authenticated and unauthenticated connections. The default value is 2,147,483,647. The supported values are from 1 through 2,147,483,647.
        ii. **Maximum connections from a single IP address**: Specifies the number of connections that the server will accept from a single IP address. The default value is 2,147,483,647. The supported values are from 1 through 2,147,483,647.
        iii. **Maximum connections from a single user**: Specifies the maximum number of connections that the server will accept from a user. The default value is 16. The supported values are from 1 through 2,147,483,647. Make sure that you set the value to 200000.
        iv. **Maximum command size (bytes)**: Specifies the maximum size of a single command. The default value is 10,240. The supported values are from 1,024 through 16,384.
        v. Click **Apply**, and then click **OK** to save your changes.

You can also set the connection limits by running the following command in the Exchange Management Shell:

Set-ImapSettings -Server "exchange server name" -MaxConnectionsPerUser 200000

After you set the connection limits, restart the IMAP4 front-end and back-end services on the Exchange Server.

1. Configure the Throttling policy for ImapMaxConcurrency, ImapMaxBurst, ImapRechargeRate, ImapCutoffBalance, and CPAMaxConcurrency to Unlimited by running the following command in the Exchange Management Shell:
2. Set-ThrottlingPolicy NPUMAdminPolicy -ImapMaxConcurrency Unlimited -ImapMaxBurst Unlimited -ImapRechargeRate Unlimited -ImapCutoffBalance Unlimited -CPAMaxConcurrency Unlimited

26.128 Configure a Superuser Account for Office 365

If you are using Office 365 as an email server, you can sync Office 365 passwords with Advanced UM as an Office 365 Superuser. Configure a Superuser account to access multiple mailboxes. This eliminates the need to update passwords manually in NuPoint.

Note:

Delegate the Superuser to those users who will be using Advance Unified messaging.

Depending on your Office 365 setup, use one of the following methods listed below:

Setting Up Superuser's Permissions from within Microsoft Exchange Admin Center

1. Log on to the **Microsoft Exchange Admin Center** using the **ECP Domain Administrator** credentials.
2. Click **recipients** > **mailboxes**
3. Select the mailboxes of users you want access to by doubling clicking on the users.
4. Click **Mailbox Delegation.**
5. Provide **Send As** and **Full Permission** to the user, on behalf of the delegator.
6. Click **Save.**

Setting up Superuser's Permissions from within Microsoft Office 365 Admin Center

Send email from another user's mailbox

1. In the admin center, go to the **Users > Active users page**.
2. Select the name of the user (who provides the sending permission) to open their properties pane.
3. On the Mail tab, select **Manage mailbox permissions**.
4. Select **Edit**.
5. Select **Add permissions** and then choose the name of the person to whom you would want to send this email.
6. Select **Save**.

Read and Manage email in another user's mailbox

1. In the admin center, go to the **Users > Active users page**.
2. Select the name of the user (from whom the sending permission should be given) to open their properties pane.
3. On the Mail tab, select **Manage mailbox permissions**.
4. Next to Read and Manage, select **Edit**.
5. Select **Add permissions** and then choose the name of the user or users that you want to allow to read the email from this mailbox.
6. Select **Save**.

Configuring Office 365 Superuser on NuPoint

1. Log in to the **Admin Web Console**.

2. Navigate to **NuPoint Web Console** > **Unified Messaging** > **Advanced UM.**
3. Select Mail Server Type as **Office 365.**
4. Enter the **Superuser account name** and **Password**.
5. Save the credentials.

Note:

Please enable Feature Class of Service (FCOS Bit 295) to only the users that will be using Advance Unified messaging.

26.129 Create a Superuser Account for Microsoft Exchange 2016 or 2019

If you are using a Microsoft Exchange Server as an email server, you can configure a Superuser account to access the individual email accounts. This eliminates the need for users to maintain passwords on the NuPoint UM system. Instead, they are required to create and update passwords in one place only: Microsoft Outlook.

NuPoint UM supports a feature called Client Throttling on MS Exchange. You can use it to give the Superuser enhanced access to server resources.

Creating a Superuser Account

To create the **NPUM Admin** Superuser account on the Active Directory platform with MS Exchange Server:

1. Log in to the Exchange Management Console to create a new user and an Exchange mailbox. You must have the rights to create new users.
2. In the Exchange Management Console, select **Recipient Configuration > Mailbox > New Mailbox > User Mailbox > New User**.
3. In the first New Mailbox window, enter **NPUMAdmin** in the **First Name**, **User logon name (User Principal Name)** and **User logon name (pre-Windows 2000)** fields. Note: The NPUMAdmin name is case sensitive.
4. Enter a password in the **Password** and **Confirm Password** fields, then click **Next**.
5. Enter the mailbox settings for a mailbox on your system, and then click **Next**.
6. When the next window appears, click **Finish**.
7. Ensure that the NPUMAdmin account can be seen on Exchange address lists. (Right-click on the NPUMAdmin user to access Properties. On the General tab, ensure that the **Hide From Exchange address lists** check box is cleared.)

Adding the Superuser Account to Active Directory Groups

To add the Superuser account to Active Directory Groups:

1. Log in to the Active Directory Users and Computers tool.
2. Locate the **NPUM Admin** Superuser account.
3. Add the account as a member of the following group for Exchange:

```
Organization
Management, ExchangeLegacyInterop
```

Setting Up Permissions for the Superuser Account

To set permissions for the Superuser account, on a computer that has Exchange Management Shell installed:

1. Launch Exchange Management Shell. Do not use Windows Powershell.
2. At the MSH prompt, enter the following information on one line:

   Get-OrganizationConfig | Add-AdPermission -user NPUMAdmin -accessRights GenericRead -extendedrights "Read metabase properties","Create named properties in the information store","View information store status","Administer information store","Receive as","Send as"

> **Note**:
> By default these permissions will be applied to all sub-containers. Do not change this setting.

3. Make sure that the **NPUMAdmin** account is a member of **Domain Users** only.

> **Note**:
> To confirm that the account has been set up correctly, repeat step 2. You should receive a message saying "Already Complete."

4. At the MSH prompt, enter the following information to give full access rights to the Superuser account:

```
get-mailbox
-ResultSize Unlimited | add-MailboxPermission -user NPUMAdmin
-accessRights FullAccess
```

Note:

- Entering the above-noted command enables the NPUMAdmin account to have access to all mailboxes currently on the Exchange Server. If new users are added after this command has been run, then the command must be run again to grant full access rights.
- Full Access permissions are not granted until the Microsoft Information Store service caches the permissions and updates the cache, which can take up to two hours. To grant the permissions immediately, stop and then start the Microsoft Exchange Information Store service on the Exchange Server. See http://technet.microsoft.com/en-US/library/aa996343(EXCHG.80).aspx for more details.

Configuring the Client Throttling Policy

You can configure a client throttling policy to give the Superuser enhanced access to the server resources.

Exchange SP1

Note:
In the following procedure, `NPUMAdmin` is the Superuser account name.

To configure the client throttling policy for SP1:

1. Access the Exchange Management Shell.
2. Run the following command to set the RCAMaxConcurrency value to zero, allowing unlimited concurrent connections for the superuser account:

```
new-throttlingpolicy
-name NPUMAdminPolicy -RCAMaxConcurrency Unlimited
```

3. Run the following command to apply the new client throttling policy to the superuser account:

   set-mailbox -identity NPUMAdmin -throttlingpolicy NPUMAdminPolicy

   To confirm that the client throttling policy is set correctly:
4. Access the Exchange Management Shell.
5. Run the following command to show the client throttling policy for the NPUMAdminPolicy Superuser account:

   Get-ThrottlingPolicy -identity NPUMAdminPolicy | Format-List

6. Run the following command to show *all* client throttling policies:

```
Get-ThrottlingPolicy
 | Format-List
```

26.130 Troubleshooting Notes for IMAP for Exchange or Office 365

Advance Unified messaging IMAP Configuration Settings on Exchange 2016 and Exchange 2019 Server

To ensure overall system stability, we engaged Microsoft to make some system modifications that will allow the overall integrated system to properly function.

Please find below the modification that has been advised by Microsoft. Changes to the exchange server configurations is at sites own risk. If the site admin is not comfortable with the changes, then please contact Microsoft.

To see IMAP setting on Exchange

- **Get-ExchangeServer | fl name,serverrole,site,fqdn,admindisplayversion**
- **Get-AcceptedDomain**
- **Get-TransportAgent**
- **Get-DomainController | fl name,dnshostname,adsite**
- **Get-IMAPSettings | FL on both the Servers**
- **Get-ThrottlingPolicy NPUMAdminPolicy | fl**

Maximum Allowed Sessions Per User and Maximum Allowed Service Sessions Per User

Create the following registry key. If there is no existing registry key, create one. If site is not comfortable creating this key in the Exchange registry or any changes to the Exchange server, please call Microsoft for assistance.

Create a Maximum Allowed Sessions Per User registry key with value 2048 under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem

Add 2 new **DWORD** entries:

- Maximum Allowed Sessions Per Userwith value2048(Hexadecimal)
- Maximum Allowed Service Sessions Per Userwith value2048(Hexadecimal)

After creating the registry key, reboot the exchange server or restart IMAP4 services and the front and back-end services.

NTLM authentication protocol authentication

This is applicable to Exchange 2016 and Exchange 2019 Mail and CAS servers.

Perform the following steps for NTLM authentication protocol:

1. Disable the parameter:

   `EnableGSSAPIAndNTLMAuth`
2. Check this KB:*https://support.microsoft.com/en-us/kb/3076376*
3. Run the **Set-IMAPSettings**, where

   `EnableGSSAPIAndNTLMAuth` is set to $false
4. To set the log file's size quota on the server, run the following command:

```
 Set-ImapSettings
-Server <ServerName> -LogPerFileSizeQuota 10MB
```

Set the IMAP4 connection limits for a server

This is applicable to Exchange 2016 and Exchange 2019 latest software load.

NOTE: Set the limit for maximum connections from a single user to 200000 from the default value of 16. Also, make sure that all other connections are set to the default settings. You can make the changes via the Exchange ECP Web console.

1. In the EAC, navigate to **Server > Servers.**
2. From the list of servers, select the **Client Access Server** and then click **Edit.**
3. On the server properties page, click **IMAP4.**
4. Click **More Options.**
5. Under Connection Limit, use the following settings:

   - Maximum connections - Specifies the total number of connections the specified server will accept. This includes authenticated and unauthenticated connections. The default value is 2,147,483,647. The possible values are from 1 through 2,147,483,647.
   - Maximum connections from a single IP address - Specifies the number of connections that the server will accept from a single IP address. The default value is 2,147,483,647. The possible values are from 1 through 2,147,483,647.
   - Maximum connections from a single user - Specifies the maximum number of connections that the server will accept from a particular user. The default value is 16. The possible values are from 1 through 2,147,483,647.
   - Maximum commands size (bytes) - Specifies the maximum size of a single command. The default size is 10,240. The possible values are from 1,024 through 16,384.
6. Click **Apply** and then click **OK** to save your changes.

After you set connection limits, restart the IMAP4 services front-end and back-end on the Exchange server services.

OR

You can make the changes via a command prompt, where you can increase the `MaxConnectionsPerUser` value from 16 (default) to 200000 by running below command:

Set-ImapSettings -Server "exchange server name" -MaxConnectionsPerUser 200000

Configuring the client through Set-Throttling Policy

You can set the Throttling policy to **Unlimited** for the following parameters:

- ImapMaxConcurrency
- ImapMaxBurst
- ImapRechargeRate
- ImapCutoffBalance
- CPAMaxConcurrency

For example:

```
Set-ThrottlingPolicy
NPUMAdminPolicy
```

```
[-ImapMaxConcurrency
<Unlimited>]
```

```
[-ImapMaxBurst
<Unlimited>]
```

```
[-ImapRechargeRate
<Unlimited>]
```

```
[-ImapCutoffBalance
<Unlimited>]
```

[-CPAMaxConcurrency <Unlimited>]

Note:
Changes to the Exchange Server configurations is at the sites own risk. If the site admin is not comfortable with the changes,kindly contact Microsoft.

Troubleshooting and fixes for one or more Exchange servers when they are of different software version (Exchange 2016 forwarding to multiple Exchange Servers)

Exchange IMAP log errors:

- Checked IMAP protocol logs on Exchange server for this ERROR:
- 993:SSL""; ErrMsg=ProxyNotAuthenticated ",

  Example:
  22T12:06:14.459Z,00000000002422BF,3,172.1.0.16:993,192.168.12.15:49088,npumadmin2,61,57,23,login,com/NPUMAdmin2/oozuna *****,"R=""MSB1 NO LOGIN failed."";Msg=""User:LegacyDn: /o=Kat,ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Olga Ozuna, RecipientType: UserMailbox, RecipientTypeDetails: UserMailbox, Selected Mailbox: Display Name: Sally Ozuna, Mailbox Guid: 4ec4d3b2-1719-4f75-93dc-78737a68fc78, Database: 1d149126-97d1-4a8f-ab95-ed0522a1f9d0, Location: ServerFqdn: FW-EXCH01.Mitel.com, ServerVersion: 1937997947, DatabaseName: Mitel FW New, HomePublicFolderDatabaseGuid: be5fc5e4-4151-4446-a88c-932d59f5f7d0;Proxy:FW-EXCH01.Kat.com:993:SSL"";ErrMsg=ProxyNotAuthenticated",

- Check System and Application Event Viewer logs on the Exchange Servers

  Log Name: System

  Source: Schannel

  Date: 2/22/2019 2:38:41 PM

  Event ID: 36888

  Task Category: None

  Level: Error

  Keywords:

  User: SYSTEM

  Computer: FW-EXCH01.Kat.com

  Description:

  The following fatal alert was generated: 51. The internal error state is 900.

  Event Xml:

  <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">

  <System>

  <Provider Name="Schannel" Guid="{1F678132-5938-4686-9FDC-C8FF68F15C85}" />

  <EventID>36888</EventID>

  <Version>0</Version>

  <Level>2</Level>

  <Task>0</Task>

  <Opcode>0</Opcode>

  <Keywords>0x8000000000000000</Keywords>

  <TimeCreated SystemTime="2019-02-22T20:38:41.809566900Z" />

  <EventRecordID>1204930</EventRecordID>

  <Correlation />

<Execution ProcessID="524" ThreadID="632" />

<Channel>System</Channel>

<Computer>FW-EXCH01.Kat.com</Computer>

<Security UserID="S-1-5-18" />

</System>

<EventData>

<Data Name="AlertDesc">51</Data>

<Data Name="ErrorState">900</Data>

</EventData>

</Event>

Log Name: Application

Source: MSExchangeIMAP4

Date: 2/22/2019 3:36:23 PM

Event ID: 1102

Task Category: (1)

Level: Error

Keywords: Classic

User: N/A

Computer: FW-EXCH01.Kat.com

Description:

The IMAP4 service failed to connect using SSL or TLS encryption. No valid certificate is configured to respond to SSL/TLS connections. Check the configured host name as well as which certificates are installed in the Personal Certificates store of the computer.

Event Xml:

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">

<System>

<Provider Name="MSExchangeIMAP4" />

<EventID Qualifiers="49156">1102</EventID>

<Level>2</Level>

<Task>1</Task>

<Keywords>0x80000000000000</Keywords>

<TimeCreated SystemTime="2019-02-22T21:36:23.000000000Z" />

<EventRecordID>4290878</EventRecordID>

<Channel>Application</Channel>

<Computer>FW-EXCH01.Kat.com</Computer>

<Security />

</System>

<EventData>

</EventData>

</Event>

Examples of issues and solutions:

1. **Issue Scenario: Voice messages are not getting delivered for recipients on Exchange servers**

   Solution:

   - Run the

     ```
     Set-ImapSettings
     ```

```
cmdlet
```

to modify the settings of the Microsoft Exchange IMAP4 service on Exchange servers.

- Add CertificateName to the X509CertificateName parameter which specifies the certificate that's used for encrypting IMAP4 client connections.
- Disabled NTLM for IMAP4 connections for `EnableGSSAPIAndNTLMAuth`parameter which specifies whether connections can use Integrated Windows authentication (NTLM) using the Generic Security Services application programming interface (GSSAPI)

If third party certificate, you may need to run the Enable-ExchangeCertificate cmdlet to enable an existing third-party certificate on the Exchange server for IMAP service.

2. Issue Scenario:

   - Voice message were not getting delivered for users on Exchange
   - IMAP SSL is not working, gives the error - "BYE connection is closed. 14"

   Solution: Resolved by adding hostname to the X509CertificateName parameter which specifies the certificate that's used for encrypting IMAP4 client connections.

Mail flow and the transport pipeline in Exchange 2016/2019

In Exchange Server 2016/2019, mail flow occurs through the transport pipeline. The transport pipeline is a collection of services, connections, components, and queues that work together to route all messages to the categorizer in the Transport service on an Exchange 2016/2019 Mailbox server inside the organization.

Understanding the transport pipeline

The transport pipeline consists of the following services:

1. **Front End Transport service:**This service acts as a stateless proxy for all inbound and (optionally) outbound external SMTP traffic for the Exchange 2016 organization. The Front End Transport service does not inspect message content, or communicate with the Mailbox Transport service, and does not queue any messages locally.

   Front End Transport will attempt to anchor on a recipient and will look-up that recipient in Active Directory and find a DAG to which the recipient belongs to.

   It will also attempt to route mail to a mailbox server in that DAG (preferably in the same site).

2. **Transport service: The Transport service on a mailbox server includes the following components and processes:**

   - **SMTP Receive**

     Whenever messages are received by the transport service, message content inspection is conducted, transport rules are applied, and anti-spam and anti-malware inspection is conducted if they are enabled.

     The SMTP session has a sequence and series of events that work together in a particular order to verify and validate the contents of a message before it’s accepted. When a message has passed

absolutely through SMTP Receive and isn't rejected by receive events, or via an anti-spam or anti-malware agent, it is directed over the Submission queue.

- **Submission queue**

  Holds messages that have been accepted by the transport service, but are not processed. Messages in the Submission queue are either waiting to be processed, or are actively being processed.

  On Mailbox servers, messages are received by a Receive connector, the Pickup or Replay directories, or the Mailbox Transport Submission service. On Edge Transport servers, messages are typically received by a Receive connector, but the Pickup and Replay directories are also available.

  Every Mailbox server or Edge Transport server has only one Submission queue.

- **Categorizer**

  The categorizer chooses one message at a time from the Submission queue.

  The categorizer performs the following steps:

  - Recipient resolution that includes top-level addressing,
  - Message bifurcation, and distribution group expansion.
  - Routing resolution.
  - Content conversion.

Moreover, mail flow rules which the organization defined are applied. After messages have been segregated, they're routed into a delivery queue which is based on the destination of the message. Messages are lined up and queued by the destination mailbox database, Active Directory site, DAG, Active Directory forest.

3. **Mailbox Transport Submission service**: This service connects to the local mailbox database using an Exchange remote procedure call (RPC) to retrieve messages. The service submits the messages over SMTP to the Transport service on the local Mailbox server or on other Mailbox servers. The Mailbox Transport Submission service has access to the same routing topology information as the Transport service.
4. **Mailbox Transport Delivery service** : This service receives SMTP messages from the Transport service on the local Mailbox server or on other Mailbox servers and connects to the local mailbox database using RPC to deliver the messages. The Mailbox Transport service doesn't communicate with the Front End Transport service, the Mailbox Transport service, or mailbox databases on other Mailbox servers. It also doesn't queue any m

Ports used for mail flow in Exchange 2016

- **Port 25 – This port just like in previous versions of Exchange is used for SMTP. Used by both External SMTP into the Front End Transport Service (FET), between MBX servers, and also from the FET to the Transport Service. There is a receive connector named Default Frontend <servername> that listens on this port.**
- **Port 587 – This port just like previous versions of Exchange is used for Client Connections (POP \IMAP). The CAS Server has a receive connection listening on this port name Client Frontend <servername>.**
- **Port 717 – Used for outbound proxy connections from the Transport service to the FET Service. When you create a Send connection you have the option to send mail destined for the Internet directly from the Transport Service to the Internet\Smart Host or relay that mail through the**

Front End Transport Service. There is a receive connector named Outbound Proxy Frontend <servername> that listens on this port.

- Port 465 – Used to accept proxies connections that were received on port 587 by the FET service for client connections. There is a receive connector named Client Proxy <servername> that listens on this port.
- Port 475 – The Mailbox Transport Delivery Service listens on this ports for connections either from the transport service SMTP Send connector or SMTP from the Transport Service on other Mailbox Servers that need to send mail to users on this server.
- **Port 2525 – if the CAS and MBX servers are collocated on the same server the SMTP Receive connection for the Transport service will listen on 2525 instead of 25. This is because two services (FET and Transport Service) can't listen on the same port.**

26.131 Configure IMAP Server Settings for Google Apps

You can use the IMAP4 protocol to connect the Google Apps for Business email server and the NuPoint UM server. A maximum of 2500 Advanced UM users are supported with this implementation.

To set up IMAP for Google Apps, do the following:

- Enable IMAP Access for Google_Apps
- Configure OAuth for Google_Apps

Note:

- Messages marked as "urgent" will be delivered as regular messages in Google Mail.
- In most cases, voice mail messages are sent immediately to the email server and then forwarded to the Advanced UM users. However, hosted email configurations such as Google Apps may experience slight delays due to virus scanning, anti-spam software, or routing delays caused by traffic volume. As a result, the timestamps of the original voice mail message and email audio attachment may not match.

Enable IMAP Access for Google Apps

You must enable global IMAP access for all users in the Google Apps domain to facilitate the synchronization of voice mail and email messages.

To enable global IMAP access:

1. Log in to the Google Apps administrator control panel: https://www.google.com/a/cpanel/yourdomainname
2. Enter the domain administrator **Email** and **password**.
3. Click the **Settings** tab and select **Email**.

4. Clear the **Disable POP and IMAP access for all users in the domain** check box.

   IMAP access is enabled for all users in the domain, irrespective of their individual account settings.

Configure OAuth for Google Apps

You must configure the OAuth (Open Authentication) 2.0 settings for service accounts. With this type of server-to-server interaction, the Mitel application has to prove its own identity to the Google API but end users do not need to be involved. This enables NuPoint UM to synchronize voice mails and email with Google Apps such as Google Calendar and eliminates the need for users to maintain email passwords on the NuPoint UM system.

Configuring OAuth is a multi-step process. First, you must log into the Google Apps console and create a new API project. Then you must select a service for the project, create a service account with client ID, and download your credentials (private key and JSON file). Finally, you must log in to MSL and upload your credentials to the server.

Note:

- If the system time is inaccurate, NuPoint UM will be unable to access user email accounts using OAuth. To ensure that your system time is correct, log in to the MSL Server Manager, click **Date and Time** under **Configuration**, and then select the **Enable Network Time Server** option. Disabling this option and using the host's real time clock for the system time is not recommended.
- Support for OAuth 1.0 has been deprecated with the release of MSL 10.1. If you are currently using OAuth 1.0 and upgrade to MSL 10.1 or later software, you should reprogram API access for your application using an OAuth 2.0 Service Account. After you have done this, the OAuth 1.0 tab will be removed from the MSL server manager interface.

Create an API Project and Client ID in Google

Note:
The following instructions are provided as a guide only. For up-to-date instructions, refer to the following resources:

- Google online help available at https://developers.google.com/console/help/
- Mitel Knowledge Base article 15-5138-00053 available at http://www.mitel.com/mol

Log In to the Google API Console

1. Open a web browser and navigate to https://code.google.com/apis/console.
2. Enter the domain administrator **Email** and **password** to log in.

Create the Project

1. Click the **Create project** button.
2. Enter the **Project name** (for example, "NuPoint Advanced UM") and click **Create**. Remain in the project.

Enable Google APIs for the project

1. Open the side menu and select **API Manager**.
2. Select a Google API such as "Calendar API" and click **Enable API**.
3. Repeat for all Google APIs you want to support. Remain in the project.

Create the Service Account with Client ID

1. Open the side menu and select **Permissions**.
2. Under the **Service accounts** tab, select **Create service account**.
3. Enter a **Name**, select **Furnish a new private key** and **JSON** as the file type, and then select **Enable Google Apps Domain-wide Delegation**. Set a **Product name** if prompted.
4. Click **Create** and **Close**. The service account is created and the file containing the Private Key and Client ID is downloaded.

> **Note**:
> Store the file in a safe location. You will require it to establish your credentials to MSL.

5. For the service account you just created, click **View Client ID**.
6. Copy the Client ID and click **Cancel**. You will require the Client ID in the next procedure.

Manage API Client Access (API Scopes)

Once a service account is created, you must enable the scope of access for your client ID.

1. Access the Google Admin console:
   a. Open a web browser and navigate to admin.google.com.
   b. Enter the domain administrator **Email** and **password** to log in.
2. Click **Security**.
3. Click **Show more** and then click **Advanced settings**.
4. Under **Authentication**, click **Manage API Client access**.

5. On the Manage API client access panel:

   a. Paste the client ID in the **Client Name** box.
   b. Enter the following in the **One or More API Scopes** box:

      To support Gmail integration (for NuPoint Advanced UM), enter: https://mail.google.com/
   c. Click **Authorize**.

The client ID now has access to resources in the specified domains.

Upload Credentials to MSL

This procedure involves uploading your OAuth 2.0 credentials (service account Client ID and Private Key) from your computer to MSL. MiCollab employs these credentials to integrate with publicly available Google Apps.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Google Apps**.
3. Select the **Service Account** tab.
4. Under **Configuration**, choose the following files from your computer:

   - Service Account ID (.json file)
   - Private Key (.p12 file)

> **Note**:
> The **Private Key (.p12 file)** file is required only for earlier implementations.

5. Click **Upload Credentials**.
6. Confirm that the Client ID, Email address, and Private Key are correct by comparing them to the corresponding fields in the Google API project.

It is now possible to configure a secure connection to publicly-available Google Apps using the OAuth 2.0 protocol for the Service Account client ID.

Note:

- You can generate another private-public key pair and then upload the private key to the Service Account in MSL.
- OAauth 2.0 data is not included in system (MSL) backups. Accordingly, if you perform a backup and restore procedure, you must then re-enter the OAuth 2.0 data in order to restore the Google Apps integration.

26.132 Configure Advanced UM Parameters

Advanced UM can also be configured from the Text console; however, it is not possible to configure Advanced UM from both consoles simultaneously.

Ensure that you have filled out the Advanced Parameters worksheet before you begin configuration.

Configuration

To configure Advanced UM Parameters:

1. From the navigation tree, under **Unified Messaging**, click **Advanced UM**.
2. The Advanced UM Configuration screen appears.
3. On the **NuPoint** tab, enter the following information from your worksheet:

- Administrator Login
- Administrator Password
- Mailbox Poll Interval (in minutes or hours)
- Permanent Delete (True or False)
- Sender Domain

Note:
If the Administrator Password is changed, you must update this field to show the new password.

4. On the **Mail Servers** tab, enter the following information from your worksheet:

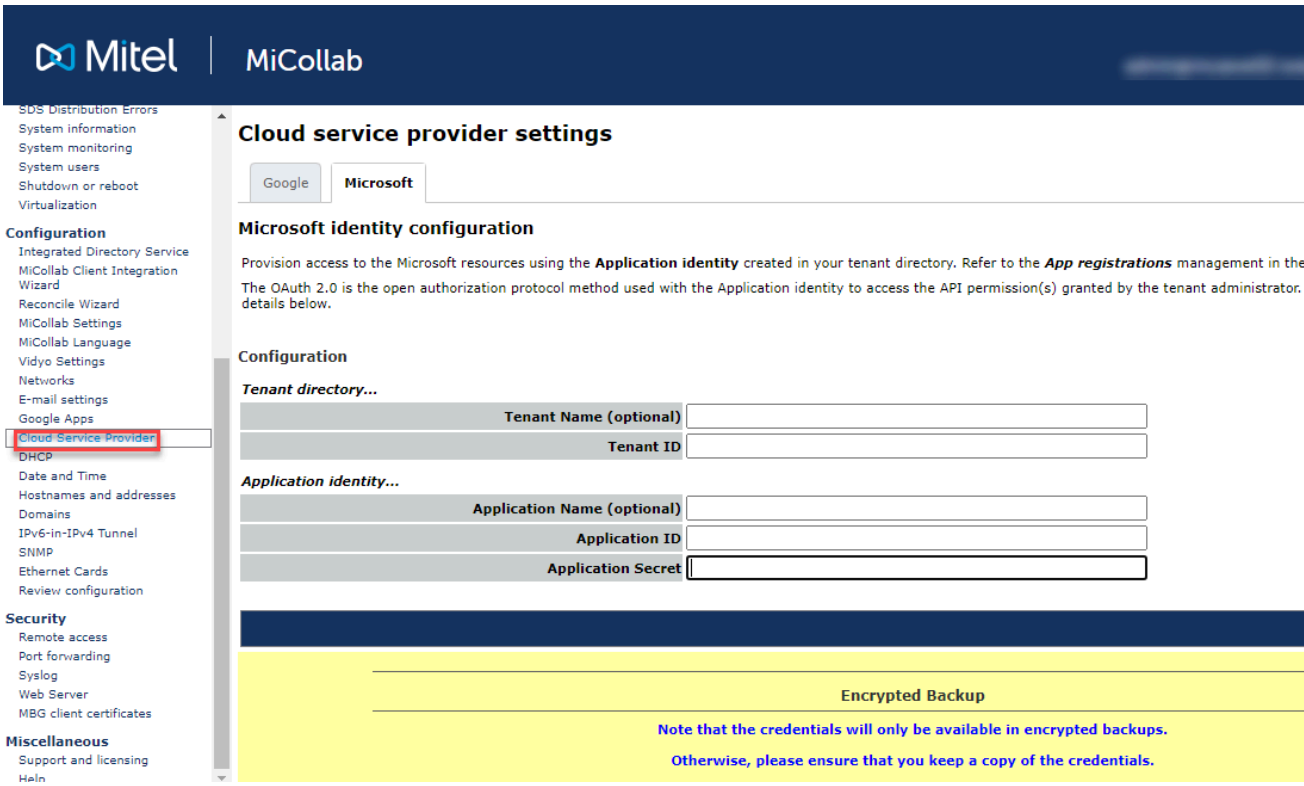
- Mail Connection Properties:
  - Unread Mail Poll Interval
  - Read Mail Poll Interval
  - Mail Server Timeout
  - Maximum Concurrent Connections
- Mail Server Connections:
  - Mail Server Type - Microsoft Exchange, Google Apps, Office 365
  - Adapter Type - This field defaults to "IMAP" if the Mail Server Type is Google Apps, or Office 365
  - Secure IMAP - True or False
  - Authentication Mode
    - Select Auth 2.0 - Authentication will be done with Microsoft Graph API (Recommended)
    - Select Basic - Authentication will be done with IMAP Secure

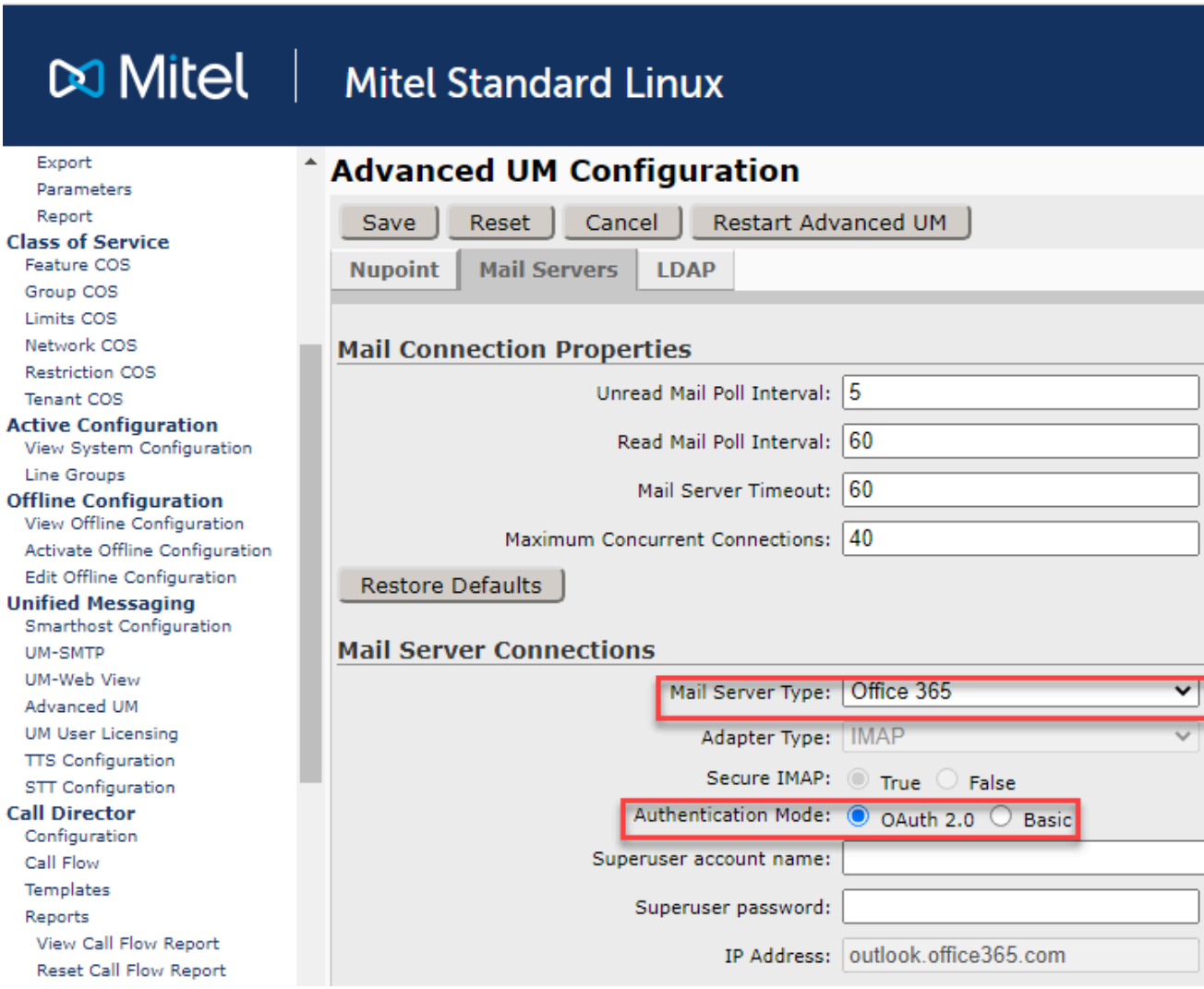
Note:

1)

To enable the Authentication Mode as OAuth 2.0 for Office 365 for NPM Advanced UM feature, the pre-requisites are as follows:

- In Microsoft Entra, the below permissions need to be added to the application for secure OAuth 2.0 to work for Office 365 with Microsoft Graph:
  - Mail.Read
  - Mail.ReadWrite
  - Mail.Send
- Configuration is needed at Cloud Service Provider in MSL. See the Configure Microsoft Identity section for details. See the below screenshots for reference





For detailed steps on how to register an application at Office 365, see Steps to register your application at Microsoft Office 365.

The Cloud Service Provider configuration is required at MSL followed by configuration at NPM Advance UM. For details on configuration at MSL, refer to the Microsoft Cloud section. Once the configuration of OAuth 2.0 is successful at MSL, the administrator has to select Authentication Mode OAuth 2.0

Note:
2)

NPM can receive voice messages from:

a. External callers
b. Internal callers

The internal callers can be categorized into:

i. User having mailbox configured and with valid O365 domain
ii. User with no mailbox configured
iii. User having mailbox configured and invalid O365 domain
iv. User having mailbox configured but no email configured

For Users having mailbox configured and with valid O365 domain, in advanced UM emails:

- The **To** field will show the recipient's Email Id and the **From** field will show the sender's Email Id.
- Sender information will also be present in the subject line and Email body.

For a, b(ii), b(iii) and b(iv), in advanced UM emails:

- The **To** and **From** fields in the Email will show the recipient's Email Id. This is because the Graph API does not support the send operations for the invalid O365 domain.
- Sender information will be present in the Subject line and in the Email body.

- Superuser account name - IMAP superuser account name.
- Superuser password - IMAP superuser password.
- Port No. / Hosted Exchange - If your implementation has a Microsoft Exchange server in a hosted environment, you can use these fields to specify a non-default IMAP inbound connector port up to five digits in length. This port number must also be configured on the Exchange server. For configuration details, see the Advanced Parameters Worksheet.
- IP Address - This field defaults to "imap.gmail.com" if the Mail Server Type is Google Apps and "outlook.office365.com" if the Mail Server Type is Office 365. Hostnames must be resolvable by the corporate DNS server defined in MSL. If a connection is being made to a Client Access Server (CAS), enter the address of the CAS in place of the mail server address. Note that either a load balancer or an Exchange server can function as a CAS.

Note:

To take advantage of Secure IMAP, you must enter the correct authentication settings in the Exchange Server. For details, see IMAP Setup for Exchange Server.

5. On the **LDAP** tab, enter the following information from your worksheet:

   - LDAP Server Address
   - LDAP Administrator DN
   - LDAP Login Password
   - LDAP Search Base

Note:

- LDAP is not available for Google Apps.
- LDAP DN syntax refers to the creation of a Distinguished Name, which is a series of name components forming a unique identifier, similar to a path to a file. The abbreviations **cn** and **dc** refer to Common Name and Domain Component, respectively. For more information about LDAP, refer to the Microsoft TechNet Library at **http://technet.microsoft.com/en-us/library/**.
- This account is used to perform queries, not updates. As such, it only requires "read" access to the database. It does not require administrative rights with "read/write" access.

6. On the Mail Servers or LDAP tab, click **Verify Connection** to test your configuration settings.

Note:
The Verify Connection function detects only one error at a time.

7. Click **Save**. The system validates your input and, when all parameters are validated successfully, a confirmation box appears indicating that the Advanced UM server must be restarted for your changes to be applied.
8. Click **OK**.

Note:
Restarting the Advanced UM server may cause an interruption to Advanced UM service. Voice mail ports are not affected.

Advanced UM Form Button Actions

Button	Action
Save	Saves the configuration.
Reset	Resets all fields on the screen to their default values.
Cancel	Exits the screen without making any changes.
Restart Advanced UM	Restarts the Advanced UM service while all other NuPoint UM services remains running.

26.133 Configure Text to Speech

Note:
This feature is applicable for releases prior to R9.1.

To configure Text-to-Speech:

1. From the navigation tree, click **Unified Messaging** and then click **TTS Configuration**.
2. The Text-to-Speech Configuration screen appears.
3. On the **Configuration** tab, enter the following information:

- **TTS rate of speech:** Select a value between 1 and 9 (1 being a very slow rate of speech and 9 being a very fast rate of speech. Default is 5.)
- **TTS volume:** Select a value between 1 and 9 (1 being low volume and 9 being high volume. Default is 5.)

4. On the **Dictionary** tab, enter the following information:

   - **Dictionary language:** Select a specific language from the drop-down menu.
   - **Note**: The supported languages are NA English and UK English.
   - **Word:** Click Add and type the word you want to define.
   - **Pronunciation:** Type the phonetic pronunciation for the word. (For example, for the name "Mitel", you might type "Mytell".

Note:
You can also edit and delete the pronunciation information using the **Edit** and **Delete** buttons.

26.134 Configure Advanced UM Parameters

Advanced UM Parameters consist of settings for the NuPoint server, the mail server, and the LDAP server.

You can configure Advanced UM parameters from the Text Console (instructions below) or from the Web Console (see the Web Console online help). If you want to switch from the Text Console to the Web Console at any point in the configuration process, you must exit the Advanced UM menu and save your changes in the Text Console before logging in to the Web Console.

Note:

- Before starting the configuration, ensure that you have completed the Advanced UM Parameters worksheet for reference.
- You can include a **Corporate Callback Number** in your notification emails. See Configuring Standard UM.

To configure Advanced UM parameters:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**.
2. In the Unified Messaging menu, select **(A) Advanced UM**.
3. In the Advanced UM menu, select **(N) NPM Parameters**.
4. Configure the following parameters using your worksheet as a reference:

   - **(L)** Administrator Login
   - **(P)** Administrator Password
   - **(I)** Mailbox Poll Interval
   - **(K)** Permanent Delete
   - **(V)** Sender Domain

5. Exit **(X)** to the Advanced UM menu: COMMAND (N/E/L/U/T/Q/X)
6. In the Advanced UM menu, select **(E) Mail server parameters**.
7. Select **(S) Mail Server Connections**.
8. Select **(R) Server Type** and enter **E** for Microsoft Exchange or **G** for Google Apps.
9. Select **(T) Adapter Type** and then do the following

   - For **IMAP**, type **I** and then select **(S) IP Address/Hostname**. Enter the IP address or hostname of the IMAP server. If the Server Type is Google Apps, this field defaults to "imap.gmail.com."
10. Select **(C) Secure IMAP** and then select "true."

> **Note**:
> To take advantage of Secure IMAP, you must enter the correct authentication settings in the Exchange Server. For details, see IMAP Setup for Exchange Server.

11. Select **(P) Port Number** and enter a free, unreserved port the non-default IMAP inbound connector port to be used by Microsoft Exchange in a hosted environment. This port number must also be entered on the Exchange server and Outlook.
12. Select **(V) Verify connection** to perform connection tests on all defined IP addresses.
13. Exit **(X)** to the Mail Server Parameters Menu (COMMAND (S/U/R/E/T/D/X):)
14. Configure the following parameters using your worksheet as a reference:

    - **(U)** Unread Mail Poll Interval (seconds) [5]
    - **(R)** Read Mail Poll Interval (seconds) [60]
    - **(E)** Mail Server Timeout (seconds) [120]
    - **(T)** Maximum Concurrent Connections [100]
    - **(D)** Restore Defaults (Select this option to return all settings to their default values.)
15. Exit **(X)** to the Advanced UM Menu: COMMAND (N/E/L/U/T/Q/X).
16. In the Advanced UM Menu, select **(L) LDAP Parameters** (LDAP is not available for Google Apps).
17. Configure the following parameters using your worksheet as a reference:

    - **(A)** LDAP server address []:
    - **(D)** LDAP Administrator DN []:
    - **(P)** LDAP login password []:
    - **(B)** LDAP search base []:
18. Select **(V) Verify connection** to perform connection tests on Active Directory server based on all LDAP parameters. (This Verify function detects only one error at a time.)
19. Exit **(X)** to the Advanced UM menu: COMMAND (N/E/L/U/T/Q/X).
20. Select **(X)** Exit -- Save Changes and enter **Y** to restart Advanced UM.

26.135 Configure Text to Speech

To configure Text-to-Speech:

1. From the Main menu, select **(S) System Maintenance**, **(R) Reconfigure System**, **(U) Unified Messaging**, and then **(A) Advanced UM**.
2. Select **(T) Text to Speech parameters**.
3. Select **(R) TTS rate of speech** and then enter a value between 1 and 9 (1 being a very slow rate of speech and 9 being a very fast rate of speech).
4. Select **(V) TTS volume** and then enter a value between 1 and 9 (1 being low volume and 9 being high volume).
5. (Optional) Select **(F) Implicit Email Count Timeout** and enter the number of seconds to wait for the system to present the summary of voice mail and email messages before skipping the summary and prompting instead to "Press 3 for email or press 8 for voice mail". (Default is 5.)
6. (Optional) Select **(S) Explicit Email Count Timeout** and enter the number of seconds to wait for the system to access email (after the user has pressed "3" for email) before responding with a "system is busy - please try again later" message and initializing the mailbox. (Default is 15.)

Note:
User Dictionary configuration is only available through the **Web Console**.

26.136 Force Manual License Update

To force a license update:

1. From the Main Menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(U) Unified Messaging**, and then **(A) Advanced UM**.
2. Select **(U) User Licensing**.
3. Select **(U) Update User Licenses**. You are prompted to confirm.
4. Enter **Y**.

Note:
For MiCollab deployments, you cannot force a license update by selecting the **Update User Licenses** option. Instead, you must access the MiCollab Users and Services application and enable **Advanced Unified Messaging**.

26.137 Enable Advanced UM for User Mailbox

When all system-level configuration is complete, the users' mailboxes must be enabled for Advanced UM.

Note:

- Each user must have a unique Advanced UM Email Alias / Full Name / Address (i.e. the ID must not be used in any other NuPoint mailbox). Duplication of IDs causes NuPoint to attempt to synchronize two voice mailboxes to one e-mail account, resulting in the deletion of all voice messages.
- If the Advanced UM service stops working, an e-mail is sent automatically to the System Administrator.

To Enable Advanced UM for a User Mailbox:

1. Customize an FCOS for UM users and add the following feature bits for each type of user:

For this feature:	Add these Feature Bits:
Advanced UM	295
Text-to-Speech	296

2. Assign the customized FCOS to the user's mailbox.
3. Force a manual license update for Advanced UM.
4. Modify the user's mailbox as follows:

- Enter the email alias (Microsoft) or address (Google) into the **Advanced UM Email Alias / Advanced UM Full Name / Advanced UM Email Address** field.
- Enter the password for the email alias into the **Advanced UM Email Password** field. (See notes below for password requirements.)

Note:

- If the password is changed in the email client, it must also be changed in the user's mailbox. If the password is not updated, messages will be rejected.
- The email alias appears in the **General** tab of the **User Properties** in Microsoft Exchange.
- Updating UM User Licensing causes a scan of mailboxes that may take some time to complete and may place an extra load on the system.

- Password Requirements:

— For IMAP, the password must be the user's actual password. The Exchange server must support cleartext passwords. If passwords are changed regularly, mailbox programming must be updated to match.

5. If the user will be using the Speech to Text feature, select the **Enable Speech-to-Text Transcription** check box. Enabling this feature causes all incoming voice mails (except Confidential, Record-a-Call, and Fax messages) to be automatically transcribed to text and sent as email messages to the user's account. The status of these transcription emails is not synchronized, and does not affect the status of the original voice mail or MWI.
6. Enable web access to voice mail in the user's e-mail client. Refer to the *Web View User Help* for specific user configuration instructions.

26.138 Troubleshooting Standard UM

SMTP-forwarded voice mail fails to reach the e-mail server destination

There are many cases where SMTP forwarding could fail:

1. Invalid address (not reaching an e-mail server)
2. SMTP server temporarily unavailable (e-mail server down)
3. Invalid user (user not valid in e-mail server)
4. Account is full.

Cases 1 and 2 are very similar from the point of view of the SMTP client. The message will not be able to reach an SMTP server.

In cases 3 and 4, the forwarded messages will be delivered to the SMTP server, but the message may bounce back in the form of a reject message. NuPoint Unified Messaging will not attempt to parse those reject messages or to inform the administrator about the failure.

At all times, NuPoint Unified Messaging will keep the messages to be SMTP-forwarded in an SMTP queue. NuPoint Unified Messaging will only remove the messages from that queue when the message is finally delivered to an SMTP server, when the end user removes the message from his/her inbox, or when the age limit timer for the message has been reached.

The amount of retries and time between the retries that the NuPoint Unified Messaging system will attempt to deliver the message to the SMTP server will be configured on a sendmail.cfg file and will not be presented in the menus. When changing the parameters registered in this configuration file, a reboot will be needed for the changes to take place.

26.138.1 Before You Call Mitel Product Support

Please provide the following information/perform the following tasks BEFORE calling Mitel Product Support. Use the link at the bottom of the page to print this task list:

Task	Site
Confirm the system is licensed for sufficient Advanced UM users.	Yes / No
Determine the NuPoint UM software version and platform (for example, NuPoint 14.0.1.7 on MiCollab server).	NuPoint Version: Platform:
Determine Active Directory version	Version #:
Is Active Directory housed on the Exchange server?	Yes / No
Are there multiple Exchange servers?	Yes / No
How many mail stores are configured on the Exchange server?	
Is the site using IMAP Gateway?	IMAP Gateway
Are all servers within the same network?	Yes / No
List the IP addresses of all servers	
Provide the SuperUser account, password, and base path: (for example, *CN=NPMAdmin,CN=Users,DC=mitel,DC=com*)	account: password: base path:
Provide the User search base: (for example, *DC=mitel,DC=com*)	user search base:

Task	Site
Be prepared to provide remote access to the NuPoint UM server, the Exchange server. If you need to contact IT to arrange remote access, please do so before you call Mitel Product Support.	
Test the system to ensure that TCP/UDP port 143 is open. • To test the connection with Exchange when using IMAP, run the Telnet tests from the NuPoint UM server to the Exchange server IP address: for example, `telnet 192.168.10.10 143`	

26.138.2 Troubleshooting Advanced UM

Advanced UM log files can be found here: **/usr/vm/log/msblog.txt**.

Outlook Client Plug-in Issues

The **Trusted Code** tab does not appear in the **Outlook Security Settings** form.

If the security settings form contains only the **Outlook Security Settings** tab and the **Programmatic Settings** tab, it means that an early version of the form (earlier than Outlook 2002) is being used. When you publish the **OutlookSecurity.oft** form, make sure that any existing security form is overwritten. At this point, it is a good idea to delete the **Outlook Security Settings** folder on the Exchange Server and recreate by following the steps described in Install Outlook Administrator Security Package and Configure Security Settings for Outlook.

There may also be complications if more than one version of the form exist together in the public folder. For example, determining which version of the form Outlook Client uses can become complicated. Additional details can be found at: http://office.microsoft.com/en-au/assistance/HA011402931033.aspx.

Unable to save changes to the **Outlook Security Settings** form.

The Mail Profile being used when modifying the **Outlook Security Settings** form through Outlook must connect to Microsoft Exchange through a user having Write permissions on the **Outlook Security Settings** folder. Check the permissions on the folder and the user the Mail Profile is using when connecting to Exchange. Also ensure that the user profile being used is in online mode.

Exchange server and NuPoint Unified Messaging server not synchronized (LDAP or IMAP services timeout)

Synchronization between the Exchange server and the NuPoint Unified Messaging server may be affected if the Exchange server has been restarted or put into maintenance mode, especially if after a prolonged outage. If synchronization is not recovered and there is an LDAP or IMAP services timeout on the NuPoint Unified Messaging server, you must restart the NuPoint Unified Messaging server.

Deleted voice messages are re-delivered

Sometimes, the synchronization between the Exchange server and the NuPoint server is temporarily lost is temporarily lost; for example, due to a system time-out or a restart of the NuPoint UM system. If a user deletes a voice mail while the synchronization is out, that email may be re-delivered when the connection is restored.

Delay in the delivery of voice messages to a user's mailbox

If a user’s mailbox is full or of limited size, there is a delay in the delivery of voice messages. An ideal mailbox size can alleviate this issue. For an ideal mailbox size, specify the following configuration while setting up a user’s mailbox:

- Maximum Connections per User – set the value to 200000
- Maximum Allowed Sessions per User – set the value to 2048
- Maximum Allowed Service Sessions per User – set the value to 2048

These are the settings recommended by Microsoft for Exchange Servers that use IMAP.

Note:

1. These settings do not affect CPU and memory usage.
2. These settings can be applied on Exchange 2016 and 2019.

NuPoint voice messages deleted prematurely

Client applications that change the MessageClass property of NuPoint voice mails in Outlook are not supported.

NuPoint UM voice mails in Outlook have a MessageClass property of "IPM.Note.Multimedia". Client applications (such as the Mitel Messaging Server) that change the message class can make NuPoint UM delete voice messages prematurely when attempting to synchronize with Outlook.

Voice mail synchronization failure due to message exceeding the 3-MB limit

If you attempt to send a voicemail of size exceeding 3 MB, you may encounter a warning in Outlook indicating that voicemail synchronization has failed. This occurs when the message size exceeds the

maximum supported length by the Office365 OAuth 2.0 system. The allowed durationmaximum duration for an MP3 file is 6 minutes, which corresponds to a size of 3 MB.

Microsoft Exchange - On-Premise In-House system

- For On-Premises In-House Microsoft Exchange IMAP system, the maximum message duration is 15 minutes (or size 7 MB) for an MP3 file.
- For On-Premises In-House Microsoft Exchange SMTP system, the maximum message duration is 60 minutes (or size 30 MB) for an MP3 file.

The default limit of 15 MB cannot be altered through the user interface. It can be modified from the command- line interface. To increase the maximum message length, use the following command:

```
config setprop qmail MaxMessageSize 100000000
signal-event email-update
```

Note:
This will adjust the limit only for the NPM-to-MSL transfer. MSL will still need to transfer the message to another system, which might have its own size limit.

Microsoft Office 365 - Cloud

- For Cloud Microsoft Office365 OAuth 2.0 system, the maximum message duration is 6 minutes (or size 3 MB) for an MP3 file.
- For Cloud Microsoft Office365 SMTP system, the maximum message duration is 60 minutes (or size 30 MB) for an MP3 file.

The default limit of 15 MB cannot be altered through the user interface. It can be modified from the command- line interface. To increase the maximum message length, use the following command:

```
config setprop qmail MaxMessageSize 100000000
signal-event email-update
```

Note:
This will adjust the limit only for the NPM-to-MSL transfer. MSL will still need to transfer the message to another system, which might have its own size limit.

NuPoint voice mail to E-mail sync with Microsoft Office365 OAuth 2.0 in a hybrid environment

Symptom:

Users are unable to synchronize their voice mails and E-mail in a hybrid environment using NuPoint voice mail to E-mail with Microsoft Office365 OAuth 2.0.

Sample Error Message:

```
Received Error From Python [error_code:ErrorAccessDenied,message: Access is
 denied. Check credentials and try again.]
```

Cause:

The issue is caused by lack of proper permissions for the Office365 account or a problem with the configuration of the hybrid environment. In particular, the NuPoint voice mail to E-mail feature requires users to be in the Office365 Microsoft Entra ID. Hybrid environments with On-Premise Active Directory are not supported by Microsoft Office365 OAuth 2.0 Education.

Corrective Action:

1. **Check User Accounts**: Ensure all user accounts in the hybrid environment are synchronized with Microsoft Entra ID. User accounts that are not synchronized will be unable to use the NuPoint voice mail to E-Mail feature.
2. **Check Permissions**: Verify that the Office365 account has the necessary permissions to access and is synchronized with the NuPoint voice mail system. Ensure that the permissions are configured correctly. Incorrect permissions can cause the sync to fail.
3. **Check Environment**: Verify that the environment is set up correctly. Ensure that the hybrid environments are not synced with On-Premises Active Directory that are not supported by Microsoft Office365 OAuth 2.0 Education.
4. **Use REST APIs**: If you are using a hybrid environment, note that using REST APIs to access mailboxes in Exchange hybrid deployments is deprecated. For more information, refer to Use REST APIs to access mailboxes in Exchange hybrid deployments (deprecated).

NuPoint voice mail to E-mail sync with Microsoft Office365 OAuth 2.0 in a hybrid environment

Symptom:

Users are unable to synchronize their voice mails and E-mail in a hybrid environment using NuPoint voice mail to E-mail with Microsoft Office365 OAuth 2.0.

Sample Error Message:

```
Received Error From Python [error_code:ErrorAccessDenied,message: Access is
 denied. Check credentials and try again.]
```

Cause:

The issue is caused by lack of proper permissions for the Office365 account or a problem with the configuration of the hybrid environment. In particular, the NuPoint voice mail to E-mail feature requires users to be in the Office365 Azure Active Directory. Hybrid environments with On-Premise Active Directory are not supported by Microsoft Office365 OAuth 2.0 Education.

Corrective Action:

1. **Check User Accounts**: Ensure that all user accounts involved in the hybrid environment are synchronized with Azure Active Directory. User accounts not synchronized will not be able to use the NuPoint voice mail to E-Mail feature.
2. **Check Permissions**: Verify that the Office365 account has the necessary permissions to access and is synchronized with the NuPoint voice mail system. Ensure that the permissions are configured correctly. Incorrect permissions can cause the sync to fail.
3. **Check Environment**: Verify that the environment is set up correctly. Ensure that the hybrid environments are not synced with On-Premises Active Directory that are not supported by Microsoft Office365 OAuth 2.0 Education.
4. **Use REST APIs**: If you are using a hybrid environment, note that using REST APIs to access mailboxes in Exchange hybrid deployments is deprecated. For more information, refer to Use REST APIs to access mailboxes in Exchange hybrid deployments (deprecated).

NuPoint Advance UM Microsoft Office365 OAuth 2.0 Access Token Issue in Virtual environment

Symptom:

Users are unable to synchronize their voice mails and E-mail using NuPoint voice mail to E-mail with Microsoft Office365 OAuth 2.0 due to Access Token issue in VMware ESXi Host Server environment.

Sample Error Message:

Advance Unified Messaging Logs shows the following error message:

```
Offcie365 Oauth2 Graph Error _code:InvalidAuthenticationToken,message:
 Access token has expired or is not yet valid
```

Cause:

The issue is related to time synchronization problems on the VMware ESXi host.

Voice Mail to E-Mail stops working.

Corrective Action:

1. Make sure the ESXi host uses the same NTP source and the time is correct on the ESXi Host Server.
2. Check the time on the ESXi Host Server using the following command via SSH or Putty:

   ```
   # /usr/bin/vmware-toolbox-cmd stat hosttime

   12 Dec 2023 17:15:07
   ```
3. Verify that the displayed time is accurate.

4. If the displayed time is not accurate, disable the periodic time synchronization in the VMware Tools using the following steps:

   a. Start **vSphere Web Client**
   b. Navigate to **Edit Settings** > **VM Options** > **VMware Tools** > **Synchronize Time with Host**.
   c. Deselect the checkbox **Synchronize time periodically**.
5. Use the following command to check VMware Tools time synchronization status:

```
# /usr/bin/vmware-toolbox-cmd timesync status

Disabled
```

6. Confirm that it reports **Disabled**.
7. If necessary, restart VMware Tools on the virtual machine to apply changes.

26.138.3 Upgrading a System With Advanced UM

After you perform an upgrade:

- If your system is connected to a Microsoft Exchange or Lotus Domino mail server and is configured to obtain user data from an LDAP server, confirm that the Advanced UM Email and Advanced UM Password fields are populated automatically.
- If your system is not configured to obtain user data from an LDAP server or is connected to a Google Apps mail server, the user data (email and password) must be reentered on the Web Console or Web View interface. See Enable Advanced UM for a User Mailbox for the required steps.

26.139 Visual Voice Mail Support

Description

Visual Voice Mail is a feature of MiVoice Business software on the MiVoice Business ICP that allows you to visually interact with your voice mail on selected Mitel IP Phones. This feature enables the user to view the voice mail details (type, caller, time, duration) and view information concerning the person who left the voice mail.

For more information about Visual Voice Mail, see the *MiVoice Business System Administration Tool Help* available at Mitel OnLine.

Conditions and Feature Interactions

- A maximum of 120 concurrent Visual Voice Mail sessions are possible to permit users to login, delete, or save their voice mail.
- A maximum of 120 audio connections to the voice mail system can be active at one time.
- A maximum of 50 IP Phones is supported.
- You are automatically logged out of the system after 5 minutes of inactivity.
- For internal calls originating from extensions that have a voice mailbox, Visual Voice Mail displays both the caller name and number. All other calls display "Unknown Caller" followed by the number (if available).

- Each user must have a NuPoint mailbox configured with a Feature Class of Service (FCOS) that contains feature bit 290 ("Unified Messaging - Web View"). To enable optional settings, ensure that the appropriate feature bit is added to the FCOS. For example, to enable "Give and Mark Urgent," add feature bit 018.
- NuPoint UM provides limited support for Visual Voice Mail message playback controls. While listening to a message, you can stop and restart it, but you cannot skip to the end, fast forward, rewind, or go to the beginning of the message. The advanced message playback controls are available only when Visual Voice Mail is implemented with an embedded voice mail system, not with NuPoint UM.

26.140VPIM - Description

Note:
VPIM must be configured using the **Text Console**.

The Administered Voice Profile for Internet Mail (VPIM) optional feature allows users to send voice messages from a NuPoint Unified Messaging system to other, different voice mail systems. The transfer uses the VPIM protocol, which enables voice mail systems from different vendors to communicate with each other.

The voice mail system routes incoming and outgoing messages through the Administered VPIM facility. Outgoing messages go to a pre-configured destination system. Incoming messages go to recipients on the local system. VPIM sets up the routing through information contained in the Digits Translation Table (DTA) and Node Translation Table (NTA).

On outgoing VPIM messages from NuPoint UM, the NTA contains the programming information that defines each node for routing purposes. After reading the node number from the DTA, the server reads the FQDN name and additional VPIM configuration (encoding type, prefix type, and alternate prefix) for the associated node, and then sends the message to the remote VPIM server.

For incoming messages, NuPoint UM compares the destination address to the prefix entries in the DTA. When the DTA table finds a match, it takes the necessary action according to the Absorb Cnt value and reads the node number for that prefix. If the digits that remain after being processed by the DTA match a mailbox listed in the alias file, the server places the message in the recipient's mailbox and activates a message waiting notification.

Nodes and Prefixes

Server that send and receive VPIM messages are called nodes. Each node is identified by a number.

Node prefixes are the leading digit of the network mailbox numbers that are associated with the node, or additional digits dialed in front of the mailbox number. Prefixes can also be used as node ID numbers. All network messages are routed by the node prefixes in the DTA.

Absorb Count

This term refers to the number of leading digits to be stripped by NuPoint UM. For outgoing messages, the VPIM compares the destination address to the prefix entries in the DTA. When it finds a match, it strips the prefix (or leading digit(s)) from the destination address. NPM absorbs the same number of digits indicated

by the absorb count. A value of 0 passes the digits unaltered; a value of 1 or higher strips the number of digits as indicated from the front of the mailbox (destination) address.

Alias

The Alias file is an ordered list of mailbox extensions on the local NuPoint UM voice mail system. This file is used by VPIM to match mailboxes for routing the messages to the appropriate mailbox.

Digits Translation Table

The Digit Translation Access (DTA) table holds the information (mail server and node identification) that sorts or routes the messages. For example:

Prefix	Node	Absorb Cnt
520	2	3
512	1	3

Node Translation Table

VPIM uses a prefix configured in the NTA table for transporting the message between nodes in the network. On outgoing VPIM messages from NuPoint UM, the NTA contains the programming information that defines each node for routing purposes. After reading the node number from the DTA, the server reads the FQDN and additional VPIM configuration (encoding type, prefix type, and alternate prefix) for the associated node, then sends the message to the remote VPIM server. After receiving a message, the remote system checks the DTA and NTA tables to derive the mailbox number from the message address.

For the various VPIM nodes to successfully send and receive messages, the DTA and NTA tables at each VPIM node must contain the same information about all VPIM nodes.

To exchange VPIM messages with a remote node, set the protocol type in the NTA table for both nodes to “VPIM”.

An example of the NTA table is:

```
Node
Number      Protocol Type
                  Access

1 VPIM Y

Domain name : sanityem.inter-tel.com

Encoding type: G.721 Prefix type: No Prefix

Node Number Protocol Type Access

2 VPIM Y

Domain name : nupoint.mitel.com

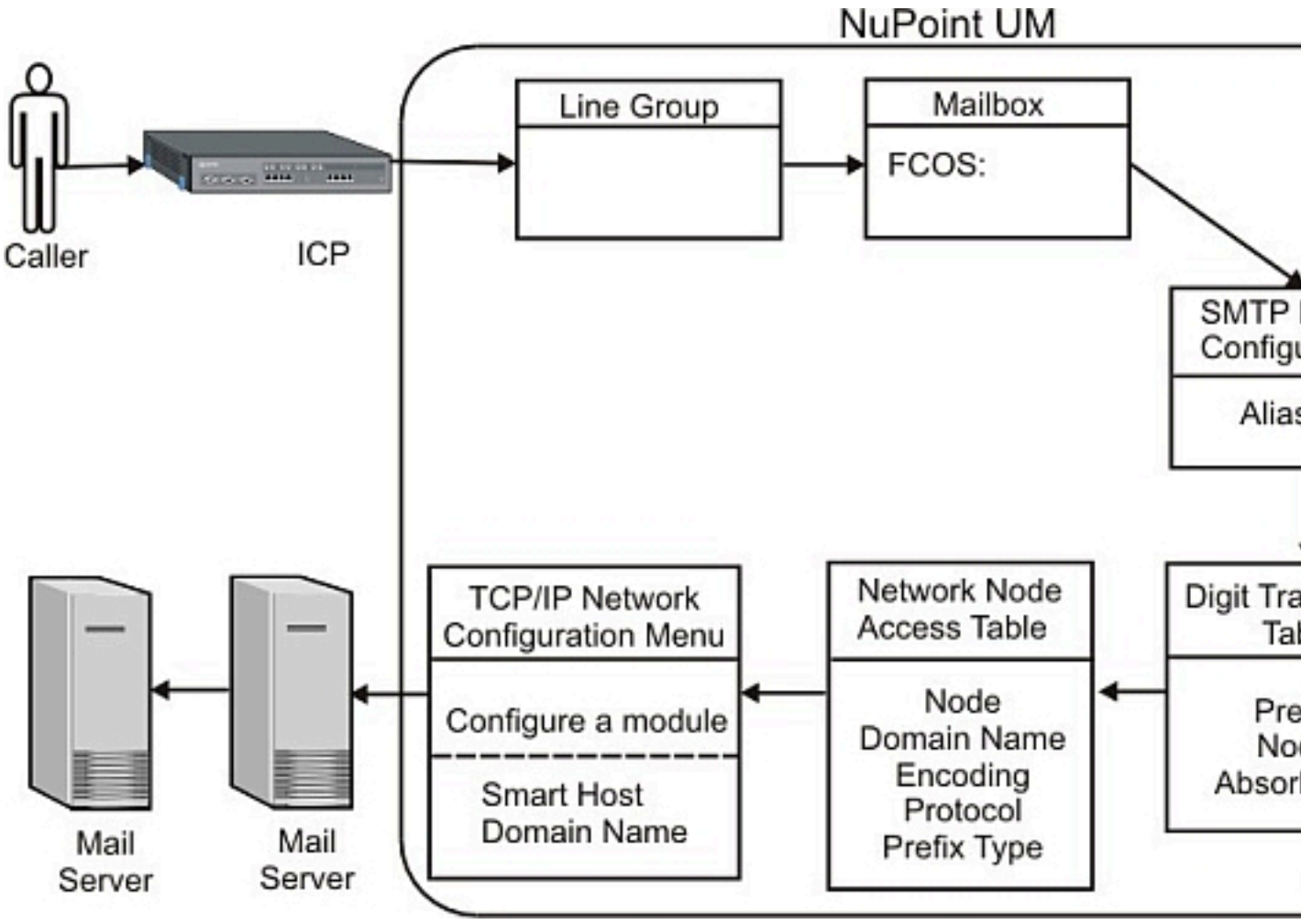
Encoding type: G.721 Prefix type: No Prefix
```

26.140.1 Configuration Overview

The following figures illustrate the flow of information and configuration required for VPIM messages to be sent and received.

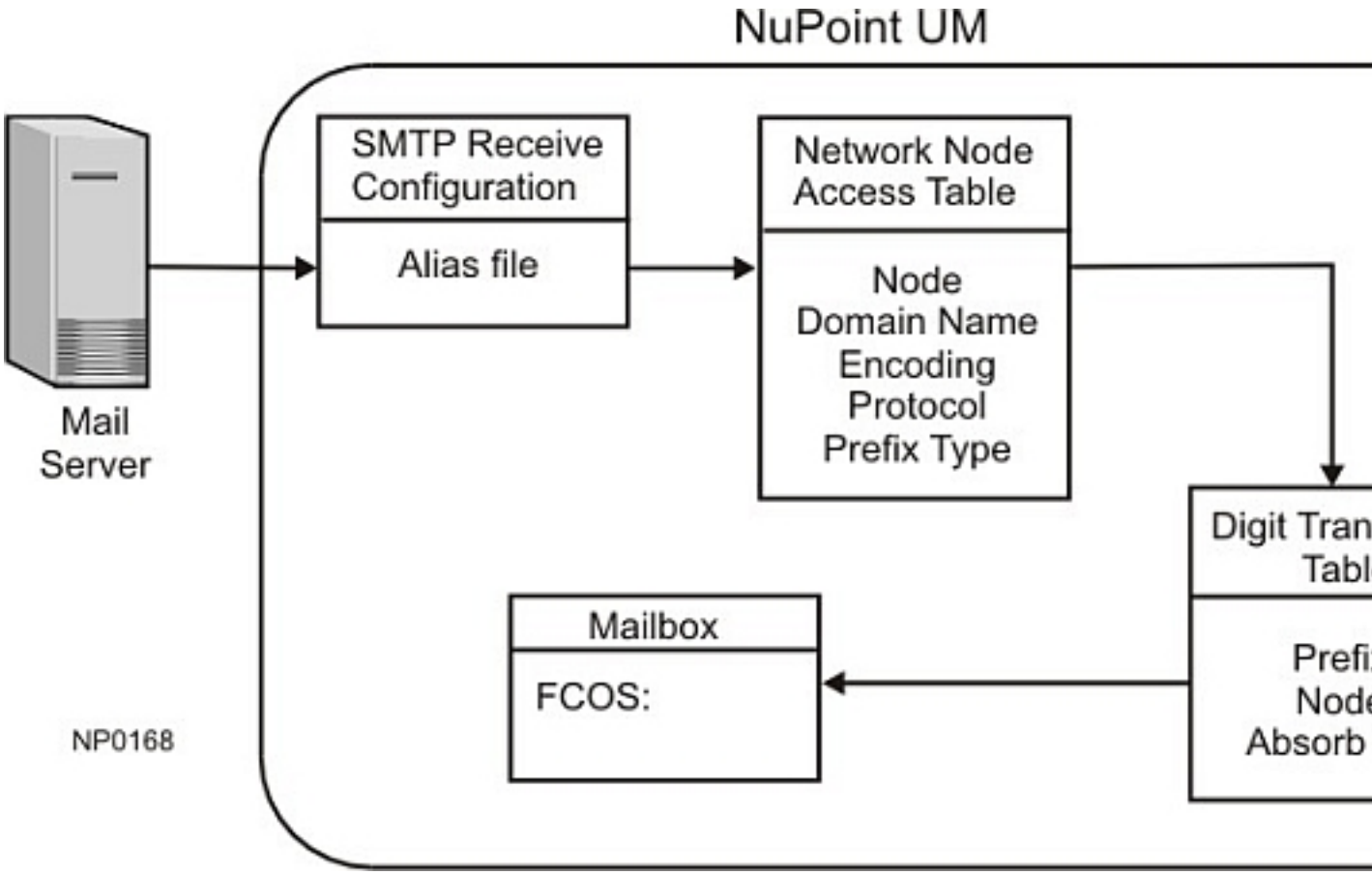
Sending a VPIM message from a Mailbox

The diagram below shows the configuration menus in NuPoint UM that must be set up for NuPoint UM to send VPIM messages.



Receiving a VPIM message and saving it to a Mailbox

The diagram below shows the configuration menus on NuPoint UM that must be set up for NuPoint UM to receive VPIM messages.



26.140.2 NuPoint-UM Configuration

Configuring VPIM includes setting basic parameters for the TCP/IP network and for mailboxes, then setting parameters that determine how the mailboxes with the VPIM feature will communicate over the network.

Before you start to configure VPIM on any node in the network, identify each node in the network and record these parameters:

- **Node Number** The number, from 2 to 8191, that identifies each node in the system; do not use 1 for any VPIM node
- **Prefix Type** Select the prefix type for each node:
  - Default: the VPIM user mailbox uses the prefix configured in the DTA table
  - No prefix: the VPIM user mailbox does not include a prefix
  - Alternate prefix: the VPIM network uses a prefix configured in the NTA table for transporting the message between nodes in the network
- **Prefix** The number, from 1 to 99,999,999,999, of the prefix for user mailboxes on ths node; set in the DTA table (set the Prefix Type to D)
- **Alternate Prefix** The number, from 1 to 999,999, if a node uses the alternate prefix set in the NTA table (set the Prefix Type to A) for transporting messages within the network.

Configure VPIM

VPIM configuration consists of the following steps (described in detail below):

1. Configure basic VPIM parameters.
2. Configure the NTA table.
3. Configure the DTA table.
4. Configure the Dial Plan.
5. Configure the Network Queue.
6. Configure SMTP Message Reception.
7. Generate and verify the Alias File.
8. Test the VPIM Feature

Configure Basic VPIM Parameters

To use the VPIM optional feature, configure as follows:

1. Add any necessary optional feature software.
2. Set up Unified TCP/IP:
   - From the console Main menu, select **(S) System Maintenance**, **(R) Reconfiguration**, **(R) Reconfigure System**, **(G) Offline Menu**, **(B) Duplicate Configuration**, and then **(U) Unified TCP/IP**
   - Select **(M) Configure a Module**
   - Select **(V) Smart Host Domain Name** and enter the fully qualified domain name for the smart host (i.e. the company e-mail server).
3. Set the Features Class of Service (FCOS). By default, the FCOS is 1, which includes permissions to receive/create/send VPIM messages.
4. Set the Network Class of Service (NCOS). Use the NCOS function to control a user's privileges, such as answering, making, or giving voice messages across the network. To include basic VPIM message capability in any mailbox, set up an NCOS with NCOS bits 2 through 9 as shown here:

NCOS Bit	Description
002	Allow user to make network messages
003	Allow user to make urgent network messages
004	Allow user to give network message
005	Allow user to give urgent network messages
006	Allow user to answer network message
007	Allow user to answer urgent network messages
008	Automatic receipt on network messages
009	Say "Remote mailbox" when playing network messages

Configure the NTA table

For the node for each server, determine these NTA parameters:

- **Node number** A number, from 2 to 8191, that identifies a particular node in the system. Do not use 1 for any VPIM node.
- **Protocol** V for VPIM
- **Access** Y for all nodes
- **Domain name** The Internet address, up to 255 alphanumeric characters
- **Prefix Type** Select the prefix type for the node:
  - D, default: the VPIM user mailbox uses the prefix configured in the DTA table
  - N, no prefix: the VPIM user mailbox does not include a prefix
  - A, alternate prefix: the VPIM network uses the prefix configured in the NTA table for transporting the message between nodes in the network
- **Alternate Prefix** The number, from 1 to 999,999, that is the alternate prefix if the Prefix Type is set to A.

To configure the NTA table:

1. From the Main menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, and then **(T) Network Node Table**.
2. Select **(C) Create new node entry** and then, when prompted, set the following parameters:
3. **Node number**: enter the **number** that identifies the node in the system.
4. **Protocol:** enter **V (VPIM Node)**
5. **Domain Name**: enter the fully qualified host name of the node, up to 255 characters.
6. **Encoding type**: enter **G**. (G.726 (formerly G.721) for VPIM-compliant communication)
7. **Select prefix to use**: enter **N (no prefix should be sent from the server)**
8. **Access**, enter **Y. (allow access)**
9. **P**ress **Enter** to return to the Network Node Access Table Maintenance menu.

Here is a sample Node Access Table Report that includes VPIM node #3 with the address "load.bayptin.com":

```
        NODE ACCESS TABLE REPORT       Wed Jan 5 03:12:45 20XX  NODE NAME  PROTO STRING   HA
RDWARE  ACCESS PARALLEL LINKS                DELAY MAX  2     VPIM        Y  Domain name : model120.bayp
tin.com  Encoding type: G.721 Prefix type: Use Default  3    VPIM        Y Domain name : load.bayptin.com Encodi
ng type: G.721 Prefix type: Use Default 4    VPIM        Y Domain name : model70.bayptin.com Encoding type: G.7
21 Prefix type: Use Default 104 npnet1   TCP  100.1.1.1   0 = ETHERNET  Y  105 npnet    TCP 100.1.1.2  0 = ETHE
RNET  Y  5 Nodes found Press any key to continue....
```

Note: The G.721 codec has been superceded by G.726, which is the standard codec for VPIM to use.

Configure the DTA table

For each node, determine these DTA parameters:

- **Node Number** A number, from 2 to 8191, that identifies a particular node in the system. Do not use 1 for any VPIM node.

- **Absorb digit** The number of digits to absorb (strip from the telephone number) for a destination node. Set this to the same length as the prefix.
- **Prefix** The number, from 1 to 99,999,999,999 that is the valid prefix for this node.

To configure the DTA table:

1. From the Main menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, and then **(D) Digits Translation**.
2. Select **(C) Create new prefix/node pairs**and enter the**number** for the VPIM node.
3. At the **Absorb digits** prompt, enter the **numbe**r of digits to strip from the telephone number.
4. At the **Prefix** prompt, enter the prefix **number** for this node.
5. Exit to the Digits Translation menu and select **(L) List the data table** to check your information. A sample DTA table is shown here:

```
PREFIX/NODE PAIR REPORT

Tue May 25 08:54:18 20XX

Prefix Node Absorb Cnt

520 2 3

512 1 3

6 6 0

888 888 3
```

In this example, the prefix "520" represents remote mailboxes that have 4 digits and leading digits 520. A message sent to 5202000 has a sender address that looks something like "2000@company.mitel.com. The 520 prefix is stripped as indicated by the Absorb Count of 3.

Configure the Dialing Plan

For more information, see About Dialing Plans.

-
- Each position or index in the Dial Plan reading left to right corresponds to a digit from 1-9 as shown below.

Position	1	2	3	4	5	6	7	8	9
Dial Plan Digit	4	4	4	4	4	N8	4	4	4

-
- The "N" indicates that the corresponding dialing plan entry represents a **N**etwork node (that is, VPIM). In the example above, the prefix for a remote office is “612” and the mailboxes are of 5 digits in length.

The “N8” placed at index number 6 indicates that all Network mailboxes starting with the digit "6" are considered remote network mailboxes with length of 8 digits. For example, when a NuPoint UM user forwards a voice mail message to mailbox 12345, that is located on the remote location Voice Mail 612, the NP-UM user enters 61212345 to send to the remote VPIM mailbox.

To configure the Dialing Plan:

1. From the Main Menu, select **(S) System maintenance**, **(R) Reconfiguration**, **(R) Reconfigure system**, **(E) Modify Active Configuration**, **(M) Modify Application**, **(D) Dialing Plan Menu**.
2. Modify the dialing plan to handle your node prefix plus the length of the mailboxes. You must set the dialing plan of every line group from which users will be allowed to send network messages.
3. Exit the active configuration menu.

Configure the Network Queue

The network queue parameters affect how NP Net and VPIM perform in a system. Use these settings, rather than the defaults, for optimum VPIM performance:

Parameter	Explanation	Set to
Message Count Threshold	The minimum number of individual messages, of any type, that must arrive in a queue before that queue sends the messages	0
Message Waiting Threshold	The maximum time, in minutes, that any message can wait in a queue, even if the message total has not reached the message count threshold	0
Total Message Minutes	The minimum total of speech time that must arrive in the queue before the queue sends the messages.	0
Maximum Call Setup Tries	The maximum number of calls that this node will make to the destination node to make a connection	3
Call Setup Retry Interval	The time, in minutes, between attempts to establish a connection with the destination node.	2

To configure network queueing:

1. From the Main menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, then **(Q) Modify Network Queueing**.
2. Set the Network Queue Time Windows for weekdays and weekends according to the guidelines for the site. For details about the Network Queue parameters, see the NP Net topic Configure the Network Queues.

Configuring SMTP Message Reception

SMTP Message Reception must be modified to set the SMTP Receive Tasks Limit to 1. This allows the server to continue processing other calls.

1. From the Main menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, **(V) SMTP Receive Configuration**, and then **(M) Modify VPIM configuration**.
2. At the **Max Number of Receivers** prompt, enter **1**.

Generating and Verifying the Alias File

To generate the alias file:

1. From the Main menu, select **(S) System Maintenance**, **(W) Network Menu**, **(M) Network Maintenance**, **(V) SMTP Receive Configuration**, then **(G) Generate Alias File**. The utility automatically creates the list of prefixes with mailbox numbers that can send and receive VPIM messages.
2. Select **(V) View Alias File** and verify that all mailboxes are included. A sample alias list is shown here:

```
# aliases for VPIM accounts

vpim: "|/usr/vm/bin/vpim_rcv"

1234:"| /usr/vm/bin/vpim_rcv -a 1234"

1235:"| /usr/vm/bin/vpim_rcv -a 1235"

1236:"| /usr/vm/bin/vpim_rcv -a 1236"

1250:"| /usr/vm/bin/vpim_rcv -a 1250"

1251:"| /usr/vm/bin/vpim_rcv -a 1251"

1252:"| /usr/vm/bin/vpim_rcv -a 1252"

1253:"| /usr/vm/bin/vpim_rcv -a 1253"

1254:"| /usr/vm/bin/vpim_rcv -a 1254"

1260:"| /usr/vm/bin/vpim_rcv -a 1260"

1261:"| /usr/vm/bin/vpim_rcv -a 1261"

1262:"| /usr/vm/bin/vpim_rcv -a 1262"

1263:"| /usr/vm/bin/vpim_rcv -a 1263"

1264:"| /usr/vm/bin/vpim_rcv -a 1264"

3333:"| /usr/vm/bin/vpim_rcv -a 3333"

3849:"| /usr/vm/bin/vpim_rcv -a 3849"
```

Each time you create or delete a mailbox with VPIM privileges, you must regenerate the alias file.

Test the VPIM Feature

When all parameters are configured and the nodes are connected, check that messages move successfully between remote mailboxes.

1. Make and send one or more messages from a mailbox on one node to mailboxes on each other node in the system.
2. Check that all messages arrived.
3. Answer each message from within the mailbox.
4. Check that each answer arrived at the originating mailbox.

26.140.3 Exchange Server 2010 Configuration

To configure VPIM on the Microsoft Exchange Server 2010:

1. Open the Exchange Management Console.
2. Expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Send Connectors** tab.
3. In the action pane, click **New Send Connector**. The New SMTP Send Connector wizard starts.
4. On the **Introduction** page, follow these steps:

   - In the **Name** field, type a meaningful name for this connector. Specify a name for the Send connector that helps you distinguish this Send connector from other Send connectors in your configuration.
   - In the **Select the intended use for this connector** field, select the usage type for the connector. The usage type determines the default permission sets assigned on the connector and grants those permissions to trusted security principals.
5. Click **Next**.
6. On the **Address space** page, click **Add** to specify an SMTP address space to which the Send connector sends mail. Enter the fully qualified domain name (FQDN) of the host.
7. Click **Next**.
8. Configure other settings as required.
9. On the **Completion** page, review your settings and then click **Finish** to close the wizard.

26.141 Web View - Description

The Web View application provides an interface for managing Unified Messaging, Call Director and NP Fax features from an e-mail client or Web browser.

To use Web View, users must be licensed and configured for Unified Messaging, Call Director and/or NP Fax, and they must also have Web View configured for email or Web browser. See Web View Configuration.

Compatible web browsers include:

- Microsoft Edge
- Internet Explorer
- Google Chrome
- Mozilla Firefox

Your user type determines your access to the tabs in the Web View interface:

User Type	Available Tabs:
UM-SMTP	Settings
UM - Web View	Messages, Settings, Distribution Lists, and Greetings
Standard UM	Messages, Settings, Distribution Lists, and Greetings
Advanced UM	Messages, Settings, Distribution Lists, Greetings and Downloads Users can launch the Web View from the optional Unified Messaging toolbar in their Microsoft Outlook email client.
Call Director	Call Director
NP Fax	Messages, Settings and Downloads

Note:
A UM user can also be a Call Director or NP Fax user, but a Call Director or NP Fax user does not have to be a UM user.

Web View is available in the following languages:

- North American English
- UK English
- Canadian French
- European French
- Dutch
- Latin American Spanish (NuPoint UM 4.0 and later)

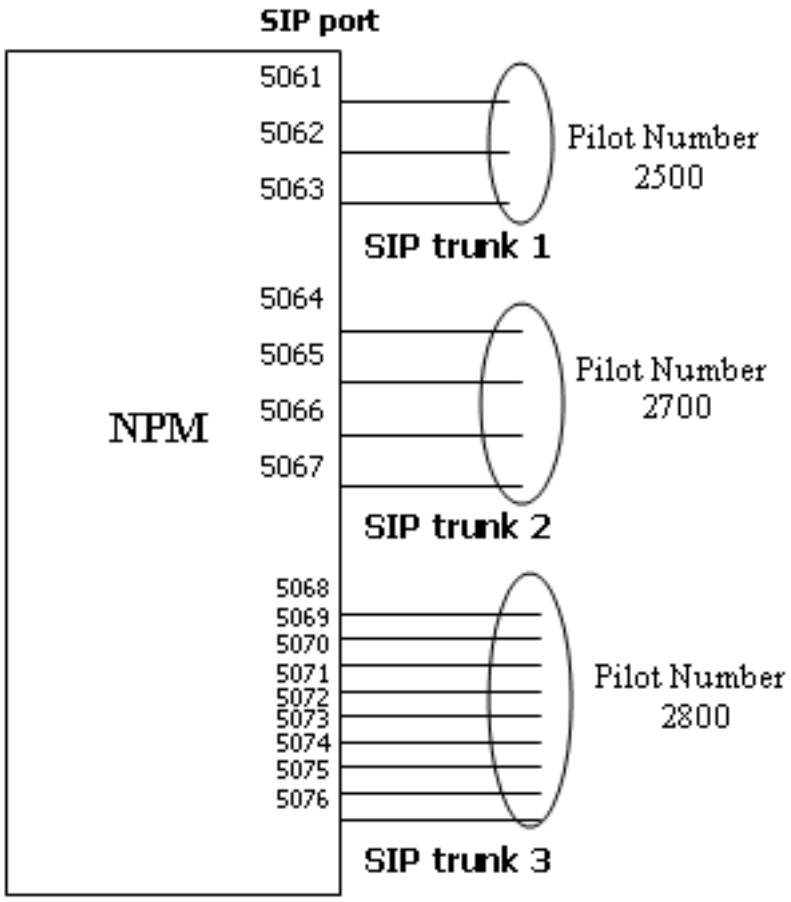
26.142 MiVoice Office 250 Integration Overview

NuPoint Unified Messaging (NuPoint UM) supports Session Initiation Protocol (SIP) integration with the MiVoice Office 250 via the MiCollab. NuPoint UM communicates with a single MiVoice Office 250 system over a SIP trunk. The MiVoice Office 250 communicates with NuPoint Unified Messaging through the SIP interface and consequently has access to the voice mail features. The maximum number of NuPoint 60 ports is 16. Speech Auto Attendant ports are licensed separately.

Note:
The MiVoice Office 250 integration is supported only on MiCollab Release 1.2 or later. The configuration for MiVoice Office 250 on NuPoint UM will fail if the NuPoint UM software is installed without the MiCollab license.

One or more SIP trunks can link NuPoint UM to the MiVoice Office 250. NuPoint Unified Messaging receives and sends SIP messages over these trunks. Each SIP trunk consists of one or multiple SIP ports.

The diagram below illustrates the SIP trunk integration:



Every SIP trunk is assigned a Pilot Number. To call into NuPoint UM, the MiVoice Office 250 provides a pilot number for the endpoint users to dial. When NuPoint UM makes a trunk call to the MiVoice Office 250 , it identifies itself using a pilot number. Therefore, when NuPoint UM receives an incoming call, the pilot number is used as the Called ID. When NuPoint UM makes an outgoing call, in the case of MWI, pager or external call transferring, the pilot number is used as the Calling ID.

A SIP session is established through connection to a SIP port in real-time. Each SIP port handles one call connection to NuPoint UM, thus the number of ports grouped in a SIP trunk determines the number of parallel-connections this trunk can handle at the same time. For example, if four callers on the MiVoice Office 250 simultaneously dial the pilot number 2500 (shown in the figure above), only three of these callers can be connected to NuPoint UM. This principle is applied to every voice mail call connection, whether it is inbound and outbound.

The pilot numbers on NuPoint UM are mapped to applications on the MiVoice Office 250. For example, pilot number 2500 for NuPoint UM Voice is mapped to extension 2500 for the Voice Mail application programmed on the MiVoice Office 250 . In the configuration where the application is configured as a mailbox, you must associate an extension to an application as well as the pilot number used to access the application. Multiple pilot numbers can exist in the system.

To be consistent with the existing IP, Digital Media Gateway (DMG - formerly PIMG/TIMG) integrations, a SIP trunk is reserved to be either a receiver or a sender, so it cannot perform both roles. The receiver SIP trunk will detect inbound calls and the sender SIP trunk will generate outbound calls.

All calls arriving to NuPoint UM on a SIP trunk are accepted at the fixed and predefined SIP port. This port is not configurable. The call is redirected based on the pilot number (which is the called ID in the case of an incoming trunk).

All SIP trunk calls generated by NuPoint UM include a pre-configured SIP port and a pilot number (which is the calling ID in the case of an outgoing trunk).

Supported Functionality

The following NuPoint Unified Messaging functionality is supported with the MiVoice Office 250 SIP integration:

- Configuring a Cluster Node and SIP Channels linked to the MiVoice Office 250
- Backing up and restoring a configuration
- Answering a telephone or Speech Auto Attendant (SAA) call
- Receiving and replying to fax messages
- Playing prompts and recording messages
- DTMF recognition and collection
- Transferring calls
- Making a call to MWI, Pager or Fax connected to the MiVoice Office 250
- Record-A-Call
- Voice Mail Softkeys

Licensing and Optioning

SIP is not a purchasable option. No special license is required for it. SIP lines or channels are licensed the same way as the DMG (formerly PIMG/TIMG) integration, and no special option will be provided.

The configuration of the MiVoice Office 250 as a cluster item is allowed if a MiCollab license is granted. Refer ***Applications*** > ***Users and Services*** > ***About UCC Licensing*** for more information on licensing.

26.142.1 Prerequisites for the MiVoice Office 250 Integration

The requirements stated below must be satisfied before NuPoint UM can be integrated with the MiVoice Office 250 via a SIP Gateway connected to IP endpoints.

1. The MiVoice Office 250 integration is supported only on MiCollab Release 1.2 or later. The configuration for the MiVoice Office 250 on NuPoint UM requires a MiCollab license. Refer ***Applications*** > ***Users and Services*** > ***About UCC Licensing*** for more information on licensing.

2. It is assumed that the SIP Gateway is running and correctly configured with IP Endpoints so that each endpoint has a registered extension.
3. Mitel Standard Linux (MSL) and NuPoint UM software must be installed and running on a computer system connected to the same physical network as the SIP Gateway. Also, full IP connectivity is assumed possible between NuPoint UM and the SIP Gateway, meaning that no security hardware or software is active.
4. MSL has been properly licensed using Mitel's Applications Management Center server (AMC). NuPoint UM features to be used or tested must be enabled in the AMC Application Record. The Application Record ID is requested and the Application Record is "activated" during the MSL installation.
5. The NuPoint UM server is mapped from the SIP gateway by a Pilot Number and configured as a SIP Trunk.
6. The security settings on the NuPoint UM server must be modified so that it is possible to establish full telephony communication between the SIP Gateway and NuPoint Unified Messaging. Follow the procedure below to modify the security settings.

Modifying the Security Settings for NuPoint Unified Messaging

You can grant server access privileges to additional networks:

1. Log into the MiCollab server console.
2. Under **Configuration**, click **Configure Networks**.
3. Click **Add a new trusted network**.
4. In the Network Address field, enter the IPv4 or IPv6 address of the network to designate as “local”.
5. In the Subnet mask or network prefix length field, enter the dot-decimal subnet mask or CIDR network prefix to apply to the Network Address. If this field is left blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6networks.
6. In the Router field, enter the IP address of the router you will use to access the newly-added network.
7. Click **Add**.

1. **Note:** Under some circumstances, modifying the "Local Networks" will not update security settings correctly. Should call connectivity or two-way audio not appear to be initiated correctly, the following command may be issued, as a last resort, to disable the NuPoint UM server firewall through a Linux console session: **service masq stop**.

26.142.2 MiVoice Office 250 Integration Configuration Overview

The Mitel MiVoice Office 250 and NuPoint Unified Messaging integration requires configuration of three different applications:

- MiCollab
- NuPoint Unified Messaging (NuPoint UM)
- MiVoice Office 250

Several prerequisites must first be satisfied before NuPoint UM can be integrated with the MiVoice Office 250 via a SIP Gateway connected to IP endpoints.

To integrate NuPoint UM with the MiVoice Office 250 , the system administrator must configure a cluster node that represents the peer MiVoice Office 250 and the line group(s) that represent the SIP trunk(s). Line(s) must be added to the line group and mapped to the SIP ports.

The system administrator must configure a SIP Gateway (add a SIP Gateway as a Cluster Node) and then configure SIP trunks as line groups before calls can be made from IP Endpoints to NuPoint UM. The information entered in these steps provides NuPoint UM with SIP Gateway IP/port data and Line mapping details used to accept calls from the SIP Gateway and re-direct them to available NuPoint UM lines. When Lines are linked to a SIP Gateway Cluster Node, incoming SIP calls can be accepted and routed to available NuPoint UM Lines for SIP.

Refer to Add a Line Group for instructions to configure a SIP Gateway and to configure NuPoint Unified Messaging lines for a SIP Gateway.

Once the configuration is complete, IP endpoints will call a Pilot Number that routes to an available NuPoint UM line and will hear a greeting prompt, such as "Welcome to the message center. Please enter a mailbox number or wait."

Constraints

- Although the NuPoint UM software system does not prevent the system administrator or installer from configuring and setting up a SIP integration that includes Digital Media Gateway (formerly PIMG, HD-PIMG, or TIMG) and the MiVoice Office 250 , this integration mix **is not supported** .
- NuPoint UM will communicate with only one MiVoice Office 250 .
- Although you can configure more than one MiVoice Office 250 node to communicate with NuPoint UM, it is not a supported configuration and many NuPoint UM features like MWI and Pager Notifications do not work with this type of configuration.
- The numbers used by the SIP interface to represent SIP ports (e.g. Port 5058 for NuPoint UM on MAS or 5060 for NuPoint UM Standalone) remain as unconfigurable data.

External Dependencies

- The SIP component on the MiVoice Office 250 is required. Refer to the MiVoice Office 250 documentation for SIP configuration instructions.
- The MiVoice Office 250 must be configured to use the correct port for SIP communication from NuPoint UM. For NuPoint UM on MiCollab , use 5058; for NuPoint UM Standalone, use 5060.
- The configuration for MiVoice Office 250 on NuPoint UM requires a MiCollab license. Refer ***Applications*** > ***Users and Services*** > ***About UCC Licensing*** for more information on licensing.

Refer to the MiVoice Office 250 Integration Task Summary for configuration task lists for each of the applications.

26.142.3 MiVoice Office 250 Integration Task Summary

This section provides task summaries for integrating NuPoint Unified Messaging voice mail with the MiVoice Office 250. Each summary provides a high-level list of the tasks that are required for each of the applications involved in the product integration.

For detailed integration procedures, refer to the *Mitel MiVoice Office 250 and NuPoint Unified Messaging Integration Guide* available at Mitel OnLine.

Task summaries are provided below for the following applications:

- MiCollab
- NuPoint Unified Messaging
- MiVoice Office 250

MiCollab Installation Summary

The table below summarizes the installation and configuration tasks necessary on the MiCollab server.

Refer to the *MiCollab Installation and Maintenance Guide* for detailed procedures.

TASK	COMMENTS
Install Mitel Standard Linux (MSL) and NuPoint UM software.	Install from boot-up on the MiCollab server connected to the same physical network as the MiVoice Office 250. Also full IP connectivity is assumed possible between NuPoint UM and the SIP Gateway, meaning that no security hardware or software is active.
Install application blades from CD.	
Install Text-to-Speech blade from the Server Manager Blades panel.	
Reboot the MiCollab server.	Make sure to select the EL version of the kernel.
Check that MSL has been properly licensed using Mitel's Applications Management Center server (AMC).	NuPoint UM features to be used or tested are enabled in the AMC Application Record. The Application Record ID is requested and the Application Record is activated during the MSL installation.

NuPoint Unified Messaging Configuration Summary

The following configuration tasks are required for NuPoint Unified Messaging voice mail to integrate with the MiVoice Office 250 .

A documentation reference is provided for each of the configuration tasks.

TASK	COMMENTS
Verify that the SIP Gateway is running and correctly configured.	This provides NuPoint UM with SIP Gateway IP/port data and Line mapping details used to accept calls from the SIP Gateway and redirect them to available NuPoint Lines. SIP endpoints will be able to call a Pilot Number that will route to an available NuPoint UM line and hear a greeting prompt, such as "Welcome to the message center. Please enter a mailbox number or wait."
Verify that the security settings on the NP-UM server have been modified so that it is possible to establish full telephony communication between the SIP Gateway and NuPoint.	Security modifications are completed within the MSL Server Console. See Modifying the Security Settings on the NuPoint Unified Messaging Server for instructions.

TASK	COMMENTS
Configure/Add a SIP Gateway as a Cluster Node to NuPoint UM.	This is necessary to set up network mappings for SIP calls. Refer to Add a Network Element for instructions to configure a SIP Gateway.
Configure NuPoint UM Line Groups, Ports, and Dialing Plan.	Each NuPoint UM line is dedicated to handle one call at a time. Therefore, the number of lines defined in NuPoint UM is the maximum number of simultaneous calls possible. NuPoint UM can have up to 120 lines. A Line Group is a collection of one or more NuPoint UM lines, each mapped to a cluster node. When lines are linked to a SIP Gateway cluster node, incoming SIP calls can be accepted and routed to available NuPoint UM lines for SIP. Refer to Add a Line Group for instructions to set up NuPoint Unified Messaging lines for a SIP Gateway.
Configure basic voice mail and mailboxes for NuPoint UM.	Add users, phones, mailboxes, and the Speech Auto Attendant. After the configuration is completed, an endpoint that calls in to NuPoint UM with an extension that matches the mailbox number in the created mailbox will be prompted to log on. For example, if mailbox 1000 is created, the Endpoint assigned to extension 1000 may call NuPoint UM and hear "Hello mailbox 1000. Please enter your passcode."
Set up and initialize the Administrator mailbox.	The Administrator mailbox is set up by default (under mailbox number 998) during the NuPoint UM software installation. It can be used to record System Message Prompts and program additional user mailboxes. See Managing Mailboxes

TASK	COMMENTS
Direct callers to NuPoint UM mailboxes on Call No Answer.	Call No Answer scenarios must be correctly configured through the SIP Gateway/SIP Endpoint Call Forwarding options. In general, when Call No Answer is detected at the SIP Endpoint, the call should be forwarded to the NuPoint UM Pilot Number (Extension) as "Call Forward Not Available." It is assumed that the Endpoint Extension forwarding the call matches a mailbox number programmed in NuPoint UM. If this is the case, when a forwarded call is received by NuPoint UM, a prompt will indicate that the recipient is not available and ask the caller to leave a message.
Enable message notifications.	Check that message notifications are set up at the mailbox level. Each mailbox may be set up for two notification types concurrently. Refer to Configure a Mailbox for Paging. **Note**: When a Message Delivery Pager Notification Type is enabled, the receiver of the Notification Call must speak within five seconds for NuPoint UM to provide message information and options. Otherwise, NuPoint UM will consider the Notification Call to be a failure.
Configure Distribution Lists.	Distribution lists allow a mailbox user to send messages to multiple mailboxes in one step. Distribution lists may be configured in the Web Console or in the Web View interface. Refer to Managing Distribution Lists. Refer to the *Web View Help* for configuration instructions through the web view interface.
Configure Line Groups voice mail, MWI notifications, and Pager Notifications if this functionality is used in the system.	Refer to Add a Line Group.
Configure Line Groups for Speech Auto Attendant, Fax, and NuPoint Receptionist if this functionality is used in the system.	
Configure NuPoint Receptionist if this functionality is used in the system.	Refer to NP Receptionist.

TASK	COMMENTS
Create call flows with Call Director.	Create customized call flows to handle incoming callers with the NuPoint UM Call Director. Before any Call Director call flow may be created, the Call Director User Interface must be enabled within associated Line Groups. Refer to the *Call Director Help* for call flow creation.
Configure Classes of Service (COS).	Each mailbox created in NuPoint UM is assigned a set of values that define features, limitations and restrictions. These attributes are defined as three Classes of Service, called Feature Class of Service (FCOS), Limits Class of Service (LCOS) and Restriction Class of Service (RCOS). Default classes already exist in NuPoint and are applied to new mailboxes automatically. However, changing privileges for a user requires an administrator to apply different classes to a mailbox. New classes definitions are often required to define a specific set of attributes adequately.

MiVoice Office 250 Configuration Summary

The following list provides a configuration summary of what to configure on the MiVoice Office 250 for NuPoint UM.

Refer to the *MiVoice Office 250 Features and Programming Guide* for detailed procedures.

TASK	COMMENTS
Create SIP Peer Voice Mail.	
Specify configuration options.	The following information is required: • IP address • Port number • Call configuration • Maximum number of ports
Configure Group Lists.	
Configure Mailboxes.	

TASK	COMMENTS
Configure IP Call Configuration.	The following configuration is required: • Set "Supports RTP Redirect" field to **No**. • Set "DTMF Encoding Settings" field to **RFC 2833**. • Set "Audio Frames/IP Packet" field to **2**. • Set "Fax Detection Sensitivity" field to **0**. • Set "Fax Encoding setting (Fax Transmission)" field to **G.711 Mu-Law**.
Create and configure SIP Peer Voice Mail Application.	

26.142.4 MiVoice Office 250 Integration Troubleshooting

The following sections provide specific information on SIP feature interactions that may help to troubleshoot some common SIP problems. Also refer to Integration Prerequisites for additional information.

SIP Feature Interactions

Clustering

The SIP subsystem on NuPoint UM communicates to only one cluster node of the MiVoice Office 250. If there is more than one MiVoice Office 250 system installed in a cluster, the MWI and pager calls may not be directed to the correct MiVoice Office 250 system.

Call Redirection

All calls that arrive on NuPoint UM are made to the same location. The SIP subsystem on NuPoint UM will redirect every incoming call to an appropriate line configured as a SIP port.

For example, when NuPoint UM receives a voice mail call at a reserved and fixed SIP port, NuPoint UM will redirect this call to one of the free ports in the SIP trunk group.

Validation of Incoming Call

In order for the SIP subsystem on NuPoint UM to accept an incoming call, this call must have the correct IP address of the MiVoice Office 250 and a correct Pilot Number. In addition, the call must arrive on the correct port for SIP communication (5058 for NuPoint UM on MAS or 5060 for NuPoint UM Standalone).

A call is rejected if validation fails.

Answering a Call

The SIP subsystem on NuPoint UM uses the called ID (i.e. pilot number of a call) to select a line pre-configured for the line group identified by the given pilot number.

A busy reply is given if all lines in this line group are busy.

Generating a Call

The SIP subsystem on NuPoint UM uses the pilot number configured for a specific outgoing line group as the calling ID and send the call via a free line in the group to a fixed location on the MiVoice Office 250.

Lighting MWI

NuPoint UM provides the MiVoice Office 250 with the extension number of an endpoint and the indication for light on or off.

Media Connection

During the set up of a pager call, the MiVoice Office 250 can negotiate with NuPoint UM for a standard DTMF payload type that is sent from NuPoint UM.

There is no specific change required for the current RTP subsystem in order for it to send and receive audio including DTMF to and from the MiVoice Office 250 .

MiCollab Licensing

The MiVoice Office 250 integration is supported only on MiCollab Release 1.2 and higher. The configuration for the MiVoice Office 250 on NuPoint UM will fail if the NuPoint UM software is installed without the MiCollab license. Refer ***Applications*** > ***Users and Services*** > ***About UCC Licensing*** for more information on licensing.

26.143 About Call Director

Call Director is an optional feature that adds powerful call-processing capabilities to your NuPoint Unified MessagingTM (NP-UM) system.

With Call Director, you can create automated attendant and call processing applications, known as *call flows*, for your organization, for departments within your organization, and for individual mailboxes and extensions.

Call Director is an optional feature that adds powerful call-processing capabilities to your NuPoint Unified Messaging (NP-UM) system. With Call Director, you can create an automated attendant application (known as a *call flow*) to handle your calls when you can't answer personally.

A call flow is a collection of call-processing *actions* programmed by the call flow owner to control how an incoming call is handled. Call flow owners can be either the end user of the phone, or the System Administrator. The end user programs personal call flows, which are associated with their own voice mailboxes. The Administrator can program corporate call flows which are applied to line groups, and can also add, modify and delete personal call flows.

Call flows actions direct NuPoint Unified Messaging to:

- Play a message,
- Perform a call transfer (blind, supervised, or screened) to an extension or external phone,
- Forward a call to a specified voice mailbox,
- Send a page or a text message,

- Send the caller to the dial-by-name application, or
- Hang up.

Without Call Director, NuPoint Unified Messaging simply sends an incoming call to the called person's voice mailbox.

There are two types of users associated with Call Director: Regular and Advanced.

A **Regular user** is defined as a user who has an LCOS assigned to the mailbox with a template assigned to the LCOS. A Regular user has the ability to customize an assigned call flow through the Web View interface.

An **Advanced user** is defined as a user who has an LCOS assigned to the mailbox with no template assigned to the LCOS. An Advanced user can create a call flow from scratch through the Web View interface.

The Call Director functionality includes a set of templates that can be assigned to a mailbox or line group. There are two sets of templates: system templates and user-defined templates.

Note:
Only System Administrators are able to assign templates to LCOS or LCOS to mailboxes. Advanced users can use an existing template as the start of the creation of a call flow.

There are five system templates provided with the Call Director functionality. These templates can be used as a starting point when creating a call flow. Additional templates may have been created by the System Administrator and are also available for the call flow. See Starting with a template to use an existing template for your call flow.

Refer to the Call Director Templates section of the *Web Console Help* for more information about creating, editing, deleting, importing and exporting templates.

Call Flow Reports can be generated from the **Reports** menu of the call flow page. The Call Flow Report contains records of each call and how it was handled.

See:

About Call Flow Reports

Viewing a Call Flow Report

Resetting a Call Flow Report

Managing Call Director Settings

The global configuration settings and call flows for users and line groups are now managed through the Web Console interface. Refer to the Call Director section of the Web Console Help for more information on managing Call Director settings.

26.144 About the NuPoint UM Documentation Suite

To access the NuPoint Unified Messaging (UM) guides (in .PDF format) and the System Administration Help file, go to Mitel Document Center and log in. You must be a registered user to access Mitel Online.

The NuPoint UM documentation set includes the following components:

General Audience

General Information Guide:

- This guide includes general information on systems architecture, resiliency, feature descriptions, licensing, and geographic availability and provides an overview of administration and maintenance.

Installers

Technician's Handbook:

- This guide includes information on hardware and software requirements, platforms and configurations, installations, basic maintenance, upgrades, data migration, configuring MSL, and trouble shooting systems and features.

Engineering Guidelines

- This guide includes information on system capacities, system requirements, and network engineering.

Administrators

System Administration Help (includes Call Director for the Administrator):

- The help file incudes information on post-installation instructions, system administration and maintenance, configuring and managing NuPoint UM and optional features, and troubleshooting Advanced UM.

End Users

Web View Help

- This Help file includes information on the features that are available to users through the web client interface. It includes configuration information for end user settings and describes unified messaging features.

Messaging User Guide

- This guide includes information on setting up and using voice mailboxes, managing voice and email messages, using PCs to receive and manage messages, and the record-a-call, fax, and speech auto attendant features.

Call Director Web Help

- This help file includes information on configuring automated attendant call flows to handle your calls when you can't answer them personally.

Mitel TUI Quick Reference Guide

- This one-page document explains how to access voice mailboxes and identifies telephone user interface (TUI) main menu options.

Mitel Online

All Mitel product documentation is available at Mitel Document Center.

Accessing Documents and Help Files

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Product Documentation**.
3. In the right pane, select **Product Documentation**.
4. Point to **Messaging** and click **NuPoint Unified Messaging**. A list of documents intended for System Administrators is displayed.
5. Select a document from the list or select **Show End User Documents** or **Show Archived Documents** to access end user or archived documents.

26.145 What's New in This Release

MSL Release 11.0

MSL Release 11.0 provides the following new features:

- The server manager **Shutdown or Reconfigure** panel has been renamed to **Shutdown or reboot**. The Reconfigure option in that panel has been removed.
- The server manager **Web Server** panel has a field for entering Subject Alternate Names (SANs) for the server, when generating a Certificate Signing Request.
- The server manager **Hostnames and addresses** panel does not comprise invalid host names section, and the **Review configuration** panel does not comprise server names section such as mail.domain, ftp.domain, www.domain, and so on.
- When running MSL on EX platform, the option to restore from removable media or another running server are not available.
- MiCollab and MBG supports licensing through the Licenses & Services Application (SLS License Server). The Mitel Licenses & Services Application manages the software licensing and entitlement of the Software Assurance Program. After you obtain a ServiceLink ID or Serial ID from the SLS License Server, the SLS uses your ServiceLink ID to provide you with access to licenses, software releases, and upgrades.
- To activate an SLS Serial ID the following connections must be allowed through any firewalls.
    - FQDN: sync.sls.mitel.com, Current IP: 18.200.183.29 Port: 22 Protocol: SSH
    - Customer must verify current IP before creating firewall rules as the IP address may be subject to occasional change.

- **Supported Upgrade Methods**: MSL 11.0 is available only as a 64-bit distribution. Migration from a 32-bit to a 64-bit system requires a fresh software installation, either manually or using the new Remote Fresh Install blade.
- The application blade software is no longer downloaded from the AMC but the AMC still provides software licensing. MSL 11.0 uses the Mitel Software Download Center, supported by a global content distribution network to increase speed and reliability of downloads. The following outbound connections must be allowed through your firewall: License entitlement: register.mitel-amc.com 216.191.234.91 port 22 sync.mitel-amc.com 216.191.234.91 port 22 Access token for content delivery network: swdlgw.mitel.com 99.81.17.20 port 443 (occurs during available blade software list update) Content delivery network for blade software download: swdl.mitel.com port 443 (IP address based on location)
- Note: For the Akamai FQDN swdl.mitel.com, the static IP address ranges cannot be guaranteed by the Content Delivery Network. Thus, any firewall rules should allow the FQDN. The following table outlines the supported upgrade methods: Upgrading from… Upgrading To... Supported Upgrade Methods 10.x releases (32-bit or 64-bit) 11.0 (64-bit) Fresh Install from CD/DVD/USB Remote Fresh Install 9.x releases (32-bit) 11.0 (64-bit) Fresh Install from CD/DVD/USB Cloud Platform Support: The following features are supported on the Azure platform: Hostname: The default hostname will be the lower case VM name. Any invalid hostname characters, such as periods or underscores, will be translated to hyphens Networking: MSL supports auto-provisioning of network elements, such as NICs, public/private IP addresses, gateways, routing and DNS On every reboot, which includes following a restore operation, the VM networking is analyzed and auto-provisioned if any changes are detected. Supports auto-registration of the VM hostname in a private DNS zone linked to the virtual network of the primary (first) NIC. Only the primary (first) private IP linked to the NIC is registered. So, if the configuration console changes the hostname, the private DNS entry will be updated accordingly when the reboot occurs. Supports custom data when creating a VM. Note:Refer to Cloud Platform Support in the Mitel Standard Linux Installation and Maintenance Guide for more information. Backup and Restore using AWS S3 buckets: Now, backups to the network file server and restoration of the backed up files stored in the network File Server can be processed using HTTPS through Amazon Web Services Simple Storage Service (that is, AWS S3). Note: Refer to Backup and Restore topics for more details.

26.146 About the Call Flow Page

A call flow is created by combining call-processing actions. These actions are executed when a call is directed to a mailbox or line group. The programming of the action determines if and how the call is treated.

The following call flow actions are available:

- Override
- Schedule
- Message
- Menu
- Blind Transfer
- Supervised Transfer
- Screened Transfer
- Alternate Transfer
- Voicemail
- Dial-by-Name
- Internal/External call handling
- Caller ID
- Daily Greeting

- Message Center

Most actions have a *result*. For example, a Supervised call transfer (the action), has three possible results depending on whether the destination receiving the transfer is busy, not answering, or does not exist. A Blind call transfer action on the other hand has no result because it doesn't matter whether the call succeeds (i.e., is answered by the call flow owner) or fails (i.e., is not answered by either the call flow owner or the call flow owner's voice mailbox).

Parts of the Call Flow Page

The Call Flow page is divided into three main windows: Call Flow Display, Properties, and Results.

Call Flow Display

This window displays the current structure of the call flow, showing how the results of each action flow into subsequent actions.

You can click on an action to select it and view its assigned properties and results.

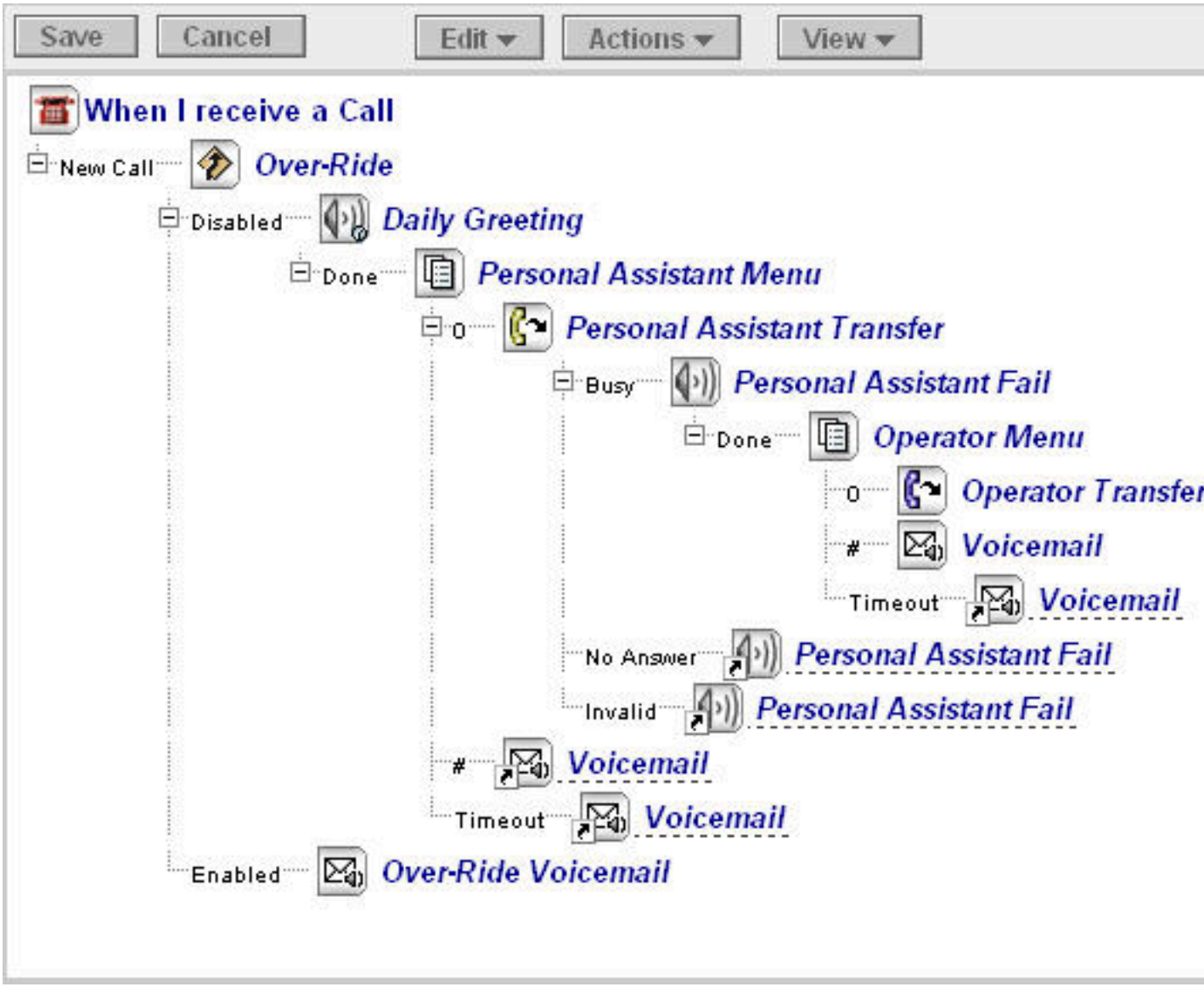
You can expand and collapse the branches of the call flow by clicking on the **+** and **-** signs on the left of the call flow tree.

Note: When an action is used more than once in a call flow, each subsequent instance is an *alias* of the original. Aliases inherit the properties of the original and are identified by an underline.

To create a call flow with multiple instances of an action, each with unique properties, assign the actions different names.

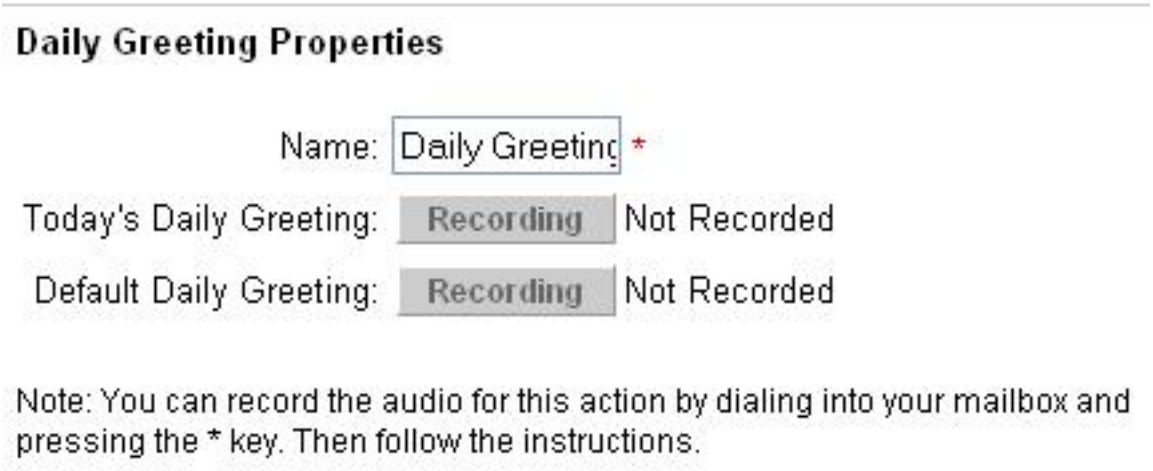
A set of menus at the top of the call flow page allows you to perform such tasks as editing the call flow, recording greetings, or viewing reports.

Note:
These menus change depending on the type of user privileges that are assigned to your mailbox.



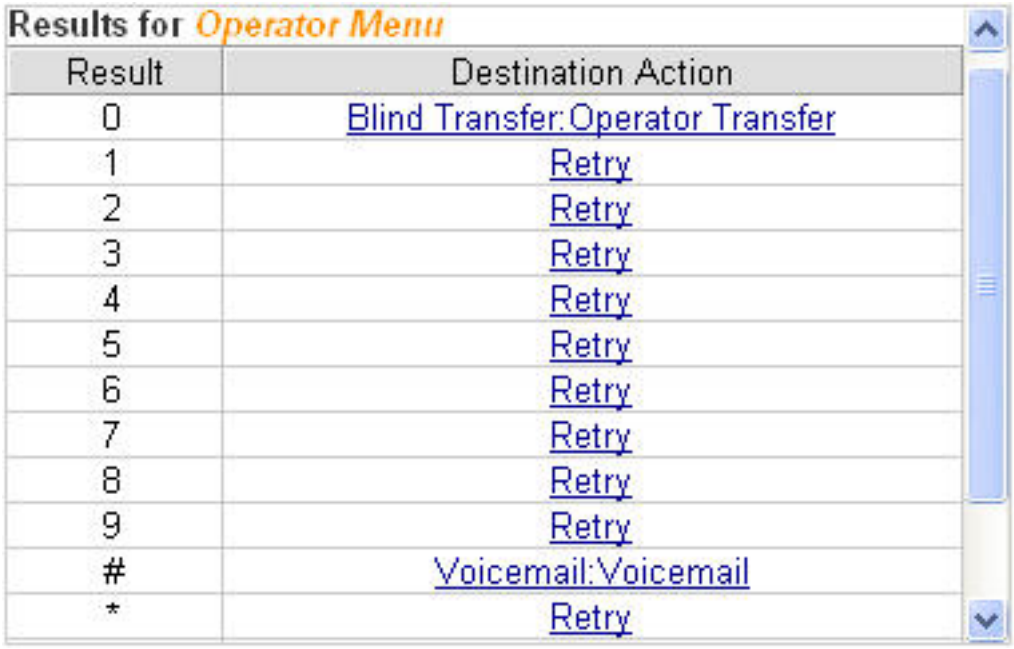
Properties

The properties belonging to the selected action are displayed and modified in this window. All actions have a name property, followed by a set of action-specific properties.



Results

This window displays the results for the selected action in the Call Flow and links for changing the results. Modifying action results here causes the call flow display to update to reflect the new flow.



26.147 About the Configuration Page

The Configuration page contains a number of Global settings that you can alter to control the behavior of individual call flows. For instance, you set call transfer sequences, valid extension lengths, and the destination for calls transferred to the attendant.

The Global settings govern the operation and programming of all newly created unmodified call flows. Unless the Administrator intentionally modifies a specific call flow, the entries in the Configuration page

govern that call flows's **default** settings. Any changes make to these settings in individual call flows always supersede the Global settings.

To open the Configuration page:

- In the navigation tree, click **Call Director**, and then click **Configuration**.
- Select the Line Group to configure and click **Edit**.

After making changes on this page, ensure that you click **Save** to save them.

The following table lists the call flow parameters that you can manage on the Configuration page:

Parameter Name	Value (default = bold)	Description
GENERAL PROPERTIES		
Attendant Extension	0	Specifies the extension of the local attendant. This parameter is used for call transfers where the user has specified the attendant's extension as the call transfer destination. Change this value only if your main attendant's extension is other than "0".
DTMF Timeout	5	Specifies the length of time a caller has to press keys for a Menu action.

Parameter Name	Value (default = bold)	Description
Loop Count	10	Specifies the maximum number of times an action in a call flow can be re-entered during the call. After the maximum number is exceeded, the call is disconnected. A simple example of a loop is when a Menu action includes an option to repeat the menu prompts. The key the repeats the prompts can only be pressed the number of times set for Loop Count, at which point the call will automatically disconnect.
Max. Extension Length	4	Specifies the maximum number of digits that a mailbox extension can contain.

Parameter Name	Value (default = bold)	Description
Menu Dial Plan	vvvvvvvvv	Specifies the global dial plan for all menu actions in all call flows. The dial plan must always contain 9 character positions. The positions correspond to the leading DTMF digits 1 to 9. The value in each position represents the total number of digits that will be collected when that leading digit is pressed (including the leading digit itself). A 'v' in any position means that the number of digits collected in total or to follow is variable. The Maximum Digit and Timeout properties for the menu govern when digit collection stops. For example, the dial plan vv4vvvvvv means that for leading digit 3, four digits will be collected in total (including the leading digit 3), and for leading digits 1,2,4,5,6,7,8,and 9 the number of digits to follow is variable. Leading digits *, #, and 0 always permit a variable number of digits to follow, and so they are not represented in the dial plan.
Time Until No Answer	20	Applies to transfer sequences that tell Call Director to supervise the call for answer. Call Director waits the indicated number of seconds before reconnecting the caller if the called number does not answer. Maximum is 60 seconds. The Time Out setting for an Alternate Transfer overrides this Time Until No Answer setting.

Parameter Name	Value (default = bold)	Description
Forward Override FAC	n/a	This is the Feature Access Code (FAC) that is programmed into the PBX to override forwarding. Call Director will use this value when performing a supervised or screened transfer to a phone from a call flow. If this value is not set, then the transfer target may forward calls due to a busy or no-answer condition, and Call Director will not be able to pull the call back for continued processing of the busy or no-answer condition in the call flow. This setting is only applicable to NP-UM systems that are integrated with Mitel MiVoice Business series PBXs. The value in the Call Director configuration must match the FAC setting in the MiVoice Business PBX, and all networked PBXs must have the same setting. Furthermore, the MiVoice Business Class of Service applied to the NP-UM ports must have Call Forward Override enabled.

Parameter Name	Value (default = bold)	Description
Hook Flash FAC	n/a	This is the Feature Access Code (FAC) that is programmed into the PBX to perform a single trunk flash. Call Director uses this value to initiate a hook flash on an outgoing trunk. The value that you enter in this field is the FAC programmed on the MiVoice Business ICP PBX to perform a single trunk flash (Trunk Single Flash). **Note**: In general, the NuPoint Unified Messaging system does not support Feature Access Codes (FACs). The exceptions are "Forward Override" and "Hook Flash", which NuPoint supports in Call Director only.
TRANSFER SEQUENCE PROPERTIES		
Reconnect Reject	NS	When a screened call is rejected by the called party, reconnect the original caller with this transfer sequence. The sequence is comprised of characters from the Dial String Table. The default (NS) = start a new activity without going off-hook, and then perform a switch hook flash, no wait required.

Parameter Name	Value (default = bold)	Description
Supervised Transfer	S+XG	When transferring a call to another number, and answer supervision is required, use this transfer sequence. The sequence is comprised of characters from the Dial String Table. The default (S+XG, where X is the target extension of the call flow) = Switch hook flash, call target extension, wait for for a voice or computer tone answer.
Attendant Transfer	S+X	The transfer sequence used when transferring a call to the Attendant. The sequence is comprised of characters from the Dial String Table. The default (S+X where X is the attendant extension) = switch hook flash, call the attendant.
Reconnect Busy	NS	When a transfer to a number encounters a ring-no-answer, reconnect the original caller with this transfer sequence. The sequence is comprised of characters from the Dial String Table. The default (NS) = start a new activity without going off-hook, and then perform a switch hook flash, no wait required.

Parameter Name	Value (default = bold)	Description
Blind Transfer	S+XH	When transferring a call to another number, and no answer supervision is required, use this transfer sequence. The sequence is comprised of characters from the Dial String Table. The default (S+XH where X is the target extension of the call flow) = switch hook flash, call target extension, hang up.
Reconnect Invalid	NS	When a transfer to a number encounters an invalid tone, reconnect the original caller with this transfer sequence. The sequence is comprised of characters from the Dial String Table. The default (NS) = start a new activity without going off-hook, and then perform a switch hook flash, no wait required.
Reconnect RNA	NS	When a transfer to a number encounters a ring-no-answer, reconnect the original caller with this transfer sequence. The sequence is comprised of characters from the Dial String Table. The default (NS) = start a new activity without going off-hook, and then perform a switch hook flash, no wait required.

26.148 Finding online Help Quickly

This online Help system provides you with a number of ways to find information quickly:

To search	Use this feature
By topic	The Contents function takes you directly to the information you need. This function provides you with a complete list of the main topics in the online Help system. To open a book in the list, double-click the book. To choose a topic, click the topic name. When you click a topic in the list, the online Help system takes you directly to the relevant information.
By word or phrase	The Search function is a handy feature for finding a particular word or phrase across all topics in the online Help system. To access the Search function, click Search, and then enter and word or phrase that relates to the subject you want more information about. The Search function will then link the subject you've specified to the relevant topic(s). At this point, you can select the topic that's most likely to have the information you're looking for. This may be the quickest way to find the information you need.
By index	The online Index works like an index in a book, except it's faster! To look for an entry in the online Index, click Index, and then enter the word you're looking for into the text box that appears just below Index. As you type, matching entries will be highlighted. To see the corresponding information, click on the corresponding topic that appears.

26.149 Accessing Documentation, Release Notes, Articles, and Downloads

The following sections detail how to access specific NuPoint UM documents from Mitel Document Center.

Documents and Help Files

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Product Documentation**.
3. Click the **Product Documentation** link.
4. Point to **Messaging** and click **NuPoint Unified Messaging**.
5. A list of documents intended for System Administrators is displayed. Select a document from the list or select **Show End User Documents** or **Show Archived Documents** to access end user or archived documents.

The Qualified Hardware List

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Product Documentation**.
3. Click the **Product Documentation** link.
4. To search for a document, press **CTL + F**.
5. To access the Mitel Standard Linux Qualified Hardware list, type **MSL** in the **CTL + F** search box.

Product Release Notes

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Mitel Knowledge Base**.
3. Click **Mitel Knowledge Base**.
4. In the **Product** list, select **Mitel NuPoint UM IP** (Standard Edition).
5. Under **Article Type**, select **Release Notes** and click **Search**.

Knowledge Base Articles

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Mitel Knowledge Base**.
3. Click **Mitel Knowledge Base**.
4. In the **Product** list, select **Mitel NuPoint UM IP** (Standard Edition).
5. Under **Article Type**, select the type of article to be viewed.
6. Specify other search parameters to narrow your search and click **Search**.

Software Downloads

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Software Downloads**.
3. Select the appropriate Mitel NuPoint UM link.
4. Click the download link for your selected release and follow the instructions on the software download page.

26.150 Contacting Mitel

Mitel Networks Corporation

World Headquarters

350 Legget Drive

Kanata, Ontario

Canada K2K 2W7

Telephone: 613-592-2122

Fax: 613-592-4784

Internet: http:// www.mitel.com

26.151 Disclaimer, Trademarks, Copyright

Disclaimer

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

NuPoint Unified Messaging is a trademark of Mitel Networks Corporation.

Mitel is a registered trademark of Mitel Networks Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Copyright

®, TM Trademark of MITEL Networks Corporation

© Copyright 2019, MITEL Networks Corporation

All rights reserved

26.152 Personal Call Flow Example

Penny Graham is a sales manager at ACME Widgets. She travels frequently and is rarely at her desk. When she happens to be in the office she is normally on the phone. Her phone (extension 1234) is forwarded to her voice mailbox if she does not answer or is on another call. Penny's specific call handling requirements are as follows:

Penny's Requirements

1. If I am temporarily out of the office or I am traveling, tell callers to press a key to transfer to John, my secretary. If he doesn't answer his phone, he may be out too, so put the caller into my voice mailbox. If he is at his desk but his phone is busy, put the caller into his voice mailbox. He will get the message faster than I will.
2. Sometimes, I need to be reached at home, but I don't want to give out my home number. If someone calls my extension and I don't answer, let them press a key that will transfer them to my home number. I only want people to try me at home until 11:00 P.M. Mondays through Thursdays. Don't let anyone call me on Friday nights. Saturday and Sunday during the day are OK.
3. Whenever I am paged because someone has left me a message, first I have to make a call to my voice mailbox to find out who called, then I have to place another call once I have their return phone number. Just let people page me directly and enter their callback numbers so I don't have to keep calling my mailbox. Of course, you should never tell a caller my pager number.

4. Sometimes, even when I'm on the road, people need to talk to me live. I don't always get around to checking my messages. Is it possible to set something up so that I can enter the telephone number of the site I'm at and have my calls transferred there? Then, I can just record something like "To reach me while I'm on the road, press [5]." (P.S. I' ll need to be able to change the telephone number from wherever I am.)
5. Sometimes I can't be interrupted by phone calls if there is a crisis. I' ve tried forwarding my phone to voice mail, but if my children call they won't be able to get through. Isn't there a way that I can let some people ring my extension and not others?

Penny's Call Flow Solution

Here is Penny's Call Flow:

"Hello. This is Penny Graham. I'm not available right now, your call is important to me.

To speak with John, my secretary, press [1];

To leave me a voice message, press [2], or stay on the line. *If you would like to speak with an operator, press [0] at any time.."*

Both internal and external callers will hear this recording. However, some of Penny's colleagues know that they can press 8 (not mentioned in the recording) for additional options:

"Hello. You have reached my personal call list.

To transfer to my pager, press [2] and enter your callback number;

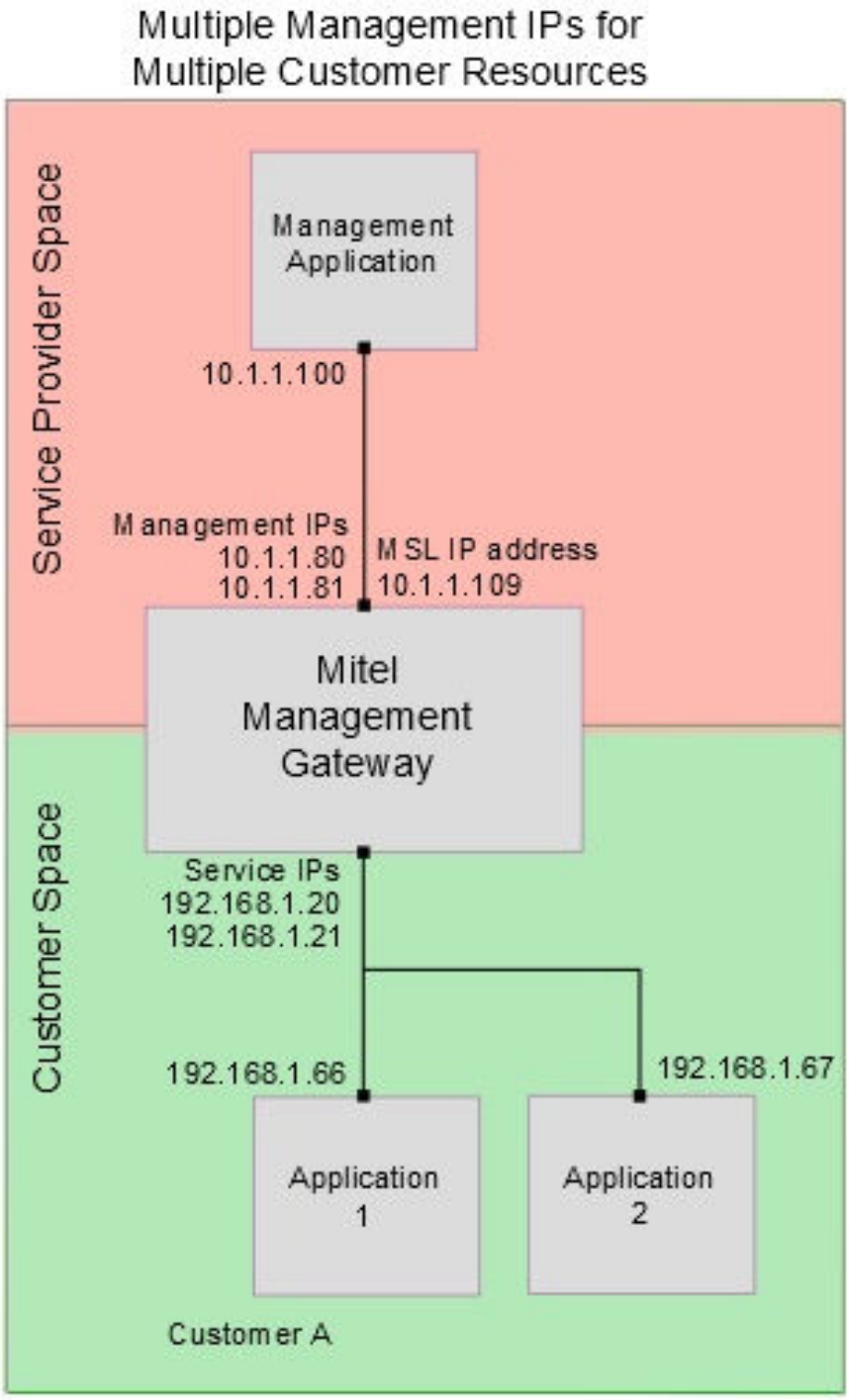
Stay on the line or press [0] to leave me a voice message."

In this example, callers dialing Penny's extension number are forwarded to NuPoint Unified Messaging if she is on the phone or does not answer. Instead of going directly to her voice mailbox, callers reach Penny's Call Flow. This gives callers the opportunity to try to speak with someone else (always a good alternative) rather than forcing everyone to either hang up or leave a message.

Penny has complete control over who can reach her and when. She can be accessible to her colleagues at the time and days of her own choosing, and still keep her home and pager numbers private.

Penny recorded a greeting ("Hello. This is Penny Graham. I'm not available right now..."), and a menu ("To speak with John, press [1] ...") in her own voice. She (or the NuPoint Unified Messaging Administrator) programmed each key to transfer to a specific extension, outside telephone number, pager number or voice mailbox. A schedule was also set up so that she would not be disturbed at all hours. To address her occasional requirement that she not be interrupted by phone calls unless they are from her kids, an override was put in that permits only calls from selected numbers (home and school for example) to ring her phone.

Show Penny's Call Flow



Explain how the Call Flow works

The following explanation should help you visualize a caller's path through a personal call flow. The call flow handles incoming calls directed to Penny's voice mailbox. It includes 12 unique actions in the order in which they are executed.

Call Flow Sequence

When a new call arrives, check the **Override** setting to see whether it is enabled or not.
If Override is enabled, perform a Supervised Transfer to Secretary (John).
If the Override is disabled, evaluate Penny's **Schedule** settings.
During off-hours, send the call to My Voicemail.

During on-hours, play the caller Penny's greeting message (**My Greeting**):

"Hello. This is Penny Graham. I'm not available right now,

but your call is important to me."

Then play the **Main Menu**:

"To speak with John, my secretary, press [1];

To leave me a voice message, press [2], or stay on the line.

If you would like to speak with an operator, press [0] at any time.."

Key [1] does a Supervised transfer to John's extension. John's extension is not call-forwarded busy or no-answer, so Penny's call flow can control the transfer. On a busy or no-answer at 5678, Call Director hook-flashes to get the caller back and moves the caller either into mailbox 5678 (busy) or 1234 (on a no-answer).

Key [0] transfers to the operator.

Key [2] or remaining on the line moves the caller to Penny's voice mailbox

Penny's staff knows to press [8] if they really need to reach her. Key [8] moves the caller to Penny's **Personal Call List Menu**:

"Hello. You have reached my personal call list

To try and reach me at home after hours, press [1];

To transfer to my pager, press [2] and enter your callback number;

If I'm traveling, and it's important that you reach me directly, press [5]

Stay on the line or press [0] to leave me a voice message."

Key [1] transfers to Penny's home phone number. NuPoint Unified Messaging automatically performs a hook switch flash to get dial tone, dials 9, pauses one second, the dials the number. The call is supervised for 20 seconds (Penny's home answering machine picks up calls after 25 seconds). If Penny's home phone rings no answer, or is busy, the caller is reconnected and continues in the call flow to hear the menu again (retry count is set to 5). This way the caller can try another option on the same phone call.

Notice the small arrow at the bottom left of the My Voicemail icon,  . This is called an alias and it means that the No Answer result of the supervised transfer goes to the same Voicemail action as the Off-hours result of the schedule action. You will normally see many aliases throughout a call flow when more than one action result leads to the same subsequent action.

Key [2] transfers the caller to Penny's outside pager number. NuPoint Unified Messaging performs a switch hook flash, gets a dial tone, dials 9 (for an outside line), pauses one second, then dials 1-800 and the pager number (789-1234). After the pager number answers, the call box connects the caller directly so that he or she can enter their callback number.

Key [5] transfers the caller to outside telephone numbers, which change as Penny travels.

Key [8] transfers to 8234, a secondary line appearance on Penny's telephone. Even when her primary extension number 1234 is forwarded to voice mail, her secondary extension will ring. This is how her children can reach her when she doesn't want to be bothered. Key 8 is not mentioned in the recording. To prevent just anyone from pressing 8, set up Caller ID to allow calls from Penny's home. To stop calls to her prime number from ringing her phone, she has to temporarily call forward always to voice mail.

26.153 Corporate Call Flow Example - Main Auto Attendant

ACME's Vice President of Voice Services submitted the following list of requirements for ACME's main automated attendant application:

ACME Main Automated Attendant Requirements

1. Anyone calling our main telephone number should be greeted with a short, professional recording telling the caller to dial an extension or to press a single key for the Sales, Shipping or Accounting departments. If the call is from a rotary phone, send them to the operator as quickly as possible.
2. If they do not know the extension number, allow the caller to spell out the person's name to find the extension number. The President and I do not want, under any circumstances, a caller to be able to find out what our extension numbers or voice mailbox numbers are. Incidentally, anyone dialing either extension should be routed to our respective secretaries.
3. Anyone calling a Department's main number directly should reach that department's automated attendant. (I don't want to have to dedicate lines in the system for this.) You should know that the Shipping department is working two shifts, including a full night shift on Sundays. Their auto-attendant should reflect this fact. Also, Accounting doesn't take outside calls on Wednesday afternoons.
4. I want a year's worth of holidays pre-programmed in the system at all times. Each holiday should have its own special cheery recordings.
5. If something happens, such as a major snowstorm, I want you to be able to change our main automated attendant from your home, so we can tell callers that no one will be in the office and the company is closed.
6. I want to be able to find out if a particular person is answering calls when they are supposed to be available... or if they are skipping out early every day. Give me statistics on this.

Auto Attendant Call Flow Solution

The NuPoint Unified Messaging Administrator designed the following solution:

"Thank you for calling ACME Manufacturing.

If you know your party's 4 digit extension number, you may enter it now or at any time during this message. To use Dial-by-Name, press [8].

For Sales and Marketing, press [1];

For Shipping, press [2];

For Accounting, press [3];

If you wish to speak with the operator, press [0], or stay on the line."

A caller pressing 2 would hear the Shipping department’s automated attendant greeting:

"Thank you for calling the ACME shipping department.

To check on the status of your order, press [1];

For new orders, press [2];

To report shipping discrepancies, press [3], or stay on the line."

The Shipping department’s automated attendant greets callers through two shifts of the day. Callers dialing Shipping’s direct outside number still reach this recording.

Accounting also has a direct outside number. Callers reach the same recordings when they press 3 from the ACME main automated attendant, or when they dial Accounting directly.

"You have reached the ACME accounting department.

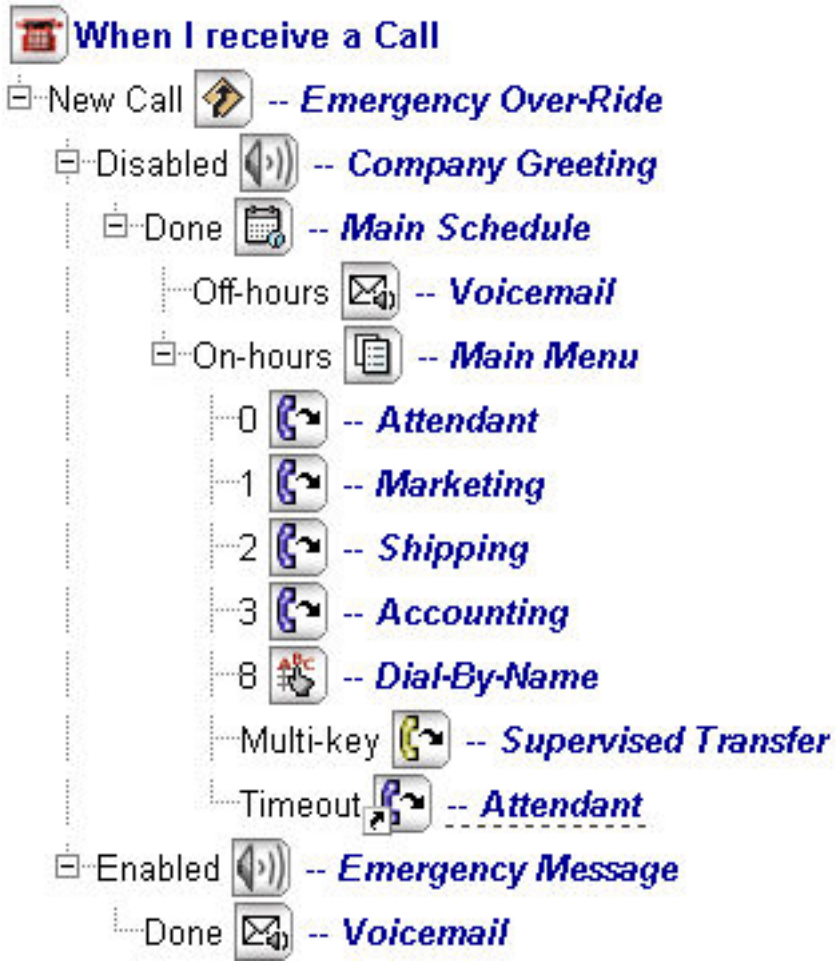
For Accounts Payable, press [1];

For Accounts Receivable, press [2];

For all other inquiries, press [0], or remain on the line."

All of the power, flexibility and features available at the organization’s NP-UM Agent application are also available to every department, extension or mailbox within the organization. This is because all NP-UM Agent applications are built from combinations of the same basic building block -- the call box.

Show the Main Auto-Attendant Call Flow



Explain how the Call Flow works

The example below should help you visualize a caller's path through a call flow. The call flow handles incoming calls to ACME on Line Group 10. It includes three actions in the order in which they are executed.

Call Flow Action	Action Description
Override	(If activated.) Send all calls to my secretary. Don't bother with the rest of this call flow.

Call Flow Action	Action Description
Schedule (Main)	Holiday Schedule Check to see if today is an observed Holiday. If it is, route call through the holiday's call flow. Otherwise, continue to next node. Weekly Schedule Between 9:00 AM and 5:00 PM, Monday through Friday, continue to the next node in this call flow. After 5:00 PM and on weekends go to the Off-hours call flow. Although not shown, the night and weekend mode (voice mailbox xxx) greets all callers with: "Thank you for calling ACME Manufacturing. Our normal business hours are 9 AM to 5 PM Monday through Fridays". The Menu offers callers the following choices: If you would like to leave a message for someone, enter their four-digit extension number. If you do not know the extension number, or are calling from a rotary phone, stay on the line. Callers entering an extension number will be transferred directly to that person's voice mailbox. Key [0] could be assigned to transfer to night bell extension. The recorded menu does not inform the caller of this key. However, any employee of the company can use key [0] to ring the night bell or night station.

Call Flow Action	Action Description
Menu	Play the recorded Greeting and Menu: "Thank you for calling ACME Manufacturing. "If you know your party's 4 digit extension number, you may enter it now or at any time during this message. To look up a name in the company phonebook, press [8]. For Sales and Marketing, press [1]; For Shipping, press [2]; For Accounting, press [3]; If you wish to speak with the operator, press [0], or stay on the line." Key [1] does a transfer to the Sales and Marketing ACD Queue. On a Ring Busy, Ring No Answer, or invalid transfer attempt (which should never happen), the call is reconnected and routed to the Attendant. Keys [2] and [3] route calls to the Shipping and Accounting departments respectively. Callers can also enter a four-digit extension number. The Multi-key action is programmed to Blind Transfer callers to the appropriate extension number. On Ring Busy or Ring No Answer at the dialed extension, the caller is routed to the corresponding voice mailbox to leave a message. Callers wish to Dial-by-Name press [8]. If the caller does nothing, (such as, a rotary phone caller) the Auto-Exit transfers the caller to the operator. Key [0] performs the same function.

26.154 System Templates

There are six system templates provided with the Call Director functionality. These templates can be used as a starting point when creating a call flow. The system templates have recorded prompts. These templates are read-only and cannot be changed or deleted.

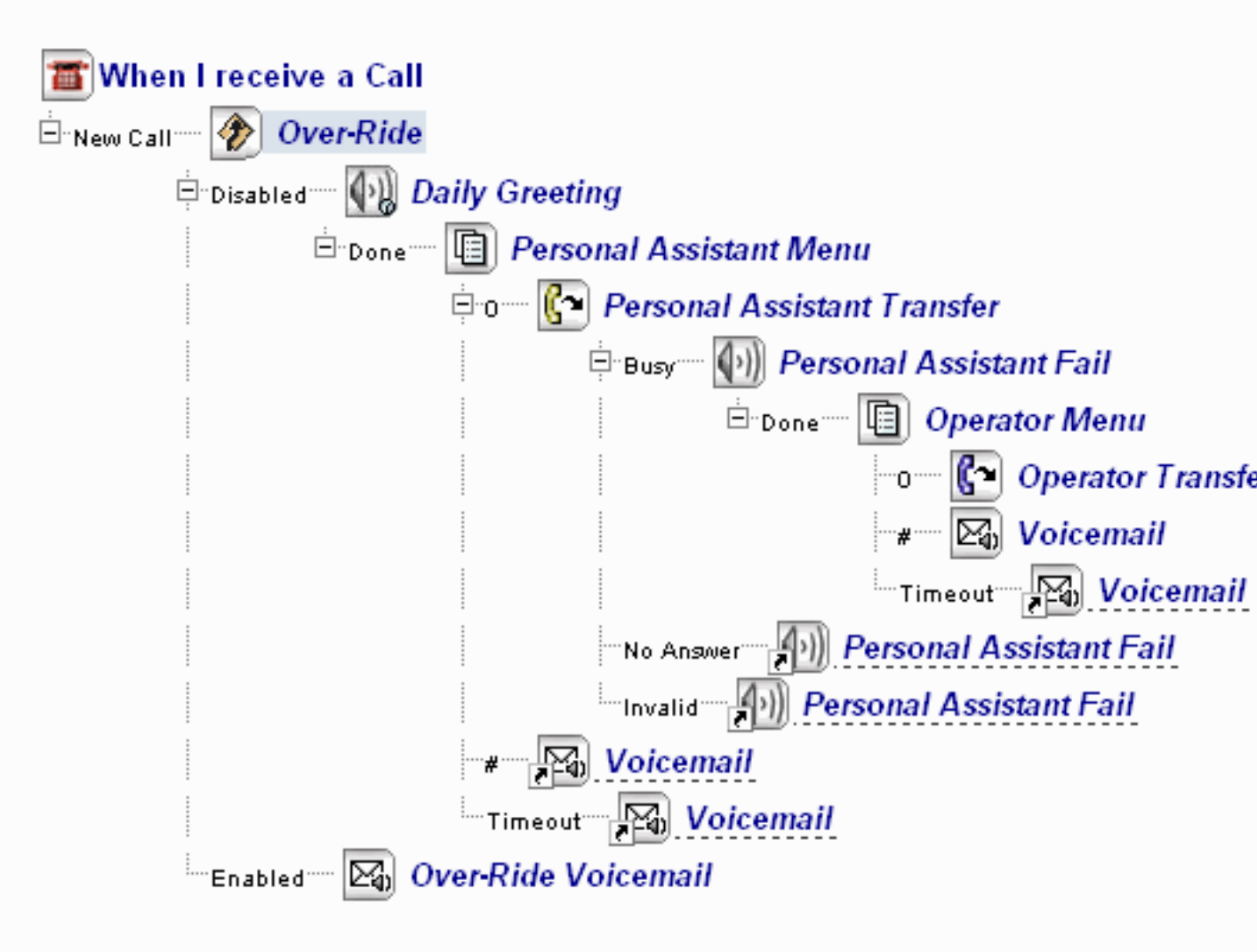
The templates are as follows: Daily Greeting, Follow Me, Find Me, Personal Dial Zero, Alternate Daily Greeting, and NP Receptionist.

The following system templates are provided:

Daily Greeting

The Daily Greeting feature allows users to customize their greeting on a daily basis, with a temporary greeting that reverts back to the user's primary personal greeting at midnight. The Daily Greeting feature is available to all licensed Call Director users.

The call flow for this template is as follows:



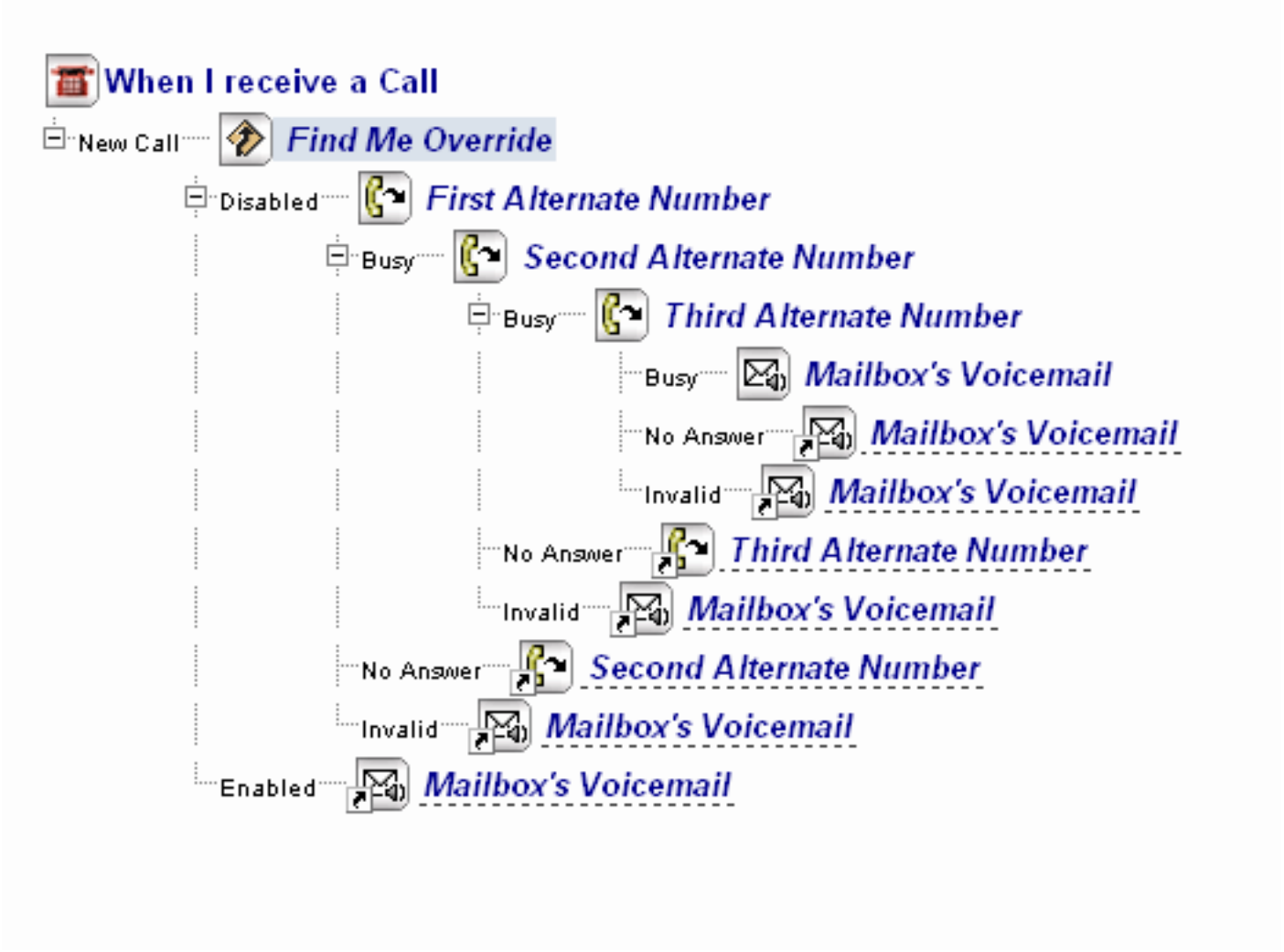
Follow Me

The call flow for this template is as follows:



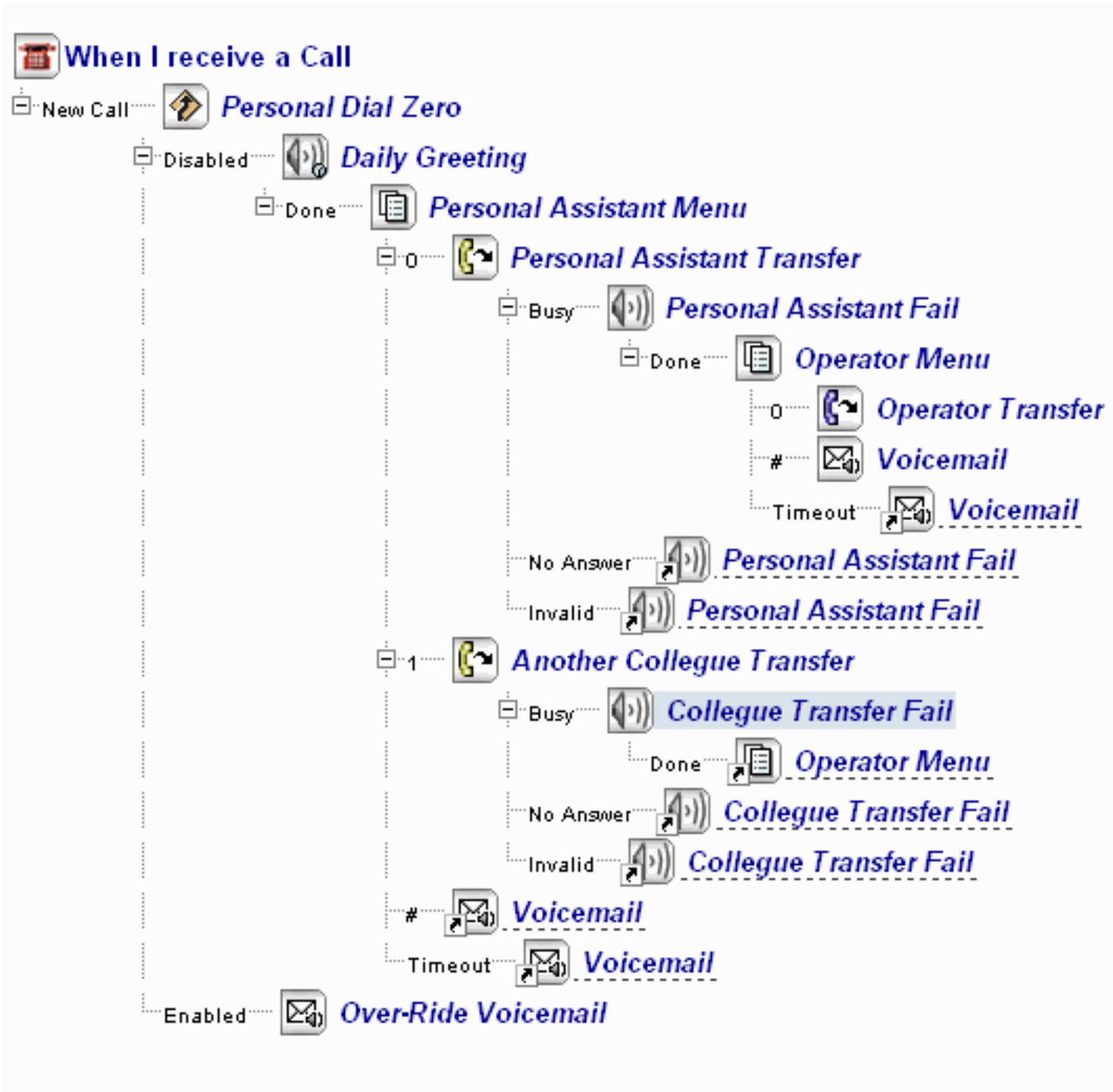
Find Me

The call flow for this template is as follows:



Personal Dial Zero

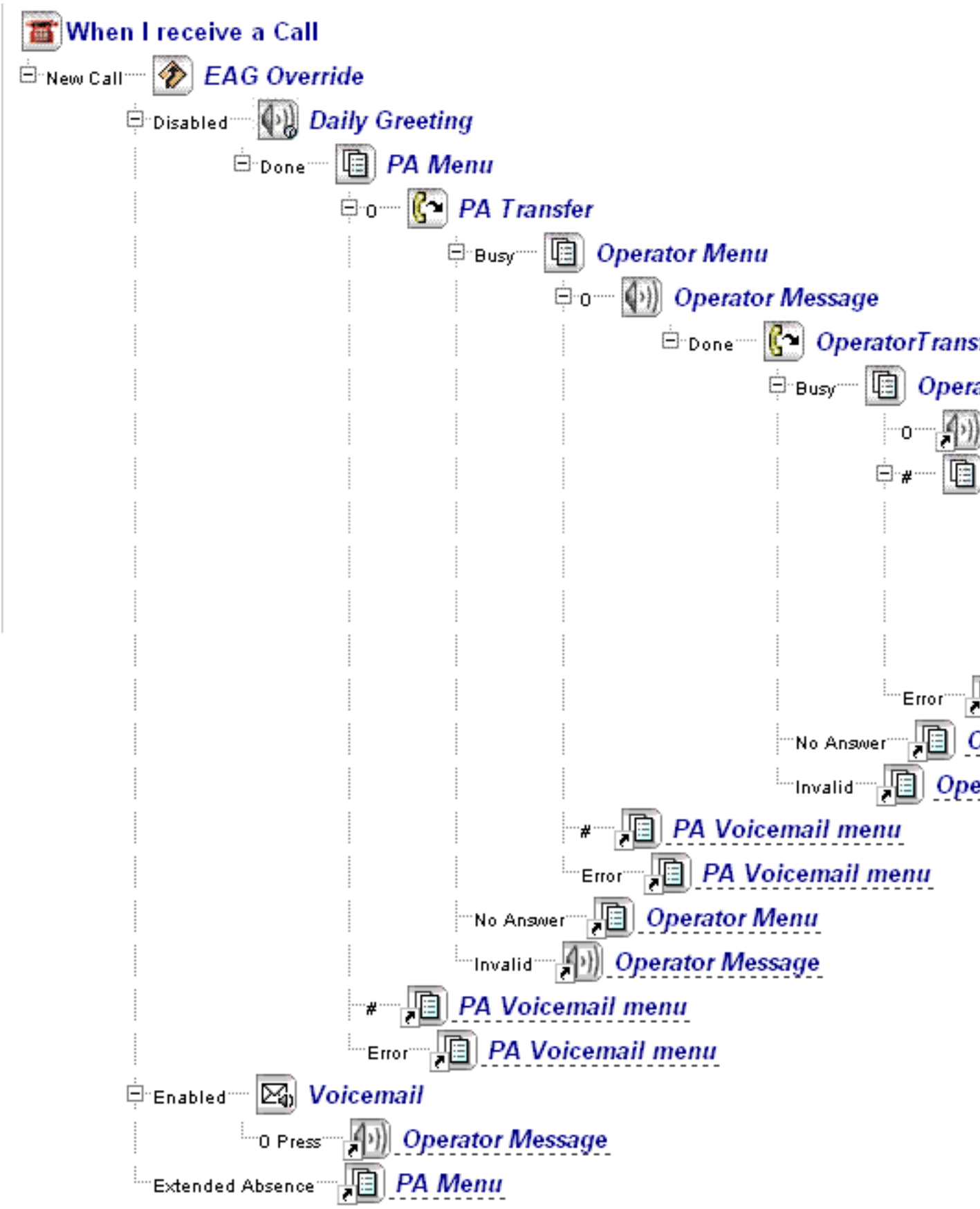
The call flow for this template is as follows:



Alternate Daily Greeting

The Alternate Daily Greeting template allows users to set up a call flow when they are using an Extended Absence Greeting (EAG). The caller hears the greeting advising that the user is away and is presented with alternative options.

The call flow for this template is as follows:


When I receive a Call
New Call
EAG Override
Disabled
Daily Greeting
Done
PA Menu
0
PA Transfer
Busy
Operator Menu
0
Operator Message
Done
OperatorTrans
Busy
Opera
0
#
Error
No Answer
Invalid
Ope
#
PA Voicemail menu
Error
PA Voicemail menu
No Answer
Operator Menu
Invalid
Operator Message
#
PA Voicemail menu
Error
PA Voicemail menu
Enabled
Voicemail
0 Press
Operator Message
Extended Absence
PA Menu

NP Receptionist

The NP Receptionist feature provides the functionality of a simple automated attendant. The template greets the caller, asks for an extension number, and transfers the call to the destination (blind transfer). This feature is available to all licensed Call Director users, but it is optimized for use by administrators.

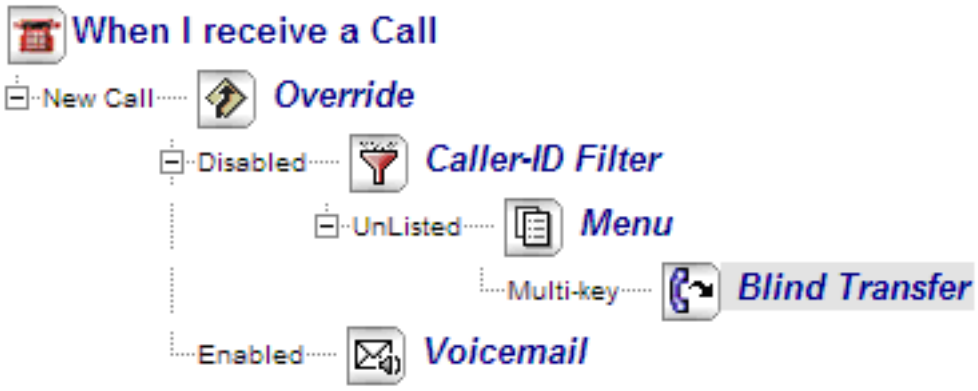
When you configure the actions for this template, note the following:

- **Override**: This action enables/disables the call flow. By default it is enabled.
- **Caller ID**: This optional action handles calls based on whether the caller's number is in your Caller ID list. You can delete this action from the call flow without impacting the operation of the NP Receptionist feature.
- **Menu**: This action causes a recording to play which prompts the caller to press a key to select a menu option. By default, the system plays, "Welcome to the automated receptionist. Please enter an extension number." Note that as part of configuring the Menu action, you must specify the "Maximum DTMF Length," which should match the extension number length for your system.
- **Blind Transfer**: This action dials the destination and then releases the call regardless whether the destination is busy or not answering.
- **Voicemail**: This optional action sends the caller to a NuPoint Unified Messaging mailbox. You can delete this action from the call flow without impacting the operation of the NP Receptionist feature.

Notes:

- The properties of the **Blind Transfer** action default to “Gathered digits” but this property can be modified to “Operator” or “Specified Extension.”
- Dial-by-Name can be configured by adding it to the configuration of the **Menu** action.
- The NP Receptionist template does not support treatment types (i.e. situational call behaviors).

The call flow for the NP Receptionist template is as follows:



26.15 Voicemail RADs

Call Director can provide Recorded Announcement Device (RAD) functionality, eliminating the need for external tape machines or other audio-playing devices.

RADs are commonly employed in ACD environments to automatically answer lines and deliver pre-recorded messages such as, "All of our representatives are busy helping other callers, please continue to hold to maintain your call priority." When the RAD message finishes playing, the caller usually hears music-on-hold while waiting for an agent to become available. RAD messages may also give the caller information, which answers their questions, thus resulting in a 'good' abandoned call. They may also provide advertising or promotional information to callers while they're waiting for someone to take their call.

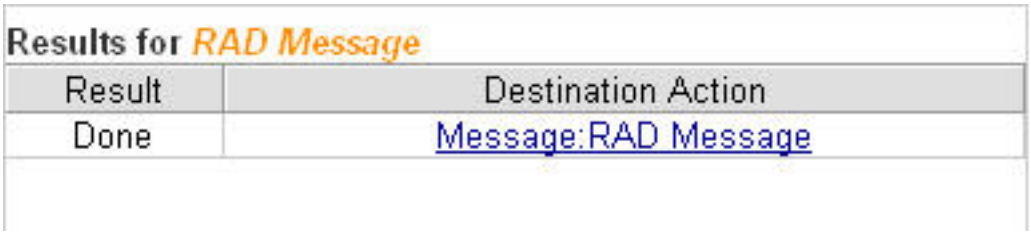
To configure RAD functionality, create a call flow containing any number of Message actions and assign it to a Line Group.

To program a RAD call flow:

1. Access the main Call Director administrator web page.
2. Create a new call flow assigned to a Line Group that will be used as the RAD.
3. Add a Message action node to the call flow.



4. In the **Message** properties, program an appropriate delay for this action.
5. For the **Done** result of the message action, select the **Message** action itself as the **Destination Action**. This creates the loop.



The call flow will look something like the following. Note that the loop is presented as the Message action followed by itself in the form of an alias.



6. Click **Save** to save the call flow.
7. Access the Administrator mailbox and follow the TUI prompts to record the message for this Line Group call flow.
8. Call the line group to test the call flow.
9. Assign the Line Group to the RAD Group of the ACD application.

Note:
In the call flow, add a Message Center action following the RAD Message action node. This prevents the call from being terminated if the user happens to press a TUI key while listening to the recorded announcement.

You need to know

- Selecting the Message action as the Destination Action for itself creates a continuous loop. You can terminate the loop after a number of revolutions by limiting the loop count value for the call flow. The maximum loop count is configured in the >Configuration Page and applicable to all call flows.
- You can “daisy chain” several messages, each with their own delay, and configure the last message return to the first message.
- Ensure that all the IP telephones representing Voicemail RAD ports are registered as 5240 IP devices if Record-A-Call is installed or 5020 IP devices if Record-A-Call is not installed. If you need to re-configure the telephones, reboot NuPoint so that it can re-register its devices.
- To enable callers to press non-numeric DTMF keys such as # and * during playback of the RAD message, ensure that the ACD group interflow paths are configured correctly on the ICP.

26.156 Tutorials

This page provides PDF tutorials with examples of common call flows:

- Personal Call Flow
- Corporate Call Flow
- Holiday Settings Call Flow

26.157 Override

When an Override action is encountered, Call Director checks to see if it is enabled. If it is not, the call flow follows the **Disabled** result. If Override is enabled, Call Director performs the action connected to the **Enabled** or **From Call Flow** results (typically a transfer to another extension, a voice mailbox, or the attendant).

Override can be turned on and off in Call Director or from any DTMF telephone.

Example — Main System Automated Attendant

Calls to the main telephone number for ACME Widgets arrive on lines assigned to Line Group 1 and are answered by the automated attendant. The Call Director Administrator has programmed an initial Override function for this line group to go to the snow emergency closure message. When Override is enabled, instead of hearing the normal automated attendant, outside callers will now hear:

"Thank you for calling ACME. Due to severe weather conditions, our offices are

temporarily closed."

"If you know the extension number of the person you wish to reach, please dial it now and

leave a message. We will return your call as soon as possible. Thank you."

To activate Override, the System Administrator needs only to enable it from any touch-tone phone.

Example — Personal Call Flow

Penny is working late and is expecting an important call. She will be working in the computer room, and overrides all of her calls to go directly to that extension (3456). Upon returning to her own desk, she simply disables Override to return her call flow to normal processing.

The following table lists the configurable properties for the Override action and its possible results:

Item	**Values (default = bold)**	**Description/Notes**
PROPERTIES		
Name	<user-definable> Override	Changing an action name renames all aliases of the action.
Override Enabled	Disabled	Indicates whether Override is enabled or disabled. When it is enabled, the result is based on either EnabledEnabled or From Call Flow.
Action ID	--	A system-generated three-digit ID used to identify this action when enabling or disabling it by telephone.
RESULTS		

Enabled	Message Center	The action taken when Override is enabled AND the call has been forwarded to your call flow by your extension. The default is *Message Center*, which plays a system message and then disconnects the call. When Override is enabled, it has priority over the other results.
Disabled	Message Center	The action taken when Override is disabled. The default is *Message Center*, which plays a message that you have pre-recorded and then disconnects the call.
From Call Flow	Unassigned	The action taken when Override is disabled AND the call has been transferred to your call flow from another call flow, as a Transfer or Voicemail action. The default is *Unassigned*, which means that for an incoming interflow call, the Disabled result is followed.
Extended Absence	Unassigned	The action taken when Override is disabled, after the Extended Absence Greeting is played. The default is *Unassigned*, which means that after playing the EAG, the Disabled result is followed.

Programming an Override Action

To program the Override action:

1. Access the Call Flow page.
2. Do one of the following:

1. • For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   • For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.

1. Add the **Override** action to the call flow.
2. Under **When I receive a Call**, click the **Override** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
3. Enter or modify the property as needed. For information about the properties, see the table above.
4. Assign actions as required to the Enabled and Disabled results from the call flow and/or Extended Absence if applicable.
5. Click **Save**. The call flow is saved.

26.15.8 Schedule

The Schedule action alters the call flow based on the user's weekly schedule and, optionally, on the user's holiday schedule.

The Weekly Schedule checks the time-of-day and day-of-week of each call. It then redirects the call according to the programmed Call Flow Action for that time and day. For example, a call flow owner can have all calls ring his extension during normal working hours, Monday through Friday. After hours and on weekends, all calls can be routed to the owner's voice mailbox.

The Holiday Schedule checks the time-of-day and day-of-year of each call. If the call falls within a predefined Holiday range, Call Director moves the caller to the next action in the call flow for further processing.

A Weekly Schedule can have an unlimited number of time slots, with a minimum one-minute difference required between the set times. For example, the call flow owner can set their work hours for Monday through Friday as 9:00a.m. to 12:00p.m., 1:00p.m. to 2:30p.m. and 3:00p.m. - 5:00p.m.

A call flow can have multiple schedules inserted at any point in the flow.

The following table lists the configurable properties for the Schedule action and its possible results:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Schedule	Changing an action name renames all aliases of the action.
Weekly Schedule	--	Opens a pop-up window for defining work hours for each day of the week. If work hours are not specified, then the call is processed by the on-hours result.

Item	Values (default = bold)	Description/Notes
Holiday Schedule	--	Opens a pop-up window for entering names, dates and times for holidays.
RESULTS		
Off-hours	Message Center	The action taken when the current time is outside of the scheduled time slots. Default is to play an appropriate pre-recorded message, and then disconnect the call.
On-hours	Message Center	The action taken when the current time is within the scheduled time slots. Default is to play an appropriate pre-recorded message, and then disconnect the call.

Note:
The Weekly Schedule and Holiday Schedule are managed by call flow owners through Call Director only.

Programming a Schedule Action

To program the Schedule action:

1. Access the Call Flow page.
2. Do one of the following:
   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
3. Add the **Schedule** action to the call flow.
4. Under **When I receive a Call**, click the **Schedule** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.

5. Do one or both of the following:

   - To configure a weekly schedule, click **Weekly Schedule**. The Weekly Schedule window opens.
   - To configure a holiday schedule, click **Holiday Schedule**. The Holiday Schedule window opens.

6. If the window fails to appear, check to see whether your browser is using a pop-up blocker.
7. Enter or modify the schedule properties as needed. Click **Apply** and then **OK** to save the information, and to return to the Call Flow main page.
8. Assign actions as required to the On-hours and Off-hours results.
9. Click **Save**. The call flow is saved.

26.159 Message

The Message action plays recorded audio, such as a greeting, to callers. Messages play once before moving the caller down to the next action in the call flow.

A greeting message should be short and friendly. ACME's greeting is typical. " *Thank you for calling ACME Widgets*." All outside callers hear this company greeting when dialing ACME's main number. Immediately after the greeting, callers hear the recorded Menu: " *If you know your party's 4 digit extension number...*"

Note:
Do not combine greetings and menus in the same recording. If you do, Call Director will not be able to repeat the menu to the caller.

For instructions on how to record a greeting, see Recording a Message.

A Message action can detect a call disconnection. If this occurs, the call-flow processing is immediately aborted.

The following table lists the configurable properties for the Message action and its possible results:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Message	Changing an action name renames all aliases of the action.

Item	Values (default = bold)	Description/Notes
Delay	< **0** - **Infinite**>	Number of seconds to wait until carrying out the action result. This property is useful in RAD applications where a recording plays continuously with a delay between plays. Default is 0 seconds.
Suppress Hangup Prompt	Disabled	Disables the system prompt that is played upon hangup.
Action ID	<xxxx>	A system-generated three-digit ID used to identify this action when recording the message by telephone.
Message Recording	**Recorded** or **Not Recorded**	Provides the status of the audio recording for this action. You can record a message from this field by clicking on the Recording button. See Recording and Importing Messages.
RESULTS		
Done	Hangup	Action taken when the message playback is complete. The default is hanging up.

Programming a Message Action

To program a Message action:

1. Access the Call Flow page.
2. Do one of the following:
3. For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click Edit.
4. For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click Edit.
5. Click **OK**. The current call flow appears.
6. Add the **Message** action to the call flow.

7. Under **When I receive a Call**, click the **Message** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.

Note:

If you select the Suppress Mailbox Greeting option for a Call Flow, a caller will not hear your mailbox greeting if going through Call Director. The caller will, however, still hear the greeting if the call goes through the message center.

1. Enter or modify the properties as needed. For information, see the table above.
2. Assign an action as required to the Done result.
3. Click **Save**. The call flow is saved.

26.160 Menu

The Menu action is a recording that presents options to an incoming caller. The recorded Menu prompts callers to press a key on their telephone keypad to select a menu option. For example, an incoming call answered by the Menu could tell the caller, " *If you know the extension of the person you wish to reach, enter it now*. *To speak to the sales desk, press 2. To speak to an attendant, press 0.*" The caller must then press the desired key on their phone's keypad, or hang up.

The Menu node includes not only the recorded Menu (that is, what callers will hear) but also a flag that determines how many times the menu should be repeated (Repetition count). You also define and program what the callers can input in response to the recorded Menu (that is, extension numbers, mailbox numbers, and single or multiple keys).

The call flow owner records the menu from the telephone interface. By default, the Menu repeats when the caller presses an invalid key.

The following table lists the configurable properties for the Menu action and its possible results:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Menu	Changing an action name renames all aliases of the action.

Item	Values (default = bold)	Description/Notes
Maximum DTMF Length	<maximum number of digits> 1	Maximum number of DTMF digits to gather from the caller. A value greater than 1, enables Multi-key result.
Retry Count	<0 - 99> 3	The number of times the Menu repeats when the caller makes invalid entries (or no entry at all). A retry count of 2, for example means that the Menu will play again, even after an invalid entry or no entry at all. This gives the caller additional opportunities to enter a valid selection.
Timeout	<0 - 99 seconds> 3	The number of seconds that the caller is given to respond with a valid key press as defined in the result. **Note**: If the timeout is set to 0 seconds, the system defaults the timeout to 3 seconds. However, 1 and 2 seconds work appropriately.
Action ID	< xxxx>	A system-generated three-digit ID used to identify this action when recording the prompt via the phone.
Prompt Recording	**Recorded** or **Not Recorded**	Provides the status of the audio recording for this action. You can record a message from this field by clicking on the Recording button. See Recording and Importing Messages.

Item	Values (default = bold)	Description/Notes
RESULTS		
DTMF Keys 0-9 * #	Retry	The action resulting from a single DTMF key pressed within the timeout period. Not all keys need to be connected to a subsequent action. Default (i.e., not connected to another action) is to play a pre-recorded system message, decrement the retry count, and repeat the menu recording.
Multi-key	Hangup	The action taken when the caller keys in more than one digit within the Timeout period or has keyed in the maximum number of digits defined by Maximum DTMF Length. Default is to play an appropriate pre-recorded system prompt, and then hang up.
Timeout	Retry	The action taken when the caller fails to press any DTMF key within the specified timeout. If the Timeout result is unassigned, each timeout decrements the Retry Count. Default result (i.e., not connected to another action) is to play a pre-recorded system message, decrement the retry count, and repeat the menu recording.
Error	Hangup	The action taken when retry count is reduced to zero as a result of the caller repeatedly pressing unassigned DTMF keys or not providing a response within the allowed timeout. Default is to play an appropriate pre-recorded system prompt, and then hang up.

Programming a Menu Action

To program a Menu action:

1. Access the Call Flow page.
2. Do one of the following:
   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click Edit.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click Edit.
3. Click **OK**. The current call flow appears.
4. Add the **Menu** action to the call flow.
5. Under **When I receive a Call**, click the **Menu** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
6. Enter or modify the properties as needed, assigning keys to voice messages. For information, see the table above.
7. Assign actions as required to the DTMF, timeout, and error results.
8. Click **Save**. The call flow is saved.

26.16 Call Transfers

A Transfer action routes the caller to a specified destination, such as an extension, the attendant, or an external telephone number.

Whenever you select a transfer Action, you can also define the transfer method as well as the subsequent incomplete transfer Action to take if the original transfer was incomplete (for example, a Ring Busy, Ring No Answer, or Invalid).

There are four types of call transfers: Blind Transfer, Supervised Transfer, Screened Transfer, and Alternate Transfer.

Note:
Call transfer privileges are governed by the system's Class of Service (COS). To use a particular type of call transfer, it must first be enabled in the system COS.

Destinations

Destination	Description/Notes
Specified Extension	The call is transferred to the extension specified when the call flow was set up.

Destination	Description/Notes
Gathered Digits	The call is transferred to the digits the caller entered in response to a previous menu. This property allows a caller to key digits to reach a desired destination—for example, an extension, a mailbox or external telephone (if permitted by system programming). See Menu for the parameters that must be set for Gathered Digits to work.
Attendant	The call is transferred to the extension for the user's mailbox configured by the system administrator or user. If the Attendant is not configured, the supervised transfer action will exit via the “Fail” path, without even attempting the transfer.
Attendant/Operator	The call is transferred first to the Attendant, then to the Operator if the Attendant extension is not configured.
Operator	The call is transferred to the Operator. The Operator is the Line Group Attendant Extension programmed on the Call Director Configuration page for the line group. If this extension is not programmed, the line group attendant extension is used.

Blind Transfers

A Blind Transfer dials the destination and then releases the call regardless whether the destination is busy or not answering.

With Call Director, the Blind Transfer action transfers a call to one of the following destinations, as configured by the call flow owner:

- An extension specified in the action properties;
- The Attendant/Operator extension;
- The extension stored as Gathered Digits during a previous Menu action that has a Multi-Key result.

The following table lists the configurable properties for the Blind Transfer action and its possible results:

Item	Value (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Blind Transfer	Changing an action name renames all aliases of the action.
Transfer To	<destination> Specified Extension	Select the destination to which the call is to be transferred—Specified Extension, Gathered Digits or Attendant/Operator.
Extension	<extension> Blank	Enter an extension number if Transfer To is set to *Specified Extension*; otherwise, leave blank.
Suppress Prompt	Disabled	Disables the system prompt that is played upon transfer.
Try Call Flow First	Disabled	Enables outgoing interflow. If the target number has a call flow, the call is transferred directly to the call flow instead of being transferred to the extension. See Override to configure your call flow for incoming interflow calls.
RESULTS		
There is no result for a Blind Transfer.		

Supervised Transfer

A Supervised Transfer waits for the called party to answer before completing the transfer. If the call is not answered or the called party is busy, it returns to the call flow for further processing.

The Supervised Transfer action transfers a call to one of the following destinations, as configured by the call flow owner:

- An extension specified in action properties;
- The Attendant/Operator extension;
- The extension stored in the Gathered Digits during a previous Menu action that has a Multi-Key result.
- The Attendant extension configured in the user mailbox
- The Operator extension

The following table lists the configurable properties for the Supervised Transfer action and its possible results. The results are dependant on the path of the call flow.

Item	Value (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Supervised Transfer	Changing an action name renames all aliases of the action.
Transfer To	<destination> Specified Extension	Select the destination to which the call is to be transferred—Specified Extension, Gathered Digits, Attendant, Operator, or Attendant/Operator.
Extension	<extension> Blank	Enter an extension number if Transfer To is set to *Specified Extension*; otherwise, leave blank.
No Answer Timeout	<timeout in seconds> 10	The number of seconds that the system waits for an answer before timing out. This setting overrides the Time Until No Answer setting in the Configuration page.
Suppress Prompt	Disabled	Disables the system prompt that is played upon transfer.

Item	Value (default = bold)	Description/Notes
Try Call Flow First	Disabled	Enables outgoing interflow. If the target number has a call flow, the call is transferred directly to the call flow instead of being transferred to the extension. See Override to configure your call flow for incoming interflow calls.
RESULTS		
Busy	Message Center	Action taken when the transfer destination is busy. The default is to play a pre-recorded system message, and then hang up.
No Answer	Message Center	Action taken when the transfer destination fails to answer within the No Answer Timeout period. The default is to play a pre-recorded system message, and then hang up.
Invalid	Message Center	Action taken if the transfer destination is invalid, as can happen for a Gathered-Digits transfer. The default is to play a pre-recorded system message, and then hang up.

Screened Transfer

A Screened Transfer is similar to a Supervised Transfer, except that the caller's name is first recorded and then played back to the called person. The called person has the option to accept or reject the call.

The Screened Transfer action transfers a call to one of the following destinations, as configured by the call flow owner:

- An extension specified in action properties;
- The extension stored in the Gathered Digits during a previous Menu action that has a Multi-Key result.

The following table lists the configurable properties for the Screened Transfer action and its possible results. The results are dependant on the path of the call flow.

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Screened Transfer	Changing an action name renames all aliases of the action.
Transfer To	<destination> Specified Extension	Select the destination to which the call is to be transferred—Specified Extension or Gathered Digits.
Extension	<extension>	Enter an extension number if Transfer To is set to *Specified Extension*; otherwise, leave blank.
No Answer Timeout	<timeout in seconds> 10	The number of seconds that the system waits for an answer before timing out. This setting overrides the Time Until No Answer setting in the Configuration page.
Suppress Prompt	Disabled	Disables the system prompt that is played upon transfer.
Try Call Flow First	Disabled	Enables outgoing interflow. If the target number has a call flow, the call is transferred directly to the call flow instead of being transferred to the extension. See Override to configure your call flow for incoming interflow calls.
RESULTS		

Item	Values (default = bold)	Description/Notes
Rejected	Message Center	The action taken when the destination rejects the transfer attempt. The default is to play a pre-recorded system message, and then hang up.
Busy	Message Center	Action taken when the transfer destination is busy. The default is to play a pre-recorded system message, and then hang up.
No Answer	Message Center	Action taken when the transfer destination fails to answer within the No Answer Timeout period. The default is to play a pre-recorded system message, and then hang up.
Invalid	Message Center	Action taken if the transfer destination is invalid, as can happen for a Gathered-Digits transfer. The default is to play a pre-recorded system message, and then hang up.

Alternate Transfer

An Alternate Transfer is used to route calls to an external destination, such as a cell phone or pager, and for text messaging. The destination is defined by the dial string sequence, which can include commands that permit complete control of the outgoing call, including:

- Dial tone detection
- Call answer supervision
- Dialing DTMF keys
- Inserting pauses

The following table lists the properties to be configured for an Alternate Transfer and the results of the action. The results are dependant on the path of the call flow:

Item	Values (default = bold)	Description/Notes
PROPERTIES		

Item	Values (default = bold)	Description/Notes
Name	<defined action name> Alternate Transfer	Changing an action name renames all aliases of the action.
Dial String	<dial string>	Enter a combination of characters, up to 16 total, from the Dial String Table.
No Answer Timeout	<timeout in seconds> 10	Number of seconds until the call is considered unanswered. Default is 10 seconds. This setting overrides the Time Until No Answer setting in the Configuration page. **Note**: This setting has no effect unless the dial string contains at least one of the "wait" codes from the Dial String Table (G,L,P, or T).
RESULTS		
Timeout	Message Center	The action taken when the called destination fails to answer within the timeout period. The default is to play a relevant system message, and then hang up.

Programming a Call Transfer Action

To program a Call Transfer action:

1. Access the Call Flow page.

2. Do one of the following:

   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
3. Click **OK**. The current call flow appears.
4. Add a call transfer action (i.e. **Blind Transfer**, **Supervised Transfer**, **Screened Transfer**, or **Alternate Transfer**) to the call flow.
5. Under **When I receive a Call**, click the call transfer action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
6. Enter or modify the properties as needed. For information, see the appropriate table above.
7. Assign actions as required to the transfer results.
8. Click **Save**. The call flow is saved.

26.162 Voicemail

The Voicemail action sends the caller to a NuPoint Unified Messaging mailbox. Normally the call is sent to a specific mailbox, but by using the Multi-key result of a Menu action the call can be sent to a caller-specified mailbox. If the mailbox is not specified, then the call is sent to the mailbox of the call-flow owner.

Note:

During an upgrade from Release 10 to Release 11, a vacant Voicemail node in a call flow is replaced with a Message Center node. However, there is no change to the user-defined name of this node that is displayed in the call flow. For example, if the user had left the name as Voicemail in Release 10, then the type of node is changed to the Message Center node in Release 11, but the name displayed in the call flow remains as Voicemail.

The following table lists the configurable properties for the Voicemail action and its possible results:

Item	Value (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Voicemail	Changing an action name renames all aliases of the action.

Item	Value (default = bold)	Description/Notes
Transfer To	<destination> Specified Extension	Select the destination to which the call is to be transferred—Specified Extension or Gathered Digits.
Target Mailbox	<target voice mailbox> Blank	Enter the mailbox in which you want to leave a message. Can be explicitly defined, obtained from the caller (via the Multi-key result of a previous Menu action), or the mailbox of the call flow owner if left blank.
Suppress Greeting	Disabled	Suppresses the greeting that is played in the Target Mailbox.
Try Call Flow First	Disabled	Enables outgoing interflow. If the target number has a call flow, the call is transferred directly to the call flow instead of being transferred to the extension. See Override to configure the behavior for calls that are transferred to your call box through interflow.
RESULTS		
Zero Press	Unassigned	Enables call processing within the current call flow when the user presses 0 after leaving a message.

Programming a Voicemail Action

To program a Voicemail action:

1. Access the Call Flow page.
2. Do one of the following:
3. For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click Edit.

4. For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
5. Click **OK**. The current call flow appears.
6. Add the **Voicemail** action to the call flow.
7. Under **When I receive a Call**, click the **Voicemail** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
8. Enter or modify the properties as needed. For information, see the table above.
9. Click **Save**. The call flow is saved.

26.163 Dial-by-Name

The Dial-by-Name action sends the caller to the NuPoint Unified Messaging Dial-by-Name application which matches the telephone keypad equivalent of the spelled names of mailbox owners (as entered by the caller) with their mailbox and extension numbers.

Note:
For the Dial-By-Name action to work, the NuPoint Unified Messaging dialing plan for the line group associated with Call Director must have the letter ‘A’ somewhere in it. The 'A’ triggers the prompt to spell the name. For more about the Dial-by-Name application, see the *NuPoint Unified Messaging System Administration Online Help*.

The following table lists the configurable properties for the Dial-by-Name action and its possible results:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Dial-By-Name	Changing an action name renames all aliases of the action.

Item	Values (default = bold)	Description/Notes
Last Name First	Disabled	Specifies that the person's last name should be entered first. If this setting is enabled, callers will be prompted to enter the mailbox owner's last name first when using the Dial-by-Name function. For example, to reach John Smith they would type S-M-I-T-H J-OH-N. If this setting is disabled, callers will be prompted to enter the mailbox owner's first name first when using the Dial-by-Name function. For example, to reach John Smith they would type J-OH-N S-M-I-T-H. The NuPoint UM server search its records for entries that match the letters the caller has typed. If it finds more than one match, it plays the names and mailbox numbers of the partial matches. If it finds a unique match, it plays either the user's name or personal greeting.
Suppress Extension	Disabled	Suppresses the mailbox extension from the search.
RESULTS		
Match	Blind Transfer	If the name entered actually matches a system mailbox, then the call is transferred to that mailbox.
No Match	Attendant	If the name entered does not match a system mailbox, then the call is sent to the Auto Attendant for completion.

Programming a Dial-by-Name Action

To program a Dial-by-Name action:

1. Access the Call Flow page.
2. Do one of the following:
   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
3. Click **OK**. The current call flow appears.
4. Add the **Dial-by-Name** action to the call flow.
5. Under **When I receive a Call**, click the **Dial-by-Name** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
6. Enter or modify the properties as needed. For information, see the table above.
7. Click **Save**. The call flow is saved.

26.164nternal/External Call Handling

The Internal/External action allows you handle internal calls one way and external calls another—for example, when you're on the phone, internal calls could go to your mailbox and external calls could go to your cell phone.

The following table lists the configurable properties for the Internal/External action and its possible results:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Internal/External	Changing an action name renames all aliases of the action.
RESULTS		
Internal	Hangup	The action taken for internal calls. The Default is to play a pre-recorded system message, and then hang up.
External	Hangup	The action taken for external calls. The Default is to play a pre-recorded system message, and then hang up.

Programming an Internal/External Action

To program an Internal/External action:

1. Access the Call Flow page.

2. Do one of the following:

   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
3. Click **OK**. The current call flow appears.
4. Add the **Internal/External Filter** action to the call flow.
5. Assign actions to the results as required. For information, see the table above.
6. Click **Save**. The call flow is saved.

26.165 Caller ID Filter

The Caller ID Filter action handles calls based on whether the caller's number is in your Caller ID list. You can use this action, for example, to transfer calls from home to your cell phone instead of your extension. That way, your family can reach you when your extension is busy or when you're away from your desk. The list can contain up to twenty Caller ID entries.

The following table lists the configurable properties for the Caller ID Filter action and its possible results:

Item	**Values (default = bold)**	**Description/Notes**
PROPERTIES		
Name	<user-definable> Caller ID	Changing an action name renames all aliases of the action.
Caller ID	<Caller ID>	Enter the extension or telephone number of the caller you want to add to your Caller ID List.
Add	--	Click to add the Caller ID entry to the Caller ID List
Remove	--	Click to delete the selected entry in the Caller ID List.
Caller ID List	<user-definable>	The list of callers that will be processed by the Listed destination action.

RESULTS		
Listed	Hang up	The action taken when the caller ID exactly matches an entry in the Caller ID List. The default is to play a pre-recorded system message, and then hang up.
UnListed	Hang up	The action taken when the caller ID is not in the Caller ID List. The default is to play a pre-recorded system message, and then hang up.

Programming a Caller ID Action

To program a Caller ID action:

1. Access the Call Flow page.
2. Do one of the following:

1. • For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   • For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.

1. Click **OK**. The current call flow appears.
2. Add the **Caller-ID Filter** action to the call flow.
3. Under **When I receive a Call**, click the **Caller-ID Filter** action listed in the call flow. The action's Properties and Results appear at the bottom of the page.
4. Use the **Add** and **Remove** buttons to manage your list of **Caller IDs**. You can add up to twenty entries to the list.
5. Assign actions to the results as required.
6. Click **Save**. The call flow is saved.

26.166 Daily Greeting

When a Daily Greeting action is encountered in the call flow, your recorded daily greeting is played.

There are two types of Daily Greeting: Today's Daily Greeting or Default Daily Greeting. Today's Daily Greeting allows users to personalize their greeting on a daily basis with a temporary greeting that will revert at midnight back to the user's Default Daily Greeting, or, if that is not recorded, to their Primary Personal Greeting.

The following table lists the configurable properties for the Daily Greeting action and its possible results:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Daily Greeting	Changing an action name renames all aliases of the action.
Today's Daily Greeting	**Recorded** or **Not Recorded**	Provides the status of the audio recording for this action. You can record a message from this field by clicking on the Recording button. See Recording and Importing Messages.
Default Daily Greeting	**Recorded** or **Not Recorded**	Provides the status of the audio recording for this action. You can record a message from this field by clicking on the Recording button. See Recording a Message.
RESULT		
Done	Hangup	Action taken after the daily greeting has finished playing. The default is hanging up.

Programming a Daily Greeting Action

To program a Daily Greeting action:

1. Access the Call Flow page.
2. Do one of the following:

   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
3. Click **OK**. The current call flow appears.
4. Add the **Daily Greeting** action to the call flow.

5. Under **When I receive a Call**, click the **Daily Greeting** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
6. Enter or modify the properties as needed. For information, see the table above.
7. Assign an action as required to the Done result.
8. Click **Save**. The call flow is saved.

26.167 Message Center

A Message Center node has been created to allow a call to end up in the message center. This node is the default destination when the voice mailbox is not specified.

The new Message Center node only has its name as a property. Like the Voicemail node, the Message Center node is a termination action meaning that there are no branches from this node.

Any existing mailbox call flow that contains a Voice mail node with no extension specified will be updated replacing the Voicemail node with a Message Center node.

Note:
During an upgrade from Release 10 to Release 11, a vacant Voicemail node in a call flow is replaced with a Message Center node. However, there is no change to the user-defined name of this node that is displayed in the call flow. For example, if the user had left the name as Voicemail in Release 10, then the type of node is changed to the Message Center node in Release 11, but the name displayed in the call flow remains as Voicemail.

The following table lists the configurable properties for the Message Center action:

Item	Value (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Message Center	Changing an action name renames all aliases of the action.
RESULTS		
There is no result for the Message Center action.		

Programming a Message Center Action

To program a Message Center action:

1. Access the Call Flow page.

2. Do one of the following:

   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click **Edit**.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click **Edit**.
3. Click **OK**. The current call flow appears
4. Add the **Message Center** action to the call flow.
5. Under **When I receive a Call**, click the **Message Center** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
6. Enter or modify the properties as needed. For information, see the table above.
7. Click **Save**. The call flow is saved.

26.16.8 Language Router

The Language Router action enables users to take advantage of the "Multilingual Service" feature if it is enabled on NuPoint. When users first reach the Message Center or Receptionist application, they are prompted to choose between multiple languages (for example, English, French, or German). Thereafter, they will receive prompts only in the language they have selected.

Note:
When callers encounter the Language Router action, they will be prompted to select a preferred language, irrespective of whether they or the mailbox they are trying to reach have a custom LCOS language. If a user reaches a mailbox number with a custom LCOS language, prompts will be delivered in the mailbox's language. To override this functionality (and have a multilingual system play prompts in the selected language rather than the mailbox language), assign an FCOS with feature bit 51, Do Not Switch Languages for Outside Caller, to the mailbox.

To take advantage of the Language Router action, you must activate the Multilingual Service feature on NuPoint by installing the alternate-language prompt software and configuring a line group with up to five prompt languages.

If the Multilingual Service is not activated, you can still add the Language Router action to a call flow. However, users will not be prompted to select a prompt language. Instead, they will receive prompts in the default language.

The following table lists the configurable properties for the Language Routing action:

Item	Values (default = bold)	Description/Notes
PROPERTIES		
Name	<user-definable> Language Router	Changing an action name renames all aliases of the action.

Item	Values (default = bold)	Description/Notes
RESULTS		
Language_1	Message Center	The action taken when the Multilingual Service feature is enabled and the primary prompt language is selected. Default is to play an appropriate pre-recorded message, and then disconnect the call.
Language_2	Message Center	The action taken when the Multilingual Service feature is enabled and the second available prompt language is selected. Default is to play an appropriate pre-recorded message, and then disconnect the call.
Language_3	Message Center	The action taken when the Multilingual Service feature is enabled and the third available prompt language is selected. Default is to play an appropriate pre-recorded message, and then disconnect the call.
Language_4	Message Center	The action taken when the Multilingual Service feature is enabled and the fourth available prompt language is selected. Default is to play an appropriate pre-recorded message, and then disconnect the call.
Language_5	Message Center	The action taken when the Multilingual Service feature is enabled and the fifth available prompt language is selected. Default is to play an appropriate pre-recorded message, and then disconnect the call.

Programming a Message Center Action

To program the Language Router action:

1. Access the Call Flow page.
2. Do one of the following:

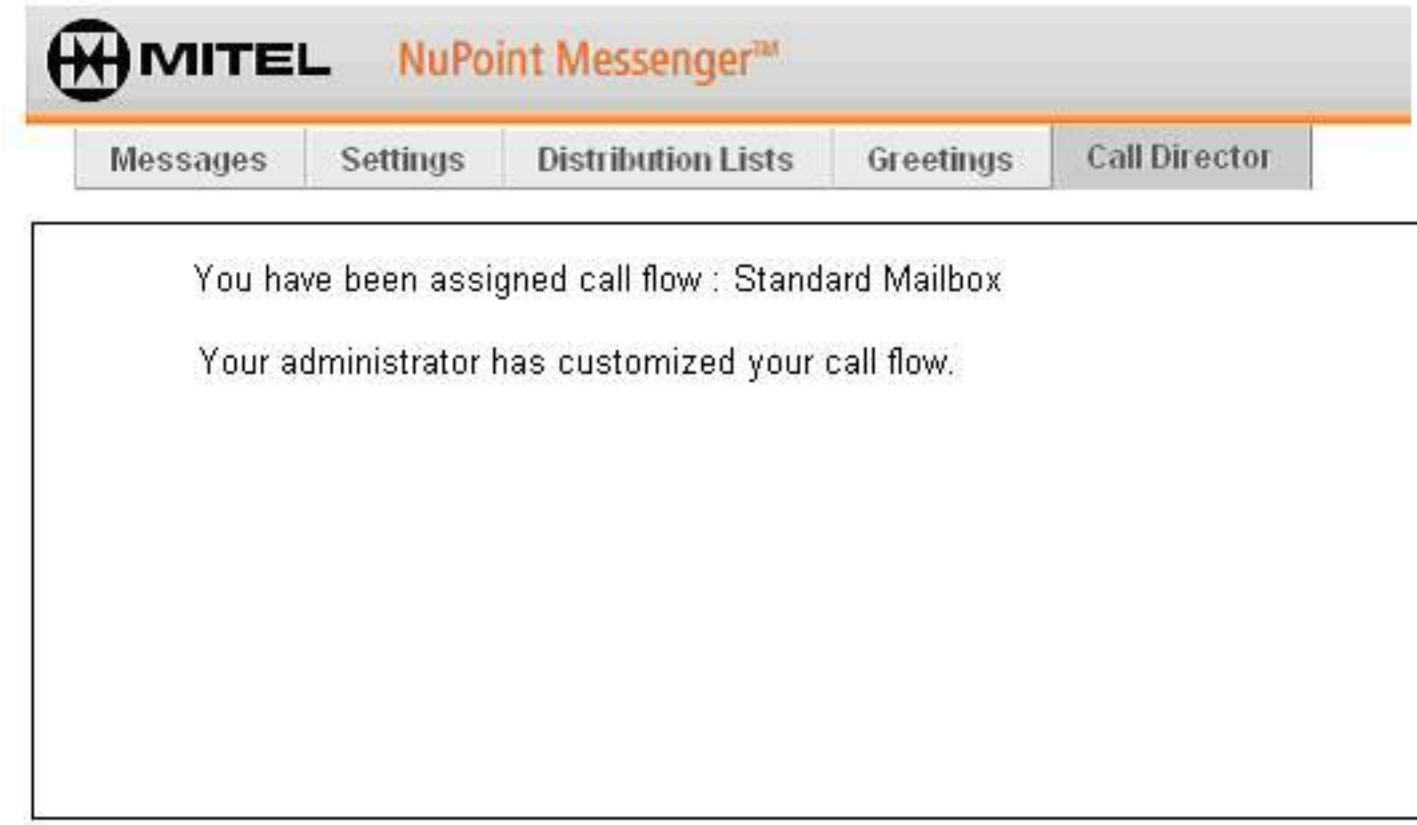
   - For personal call flows, select **Mailbox** from the Call Flow list at the top of page, enter the desired Mailbox number, and then click Edit.
   - For line group call flows, select **Line Group** from the Call Flow list at the top of page, enter the desired Line Group number, and then click Edit.
3. Add the **Language Router** action to the call flow.
4. Under **When I receive a Call**, click the **Language Router** action listed in the call flow. The action's Properties and Results appear at the bottom of the window.
5. Assign actions as required to the Language_1 and Language_2 to Language_5 results.
6. Select **Auto** as the Prompt language for the call flow.
7. Click **Save**. The call flow is saved.

26.169 Call Flow Authoring Procedures - Overview

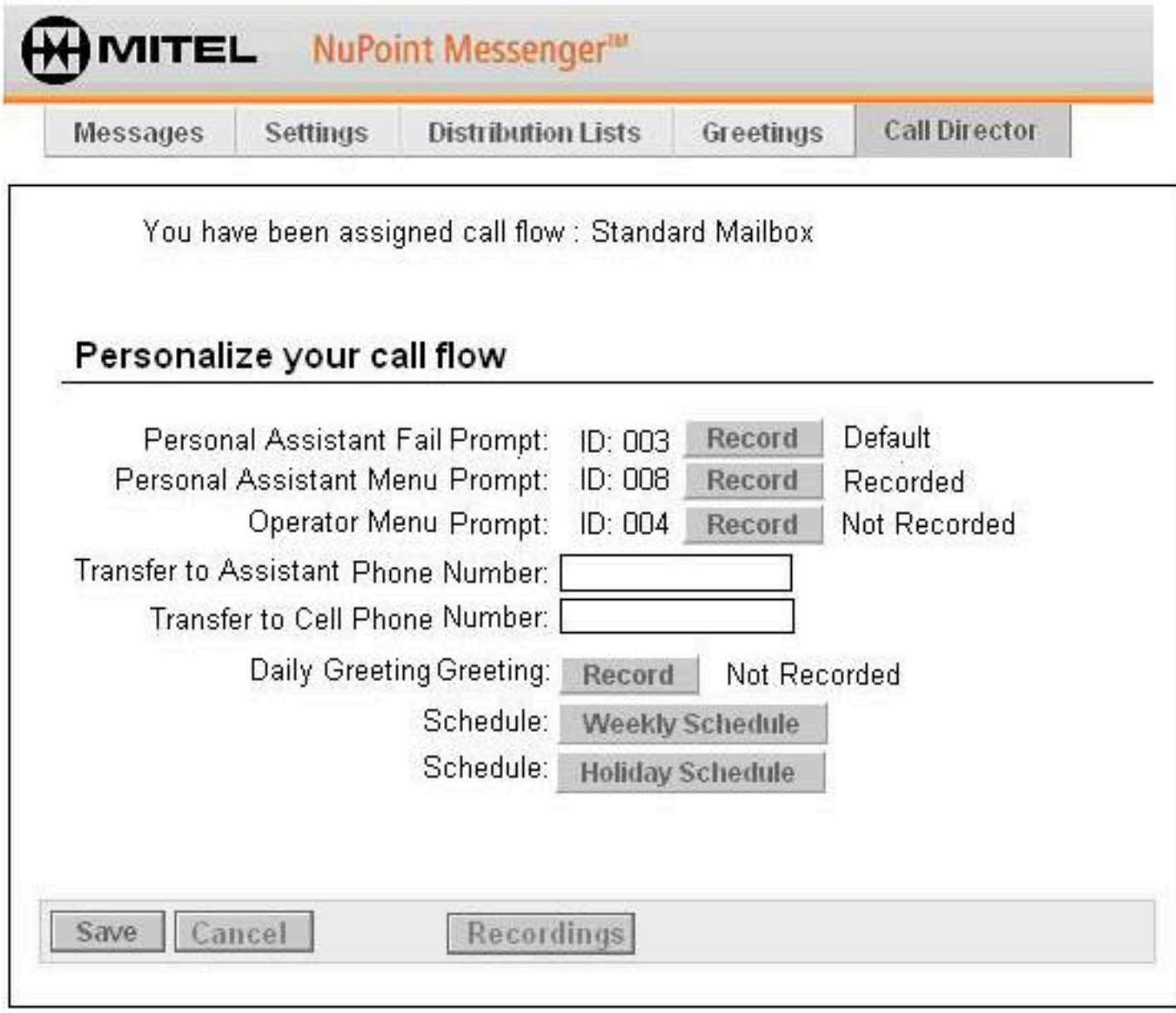
Regular Call Director users are assigned a call flow by their system administrator. The administrator can configure all parameters for the user, or give the user the ability to change some parameters. Advanced Call Director users can create their own call flows.

Regular Call Director Users

If you are a Regular user and the system administrator has configured the parameters of your call flow for you, your Call Director tab will look something like the following example:



If you have the ability to change parameters, your Call Director tab will show which parameters you can change, as in the following example:



For information on changing the parameters shown, see Recording greetings and Schedule.

Advanced Call Director Users

If you are an Advanced user, your system administrator has not assigned a call flow to you. You can create your own call flows and customize them as you choose.

For information on creating call flows see:

Starting with a template

Adding an action

Deleting an action

Reusing an action

Copying a call flow

Deleting a call flow

Inserting an action

Setting action properties

Setting the prompt language

Recording greetings

Viewing call flow paths

Printing call flows

26.17.3 Starting with a template

There are five system templates provided with the Call Director functionality. These templates can be used as a starting point when creating a call flow. Additional templates may have been created by the System Administrator and are also available for the call flow.

The five system templates are as follows: Daily Greeting, Follow Me, Find Me, Personal Dial Zero and Alternate Daily Greeting.

Note:
Only Advanced users are able to use templates to create call flows.

To select a template for the call flow:

1. From the **Edit** menu on the call flow page, click **Start with Template**.
2. A window with the list of available templates appears. Select the template you want to use for the call flow.
3. Click **OK**.

The selected call flow is activated and all default property values and recordings associated with that template are also activated. These property values and recordings can be edited once the call flow has been activated.

26.171 Adding an action

Adding an action is done by assigning a new action to a result of an existing action.

All call flows begin with the *When I receive a call* action.

There are no restrictions on the number and order of actions in call flow. The same action can be used more than once (see Reusing an Action).

To add an action to a call flow:

1. Do one of the following:

1. • For a new call flow, click on **When I receive a call** in the **Call Flow** display area.
   • For an existing call flow, click the action after which you want the new action added.

1. In the action's **Results** area, click a link representing a result (there may be more than one).
2. From the **New Actions** menu that appears, select the desired action type.
3. The new action item is added to the Call Flow display area and automatically selected.
4. Program the desired properties for the new action. At this point you can either assign actions to the results of the new action, or return to the original action and assign actions to its unassigned results. To create a call flow with multiple instances of an action, each with unique properties, assign the actions different names.
5. Click **Save**. The call flow is saved.

26.172 Deleting an action

When deleting an action, all actions to which it is connected become *Unused Actions*. These actions can be re-inserted into the call flow or deleted altogether.

To delete an action:

1. Select the action to be deleted.

   Example:

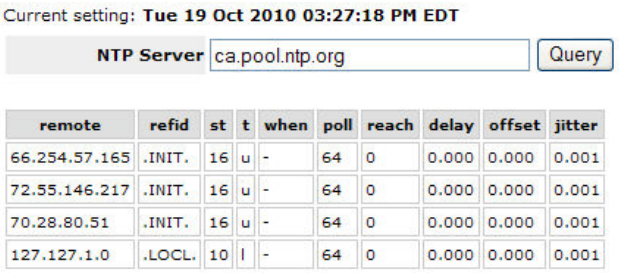


2. From the **Edit** menu, click **Delete Action**.

3. A confirmation message appears. Click **OK** to confirm the deletion.

   Any actions connected to the deleted action become *unused actions*. The unused actions are presented in a separate branch in the call flow tree. Because the actions are unused, they're ignored when a call is processed by the call flow.

   Example:



4. To delete an unused actions, select it, and then click **Delete Action**.
5. Click**Save**to save the call flow changes.

26.173 Reusing an action

The same action can be assigned to results of other actions. For example, the **Busy** and **No answer** results of a **Supervised Transfer** action could both send a call to the same **Voicemail** action.

Reusing an action is always done by assigning an existing action to a result of an action. The resulting action may even be itself. For example, a **Menu** action might present a set of options followed by "…to hear these choices again, press the 8 key". The 8-key result of the Menu action could be assigned to the Menu action itself, thus creating a loop in the call flow.

Because actions are always created with the same name, you should be careful to assign meaningful names to actions to make them distinct. Reusing actions is a lot easier if the actions have distinct names.

There is no limit on the number of times an action can be reused.

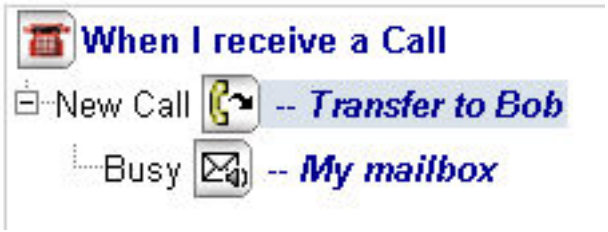
To reuse an action:

The procedure for reusing an action is best explained by example. In the following scenario, we will make the Busy and No answer result of a Supervised Transfer go to the same Voicemail action.

1. Add a **Supervised Transfer** action to your call flow.
2. To the **Busy** result of the new **Supervised Transfer** action, add a **Voicemail** action.
3. Enter the required properties for the **Voicemail** action, including a meaningful name, such as *My mailbox*.

4. Click on the original **Supervised Transfer** action to select it.

   The call flow will look similar to this:



5. Click on the **No Answer** result.

   The resulting menu provides the option of creating a new action and a list of existing actions, including the Voicemail action created in step 2.

6. From this menu, select Voicemail:My mailbox This will assign the **No Answer** result to the same action as the **Busy** result. Your call flow will now look something like this:



   Notice the small arrow at the bottom right of the icon beside the **No Answer** result. This means that the action is an *alias*. An alias acts like a reference to the “real” action elsewhere in the call flow. Clicking an alias selects the action it refers to. Thus, the alias has the same properties as the other action; any change made to the properties of the other action is automatically made to the alias.

7. Click **Save** to save the call flow changes.

26.174 Copying a call flow

A call flow can be copied from one mailbox or line group to another. This can be used in the scenario where a person has changed extensions and the existing call flow needs to be copied to the new mailbox.

Note:

- Only System Administrators are able to copy a call flow.
- To successfully copy a call flow, you must use the menu commands described in the following procedure. Do *not* attempt to manually copy a call flow using a copy-and-paste operation.

An existing call flow can also be copied and saved as a template.

To copy a call flow:

1. From the **Edit** menu on the call flow page, click **Copy From**.

Note:
This menu item is only available in the Web Console.

2. A window requesting you to enter the call flow for a particular mailbox or line group appears. Enter either the mailbox or line group number.

Note:
When the "Copy From" command is invoked from the Call Flow editing window for a mailbox, the feature is limited to copying mailboxes. An Advanced user's call flow can only be copied to another Advanced user's call flow. A Regular user's call flow can only be copied to another Regular user that has the same assigned template. When the "Copy From" command is invoked from the Call Flow editing window for a line group, the feature is limited to copying the call flow for a line group. A line group call flow can be only be copied into another line group.

3. Click **OK**. The call flow and its associated properties are copied into the current call flow.

Note:
When the "Copy From" command is invoked from the create/edit template page in the Web Console, you can copy the call flow from an Advanced mailbox user OR line group into a template for the purposes of creating a new template. In this case, both the "Mailbox" and "Line Group" options are available.

26.175 Deleting a call flow

You can delete an entire call flow. When deleting a call flow, all actions to which the call flow is connected are deleted. All nodes including the nodes in the unused nodes branch will be deleted.

Note:
Only Advanced users and System Administrators are able to delete a call flow.

To delete a call flow:

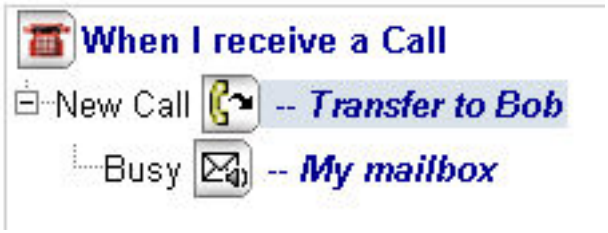
1. Select the call flow you want to delete.
2. From the **Edit** menu on the call flow page, click **Delete Call Flow**.
3. A confirmation window appears. Click **Yes** to confirm the deletion. All nodes including the nodes in the unused nodes branch will be deleted.

26.176 Inserting an action

You may find that you need to add an action to your existing call flow, not at the end of a branch but somewhere in the middle. For example, your existing call flow does not make use of an Override action, but now you want to start off with an Override, while preserving the structure of your existing call flow.

To insert an action:

The procedure for inserting an action is best explained by example. In the following scenario, we build on the example in the Reusing an Action topic. Assuming the following call flow, we will insert an Override action between the When I receive **a call** and **Transfer to Bob** actions.



1. Click When I receive a call. Note that the **New Call** result is the **Supervised Transfer: Transfer to Bob** action.
2. In the **Results** area, click the **Supervised Transfer: Transfer to Bob** link.

3. From the New Actions menu, select **Override** as the new action type.

   The new action item is added to the Call Flow display area and the new Override action is assigned to the New Call result. The entire call flow is moved under Unused Actions as follows (you may need to click the ⊞ sign on the left of the call flow to expand the collapsed branches):



4. Click on the new **Override** action, and then on the **Disabled** result link.
5. Click on Supervised Transfer:Transfer to Bob. This will assign that action to the **Disabled** result of the **Override** action.

   The call flow is re-created under the **Override** action's **Disabled** result and now appears as follows:



6. Assign actions to the **Enabled** result of the **Override** action as required. (These are typically a Message action followed by a Voicemail action.)
7. Click the Save button to save the call flow changes.

26.17 Setting action properties

You can change the properties of an action at any time. The changes take effect immediately after they are saved.

To set the properties of an action:

1. Click the action in the Call Flow that you want to modify.

2. Under Properties for (selected action), make the required changes.
3. Click **Save** to save the call flow changes.

26.178 Setting the prompt language

You can set the prompt language for a call flow.

To set the prompt language:

1. From the Actions menu on the call flow page, click **Set Prompt Language**.
2. A window with the list of available languages appears.
3. Select a language or accept "Auto" as the default value.

> **Note**:
> Use "Auto" to take advantage of the Multilingual Service feature, whereby users are asked to select between up to five prompt languages when the Language Router action is performed.

4. Click **OK**. The selected language will be used for the call flow.

> **Note**:
> Changes to the prompt language are not saved until you press the **Save** button.

26.179 Recording and Importing Messages

Each Message and Menu action in a call flow requires an audio recording. You can add your own recording or, if you are an Advanced user, import an existing one.

> **Note**:
> A maximum of 100 greetings are supported in call flow by Call Director.

Recording Messages in Call Director

Each message is assigned an Action ID by Call Director. The ID is a property of the action and is presented in the Properties area when the action is selected. You are prompted to enter the ID when recording the message. The Actions > Recordings menu item on the Call Flow page lists IDs for all messages in the call flow and shows whether or not the messages have been recorded.

Note: Do not combine greetings and menus in the same recording. If you do, Call Director will not be able to repeat the menu to the caller.

To record a message:

1. Using any touch-tone telephone, log into your NuPoint Unified Messaging mailbox, and press the * key. This will connect your call into the Call Director Telephony User Interface (TUI).
2. As an alternative to pressing the * key, follow the voice prompts to record your message.

Recording a Message for a Single Action

To record a message for a single action:

1. Select a Message or Menu action in the call flow.
2. (Optional) If you want the system to call your extension and allow you to record the message, complete the following steps in the Properties area:

   a. Select the **Call Me** check box.
   b. Enter your extension number in **Call Me Number**.
   c. Click **Save**.
3. Click **Recording**. The Recording Status window opens.
4. Click **Record** under the Actions column.
5. The Record Message dialog opens, prompting you to record your message. The prompts differ depending on whether you have configured a **Call Me Number**:

   - If you have programmed a Call Me Number, the system calls your extension. Answer the call and proceed to the next step to make your recording.
   - If have *not* programmed a Call Me Number, the system prompts you to call in to your NuPoint voice mailbox, log in, and press the * key to access the Call Director Telephone User Interface (TUI). Proceed to the next step to make your recording (you will not receive any voice prompts).
6. In the Record Message dialog, click the **Record** button and then record your message over the telephone. When you have finished recording, click the **Stop** button. To review your message before saving it, click the **Play** button. After you have finished recording your message, click **Save** to exit the Record Message dialog.
7. Click **Close** to exit the Recording Status window.

Note:
You cannot use Call Me functionality to record messages for multiple actions or Line Group call flows, or to edit Templates.

Recording a Message for Multiple Actions

To record a message for one or more actions:

1. Select **Actions > Recordings**. The Recording Status window opens.
2. Locate the messages you wish to record and click **Record** under the Actions column.
3. A dialog opens, prompting you to call in to your NuPoint voice mailbox, log in, and press the * key to access the Call Director Telephone User Interface (TUI).
4. Use the TUI to specify an action ID and record your message.
5. After you have finished recording your message, click **Close** to exit the Recording Status window.

Note:

- If you call in to your mailbox, as an alternative to pressing the * key, you can simply follow the voice prompts to access the Call Director TUI and record your message.
- You can also record a message from the **Actions > Recordings** menu item on the call flow page or from the Recording button in the Properties area of the call flow page.
- There are two methods to call into your mailbox and record the Daily Greeting for the call flow:
- Press the * key to access the Call Director TUI. Use the TUI to navigate through the system and record the message.
- Access the User Options menu and select Greetings (4) and Record Daily Greeting (8).

Importing Greetings into Call Director

Instead of recording greetings, you can also import a recorded greeting (prompt). Once the prompt has been imported, it is treated like any other recorded prompt.

Note:

- Only Advanced users and System Administrators are able to import recorded prompts.
- To be imported into a call flow, audio recordings are required to be in 8-bit, 8 KHz u-law or a-law format. Audio files recorded in any other format must be converted to this format before attempting the import function. In addition, the recording duration of the file being imported cannot exceed 5 minutes.
- The audio file must be in 8k u-law or 8k a-law format. If the file being imported is not in this format or does not exist, the Status will show "Import Error" and the file name controls will remain displayed for that prompt. An error message "Please specify a valid 8k u-law or a-law audio file" will also be displayed.
- If you are unable to import the audio file (indicated by a failure to save the recording or call flow), verify that your web browser security settings are correct. To do this, click the**Start**button and type**Internet Options**in the search box. Select the**Security**tab and click the**Custom Level**button. In the**Miscellaneous**section, ensure that**Display mixed content**is set to**Prompt**. If**Display mixed content**is disabled, file import will fail.

To import a recorded prompt:

1. Select **Actions > Recordings**. The Recording Status window appears showing the list of prompts. A status of "Recorded" or "Not Recorded" is displayed in the Status field.
2. Select the item for which you want to import a prompt and click **Import**.
3. A new File option appears in the window. Type the name of the filename or browse to the appropriate prompt file.
4. Click **Sta rt Import** to import the prompt.

Note:
You can import a prompt one at a time, or specify all the prompts to import and then press the "Start Import" button.

26.180Viewing call flow paths

You can view all the unused paths of a specific call flow. An unused path is an action, such as a Menu key, that does not have a result programmed.

To view the call flow paths:

1. From the View menu on the call flow page, click **Show All Paths**.
2. The call flow will expand to show all the unused paths within the call flow.

> **Note**:
> Once all paths are shown, the menu item will change to "Hide Unused Paths".

3. To hide the unused paths, click **Hide Unused Paths**.

26.18.1 Printing call flows

You can print an entire call flow, including its unused paths.

To print a call flow:

> **Note**:
> To include unused paths in the printout, click **Show All Paths** from the View menu prior to commencing the procedure.

1. On the call flow page, click **Print Callflow**.
2. Access the print preview dialog by entering the appropriate keyboard shortcut, such as **Control + P** in Windows or **Command + P** in Mac.
3. In the print preview dialog, select a **Destination**. You may send the printout to a regular printer or save it to file (PDF or XPS).
4. Click **Print**.

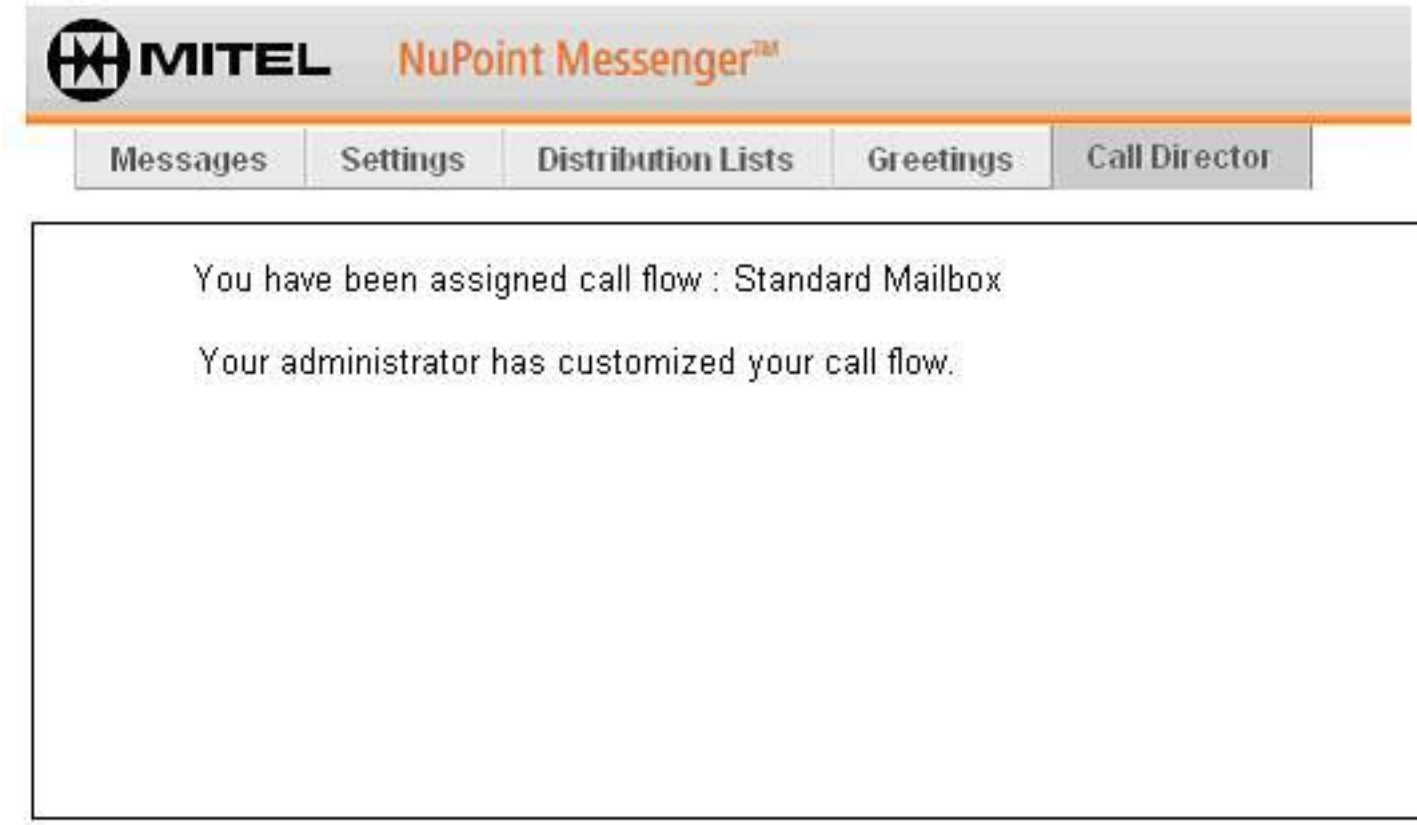
> **Note**:
>
> - If you receive a certificate error which prevents the print preview from displaying correctly, click **Show Content** at the bottom of the dialog.
> - If you are saving the printout to file, follow the prompts to assign a name and location for the document.

26.182 Call Flow Authoring Procedures - Overview

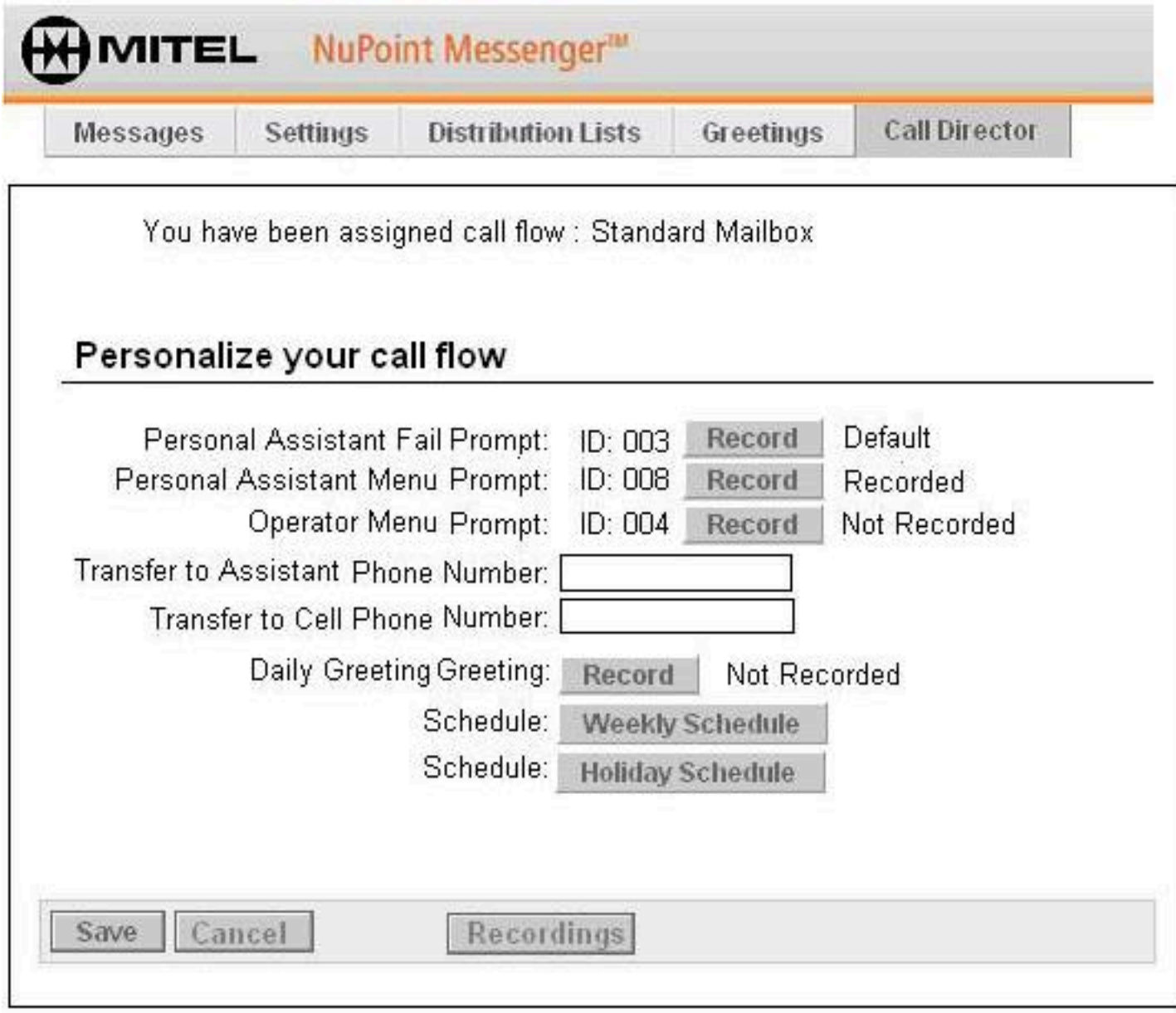
Regular Call Director users are assigned a call flow by their system administrator. The administrator can configure all parameters for the user, or give the user the ability to change some parameters. Advanced Call Director users can create their own call flows.

Regular Call Director Users

If you are a Regular user and the system administrator has configured the parameters of your call flow for you, your Call Director tab will look something like the following example:



If you have the ability to change parameters, your Call Director tab will show which parameters you can change, as in the following example:



For information on changing the parameters shown, see Recording greetings and Schedule.

Advanced Call Director Users

If you are an Advanced user, your system administrator has not assigned a call flow to you. You can create your own call flows and customize them as you choose.

For information on creating call flows see:

Starting with a template

Adding an action

Deleting an action

Reusing an action

Copying a call flow

Deleting a call flow

Inserting an action

Setting action properties

Setting the prompt language

Recording greetings

Viewing call flow paths

Printing call flows

26.183 Starting with a template

There are five system templates provided with the Call Director functionality. These templates can be used as a starting point when creating a call flow. Additional templates may have been created by the System Administrator and are also available for the call flow.

The five system templates are as follows: Daily Greeting, Follow Me, Find Me, Personal Dial Zero and Alternate Daily Greeting.

Note:
Only Advanced users are able to use templates to create call flows.

To select a template for the call flow:

1. From the **Edit** menu on the call flow page, click **Start with Template**.
2. A window with the list of available templates appears. Select the template you want to use for the call flow.
3. Click **OK**.

The selected call flow is activated and all default property values and recordings associated with that template are also activated. These property values and recordings can be edited once the call flow has been activated.

26.184 Adding an action

Adding an action is done by assigning a new action to a result of an existing action.

All call flows begin with the *When I receive a call* action.

There are no restrictions on the number and order of actions in call flow. The same action can be used more than once (see Reusing an Action).

To add an action to a call flow:

1. Do one of the following:

1. • For a new call flow, click on **When I receive a call** in the **Call Flow** display area.
   • For an existing call flow, click the action after which you want the new action added.

1. In the action's **Results** area, click a link representing a result (there may be more than one).
2. From the **New Actions** menu that appears, select the desired action type.
3. The new action item is added to the Call Flow display area and automatically selected.
4. Program the desired properties for the new action. At this point you can either assign actions to the results of the new action, or return to the original action and assign actions to its unassigned results. To create a call flow with multiple instances of an action, each with unique properties, assign the actions different names.
5. Click **Save**. The call flow is saved.

26.185 Deleting an action

When deleting an action, all actions to which it is connected become *Unused Actions*. These actions can be re-inserted into the call flow or deleted altogether.

To delete an action:

1. Select the action to be deleted.

   Example:

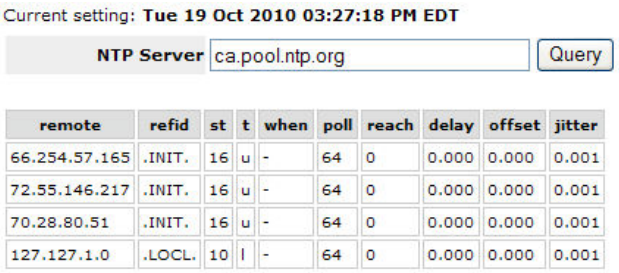


2. From the **Edit** menu, click **Delete Action**.

3. A confirmation message appears. Click **OK** to confirm the deletion.

   Any actions connected to the deleted action become *unused actions*. The unused actions are presented in a separate branch in the call flow tree. Because the actions are unused, they're ignored when a call is processed by the call flow.

   Example:



4. To delete an unused actions, select it, and then click **Delete Action**.
5. Click**Save**to save the call flow changes.

26.18.6 Reusing an action

The same action can be assigned to results of other actions. For example, the **Busy** and **No answer** results of a **Supervised Transfer** action could both send a call to the same **Voicemail** action.

Reusing an action is always done by assigning an existing action to a result of an action. The resulting action may even be itself. For example, a **Menu** action might present a set of options followed by "…to hear these choices again, press the 8 key". The 8-key result of the Menu action could be assigned to the Menu action itself, thus creating a loop in the call flow.

Because actions are always created with the same name, you should be careful to assign meaningful names to actions to make them distinct. Reusing actions is a lot easier if the actions have distinct names.

There is no limit on the number of times an action can be reused.

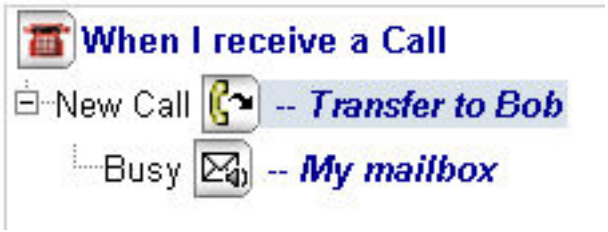
To reuse an action:

The procedure for reusing an action is best explained by example. In the following scenario, we will make the Busy and No answer result of a Supervised Transfer go to the same Voicemail action.

1. Add a **Supervised Transfer** action to your call flow.
2. To the **Busy** result of the new **Supervised Transfer** action, add a **Voicemail** action.
3. Enter the required properties for the **Voicemail** action, including a meaningful name, such as *My mailbox*.

4. Click on the original **Supervised Transfer** action to select it.

   The call flow will look similar to this:



5. Click on the **No Answer** result.

   The resulting menu provides the option of creating a new action and a list of existing actions, including the Voicemail action created in step 2.

6. From this menu, select Voicemail:My mailbox This will assign the **No Answer** result to the same action as the **Busy** result. Your call flow will now look something like this:



   Notice the small arrow at the bottom right of the icon beside the **No Answer** result. This means that the action is an *alias*. An alias acts like a reference to the “real” action elsewhere in the call flow. Clicking an alias selects the action it refers to. Thus, the alias has the same properties as the other action; any change made to the properties of the other action is automatically made to the alias.

7. Click **Save** to save the call flow changes.

26.187 Copying a call flow

A call flow can be copied from one mailbox or line group to another. This can be used in the scenario where a person has changed extensions and the existing call flow needs to be copied to the new mailbox.

Note:

- Only System Administrators are able to copy a call flow.
- To successfully copy a call flow, you must use the menu commands described in the following procedure. Do *not* attempt to manually copy a call flow using a copy-and-paste operation.

An existing call flow can also be copied and saved as a template.

To copy a call flow:

1. From the **Edit** menu on the call flow page, click **Copy From**.

Note:
This menu item is only available in the Web Console.

2. A window requesting you to enter the call flow for a particular mailbox or line group appears. Enter either the mailbox or line group number.

Note:
When the "Copy From" command is invoked from the Call Flow editing window for a mailbox, the feature is limited to copying mailboxes. An Advanced user's call flow can only be copied to another Advanced user's call flow. A Regular user's call flow can only be copied to another Regular user that has the same assigned template. When the "Copy From" command is invoked from the Call Flow editing window for a line group, the feature is limited to copying the call flow for a line group. A line group call flow can be only be copied into another line group.

3. Click **OK**. The call flow and its associated properties are copied into the current call flow.

Note:
When the "Copy From" command is invoked from the create/edit template page in the Web Console, you can copy the call flow from an Advanced mailbox user OR line group into a template for the purposes of creating a new template. In this case, both the "Mailbox" and "Line Group" options are available.

26.188 Deleting a call flow

You can delete an entire call flow. When deleting a call flow, all actions to which the call flow is connected are deleted. All nodes including the nodes in the unused nodes branch will be deleted.

Note:
Only Advanced users and System Administrators are able to delete a call flow.

To delete a call flow:

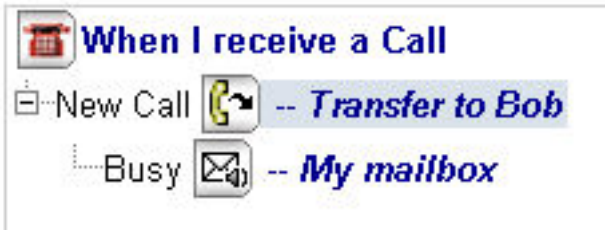
1. Select the call flow you want to delete.
2. From the **Edit** menu on the call flow page, click **Delete Call Flow**.
3. A confirmation window appears. Click **Yes** to confirm the deletion. All nodes including the nodes in the unused nodes branch will be deleted.

26.189 Inserting an action

You may find that you need to add an action to your existing call flow, not at the end of a branch but somewhere in the middle. For example, your existing call flow does not make use of an Override action, but now you want to start off with an Override, while preserving the structure of your existing call flow.

To insert an action:

The procedure for inserting an action is best explained by example. In the following scenario, we build on the example in the Reusing an Action topic. Assuming the following call flow, we will insert an Override action between the When I receive **a call** and **Transfer to Bob** actions.



1. Click When I receive a call. Note that the **New Call** result is the **Supervised Transfer: Transfer to Bob** action.
2. In the **Results** area, click the **Supervised Transfer: Transfer to Bob** link.

3. From the New Actions menu, select **Override** as the new action type.

   The new action item is added to the Call Flow display area and the new Override action is assigned to the New Call result. The entire call flow is moved under Unused Actions as follows (you may need to click the ⊞ sign on the left of the call flow to expand the collapsed branches):



4. Click on the new **Override** action, and then on the **Disabled** result link.
5. Click on Supervised Transfer:Transfer to Bob. This will assign that action to the **Disabled** result of the **Override** action.

   The call flow is re-created under the **Override** action's **Disabled** result and now appears as follows:



6. Assign actions to the **Enabled** result of the **Override** action as required. (These are typically a Message action followed by a Voicemail action.)
7. Click the Save button to save the call flow changes.

26.19 Setting action properties

You can change the properties of an action at any time. The changes take effect immediately after they are saved.

To set the properties of an action:

1. Click the action in the Call Flow that you want to modify.

2. Under Properties for (selected action), make the required changes.
3. Click **Save** to save the call flow changes.

26.191 Setting the prompt language

You can set the prompt language for a call flow.

To set the prompt language:

1. From the Actions menu on the call flow page, click **Set Prompt Language**.
2. A window with the list of available languages appears.
3. Select a language or accept "Auto" as the default value.

> **Note**:
> Use "Auto" to take advantage of the Multilingual Service feature, whereby users are asked to select between up to five prompt languages when the Language Router action is performed.

4. Click **OK**. The selected language will be used for the call flow.

> **Note**:
> Changes to the prompt language are not saved until you press the **Save** button.

26.192 Recording and Importing Messages

Each Message and Menu action in a call flow requires an audio recording. You can add your own recording or, if you are an Advanced user, import an existing one.

> **Note**:
> A maximum of 100 greetings are supported in call flow by Call Director.

Recording Messages in Call Director

Each message is assigned an Action ID by Call Director. The ID is a property of the action and is presented in the Properties area when the action is selected. You are prompted to enter the ID when recording the message. The Actions > Recordings menu item on the Call Flow page lists IDs for all messages in the call flow and shows whether or not the messages have been recorded.

Note: Do not combine greetings and menus in the same recording. If you do, Call Director will not be able to repeat the menu to the caller.

To record a message:

1. Using any touch-tone telephone, log into your NuPoint Unified Messaging mailbox, and press the * key. This will connect your call into the Call Director Telephony User Interface (TUI).
2. As an alternative to pressing the * key, follow the voice prompts to record your message.

Recording a Message for a Single Action

To record a message for a single action:

1. Select a Message or Menu action in the call flow.
2. (Optional) If you want the system to call your extension and allow you to record the message, complete the following steps in the Properties area:

   a. Select the **Call Me** check box.
   b. Enter your extension number in **Call Me Number**.
   c. Click **Save**.
3. Click **Recording**. The Recording Status window opens.
4. Click **Record** under the Actions column.
5. The Record Message dialog opens, prompting you to record your message. The prompts differ depending on whether you have configured a **Call Me Number**:

   - If you have programmed a Call Me Number, the system calls your extension. Answer the call and proceed to the next step to make your recording.
   - If have *not* programmed a Call Me Number, the system prompts you to call in to your NuPoint voice mailbox, log in, and press the * key to access the Call Director Telephone User Interface (TUI). Proceed to the next step to make your recording (you will not receive any voice prompts).
6. In the Record Message dialog, click the **Record** button and then record your message over the telephone. When you have finished recording, click the **Stop** button. To review your message before saving it, click the **Play** button. After you have finished recording your message, click **Save** to exit the Record Message dialog.
7. Click **Close** to exit the Recording Status window.

Note:
You cannot use Call Me functionality to record messages for multiple actions or Line Group call flows, or to edit Templates.

Recording a Message for Multiple Actions

To record a message for one or more actions:

1. Select **Actions > Recordings**. The Recording Status window opens.
2. Locate the messages you wish to record and click **Record** under the Actions column.
3. A dialog opens, prompting you to call in to your NuPoint voice mailbox, log in, and press the * key to access the Call Director Telephone User Interface (TUI).
4. Use the TUI to specify an action ID and record your message.
5. After you have finished recording your message, click **Close** to exit the Recording Status window.

Note:

- If you call in to your mailbox, as an alternative to pressing the * key, you can simply follow the voice prompts to access the Call Director TUI and record your message.
- You can also record a message from the **Actions > Recordings** menu item on the call flow page or from the Recording button in the Properties area of the call flow page.
- There are two methods to call into your mailbox and record the Daily Greeting for the call flow:
- Press the * key to access the Call Director TUI. Use the TUI to navigate through the system and record the message.
- Access the User Options menu and select Greetings (4) and Record Daily Greeting (8).

Importing Greetings into Call Director

Instead of recording greetings, you can also import a recorded greeting (prompt). Once the prompt has been imported, it is treated like any other recorded prompt.

Note:

- Only Advanced users and System Administrators are able to import recorded prompts.
- To be imported into a call flow, audio recordings are required to be in 8-bit, 8 KHz u-law or a-law format. Audio files recorded in any other format must be converted to this format before attempting the import function. In addition, the recording duration of the file being imported cannot exceed 5 minutes.
- The audio file must be in 8k u-law or 8k a-law format. If the file being imported is not in this format or does not exist, the Status will show "Import Error" and the file name controls will remain displayed for that prompt. An error message "Please specify a valid 8k u-law or a-law audio file" will also be displayed.
- If you are unable to import the audio file (indicated by a failure to save the recording or call flow), verify that your web browser security settings are correct. To do this, click the**Start**button and type**Internet Options**in the search box. Select the**Security**tab and click the**Custom Level**button. In the**Miscellaneous**section, ensure that**Display mixed content**is set to**Prompt**. If**Display mixed content**is disabled, file import will fail.

To import a recorded prompt:

1. Select **Actions > Recordings**. The Recording Status window appears showing the list of prompts. A status of "Recorded" or "Not Recorded" is displayed in the Status field.
2. Select the item for which you want to import a prompt and click **Import**.
3. A new File option appears in the window. Type the name of the filename or browse to the appropriate prompt file.
4. Click **Sta rt Import** to import the prompt.

Note:
You can import a prompt one at a time, or specify all the prompts to import and then press the "Start Import" button.

26.193 Viewing call flow paths

You can view all the unused paths of a specific call flow. An unused path is an action, such as a Menu key, that does not have a result programmed.

To view the call flow paths:

1. From the View menu on the call flow page, click **Show All Paths**.
2. The call flow will expand to show all the unused paths within the call flow.

> **Note**:
> Once all paths are shown, the menu item will change to "Hide Unused Paths".

3. To hide the unused paths, click **Hide Unused Paths**.

26.194 Printing call flows

You can print an entire call flow, including its unused paths.

To print a call flow:

> **Note**:
> To include unused paths in the printout, click **Show All Paths** from the View menu prior to commencing the procedure.

1. On the call flow page, click **Print Callflow**.
2. Access the print preview dialog by entering the appropriate keyboard shortcut, such as **Control + P** in Windows or **Command + P** in Mac.
3. In the print preview dialog, select a **Destination**. You may send the printout to a regular printer or save it to file (PDF or XPS).
4. Click **Print**.

> **Note**:
>
> - If you receive a certificate error which prevents the print preview from displaying correctly, click **Show Content** at the bottom of the dialog.
> - If you are saving the printout to file, follow the prompts to assign a name and location for the document.

26.195 About Call Director Reports

Several Call Director reports can be generated from the **Reports** menu of the Web Console.

The access to the reports has changed since most mailbox users will not have access to the full call flow editing interface, and thus the Reports feature will no longer be present there.

The following reports can be generated:

- Call Flow Report
- System Reports (which include a Mailbox System Report, Line Group System Report, and a combined System Report).

26.195.1 View a Call Flow Report

The report for a call flow contains statistics on how a call travels through the call flow. All call flows generate call flow reports that you can access. The report contains records of each call and how it was handled.

Note:
Programming changes to a call flow automatically clears the call flow report.

To view a Call Flow Report:

1. From the navigation tree, click **Call Director**, and then click **Reports**.
2. Click **View Call Flow Report**.
3. Select **Mailbox** or **Line Group** from the Call Flow drop-down menu.
4. Enter the number of the mailbox or line group call flow.
5. Click **View**.
6. The Call Flow Statistics window opens with the report criteria.

Note:
You can also view a call flow report when you are editing a call flow by selecting View Report from the Reports menu.

The following table lists the information in a call flow report:

Statistic	Meaning
Internal Calls	Number of incoming internal calls.
External Calls	Number of incoming external calls.
Total Calls	Total number of incoming calls.
Hourly Totals	Number of calls received during each hour.

For each action in the call flow, the following summary is provided:

Name	Name of the action used in the call flow.
Type	Type of action (e.g. Call Transfer; Greeting; etc.) applied to the call.
ID	A unique number assigned to the call flow action by Call Director.
Entry Count	The number of times a call flow action was entered.
Exit Count	The number of times each result of the call flow action was invoked.

26.195.2 Reset a Call Flow Report

You can reset a report without having to edit the call flow. You can reset a specific report or all reports at once. Once invoked, the report values are reset to 0.

Note:
Programming changes to a call flow automatically resets the call flow report.

To reset a specific report:

1. From the navigation tree, click **Call Director**, and then click **Reports**.
2. Click **Reset Call Flow Report**.
3. Select **Mailbox** or **Line Group** from the Call Flow drop-down menu.
4. Enter the number of the mailbox or line group call flow.
5. Click **Reset**.
6. A confirmation message appears indicating that the selected report values have been reset.

To reset all reports:

1. From the navigation tree, click **Call Director**, and then click **Reports**.
2. Click **Reset Call Flow Report**.
3. Click **Reset All**.
4. A confirmation message appears indicating that all report values have been reset.

26.195.3 Run a System Report

The following system reports can be generated:

- Mailbox System Report
- Line Group System Report
- **Combined System Report** (a combined report of the mailbox and line group statistics; the mailbox statistics will appear first and the line group statistics will appear second)

Reports are generated in a .csv file which has the following format: **reportnamedate.csv**. (For example, a mailbox report that was run on February 2nd, 2007 will have the following naming convention: **MailboxReport_2007_2_2.csv**)

Note:
When you generate a System Report you are given the option to Save or Open the file. If you click Save, the report is saved and you can open and view it. However, if you click Open, the file is empty.

To run a system report:

1. From the navigation tree, click **Call Director**, and then click **Reports**.
2. Click **Run System Report**.
3. Select the type of report to run by clicking the appropriate report button.
4. The File Download window appears.
5. Click **Save** and then specify a location for the file.
6. Click **Save** again.
7. The report is now saved to the specified location.

The following report criteria are listed within the system reports:

- Mailbox or Line Group Number
- Start Date & Start Time
- Report Date & Report Time
- Total Minutes
- Total Calls
- Total Successful Call Transfers
- Total Failed Call Transfers
- Total Hang Ups
- Hourly Totals (24 hours)
- Menu Key Presses (0-9)

26.19.6 About Call Flow Reports

All call flows generate call flow reports that you can access. The report contains records of each call and how it was handled.

Note:
Programming changes to a call flow automatically clears the call flow report.

Note:
Only Advanced users and System Administrators have access to the Reports menu from the full call flow-editing interface.

The following table lists the information in a call flow report:

Statistic	Meaning
Internal Calls	Number of incoming internal calls.
External Calls	Number of incoming external calls.
Total Minutes	Total length of telephone calls in minutes.
Total Calls	Total number of incoming calls.
Hourly Totals	Number of calls received during each hour.

For each action in the call flow, the following summary is provided:

Name	Name of the action used in the call flow.
Type	Type of action (e.g. Call Transfer; Greeting; etc.) applied to the call.
ID	A unique number assigned to the call flow action by Call Director.
Entry Count	The number of times a call flow action was entered.
Exit Count	The number of times each result of the call flow action was invoked.

26.196.1 Viewing a Call Flow Report

All call flows generate call flow reports that you can access.

To view a Call Flow Report:

1. From the Reports menu on the call flow page, click **View Report**.

> **Note**:
> Only Advanced users and System Administrators have access to the Reports menu from the full call flow-editing interface.

2. The Call Flow Statistics report opens in a new window.

26.196.2 Resetting a Call Flow Report

A Call Flow Report can be reset without having to edit the call flow. Once the reset is invoked, the report values are reset to 0.

> **Note**:
> Editing a call flow will cause the report to reset.

To reset a Call Flow Report:

1. From the Reports menu on the call flow page, click **Reset Report**.

> **Note**:
> Only Advanced users and System Administrators have access to the Reports menu from the full call flow-editing interface.

2. A confirmation message appears indicating that the report has been reset.
3. Click **OK** to clear the message.

26.197 About MiCollab Client

MiCollab Client is an application that converges Mitel communication platform call control capabilities with Dynamic Status, presence, contact management, and collaboration to simplify and enhance real-time communications.

Note:
MiCollab Client functionality described in documentation refers to enterprise **as a single company entity**. In scenarios where multiple server domains are created, it is understood to be within a single company environment where multiple MiCollab Client Services or mixed PBX nodes are required to manage the solution.

Users can access MiCollab Client features from the following interfaces:

- MiCollab for PC Client
- MiCollab for Web Client
- MiCollab for Mobile Client
- MiCollab for MAC Client
- MiCollab for Microsoft Client

MiCollab Client user interfaces support several languages.

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English (US)
- English (UK)
- French (Canadian)
- French (European)
- German
- Italian
- Portuguese (European)
- Portuguese (Brazilian)
- Russian
- Spanish (European)
- Spanish (Latin American)
- Swedish
- Norwegian
- Finnish
- Danish

User documentation for MiCollab Client is available in the following languages:

- Dutch
- English (US)
- French (Canadian)
- French (European)
- Italian
- Portuguese (Brazilian)
- Portuguese (European)
- Spanish (Latin American)
- Spanish (European)

- Swedish
- Norwegian
- Finnish
- Danish
- German
- Chinese

MiCollab Client is integrated with other Mitel applications.

- **MiCollab Audio, Web and Video Conferencing (formerly known as Mitel collaboration Advanced)**: Access to MiCollab Audio, Web and Video Conferencing is integrated within MiCollab Client. When users are licensed for MiCollab Audio, Web and Video Conferencing , they can use collaboration features such as real-time audio and Web conferencing, annotation, chat, file transfer, and desktop sharing.
- **MiCollab Unified Messaging™ (UM)**: Provides access to NuPoint UM voice mail and FAX messages from the Desktop Client's Visual Voice Mail view. Voice mail messages can also be retrieved from the MiCollab Client Web/Mobile Portals, MiCollab Mobile Client for Android and MiCollab Mobile Client for iOS.
- **MiVoice Border Gateway**: Provides a secure communications path for remote MiCollab Client softphones and IP desk phones to the Unified Communications server. *This product is supported for MiVoice Business communication systems only*.
- **Mitel Web Proxy v2.0**: Web Proxy provides a secure communications path from remote users to the MiCollab Web Clients. *This product is supported for MiVoice Business communication systems only.*

See the Administrator Tasks topics for basic administrator and links to task-related instructions.

See the Administrator Interface topic for a description of the UI elements in the MiCollab Client Service Administrator pages.

Note:
For instructions on how to integrate the MiCollab Client database into the USP database using the MiCollab Client Integration Wizard, refer to the *MiCollab Installation and Maintenance Guide*.

MiCollab Client Service Administration Page

This page includes the following sections:

- **Configuration**:

  Provides a button that links to the administration tabs and associated pages. Click **Configure MiCollab Client Service**to access.

Note:

While configuring, the MiCollab Client Service must use an FQDN of 57 characters or less.

- **Status**:

  Provides the current status for the MiCollab Client Service , and the ability to start, stop, or refresh the server. For Server Status, the name of the server is displayed along with one of the following:

  - **Active**: The server is online and operational.
  - **Becoming Active**: The server is in the process of coming online.
  - **Idle**: The server is offline and not operational.

  To start, stop, or refresh the server:

  1. Select an action from the list box:
     - Start Mitel MiCollab Client Service
     - Stop Mitel MiCollab Client Service
     - Refresh Status
  2. Click **Perform Requested Action**.

- **Client Versions**:

  Under the MiCollab Client Service, the Client Versions section lists all the MiCollab Client software versions that are available on the server for the particular release.

  The administrator also has an option to enable/disable the feature to Upgrade PC Clients from Cloud. By default, this setting would remain enabled in the server, which means that all users will upgrade their clients from Cloud unless the administrator explicitly disables the option.

Note:

Even if the **Upgrade PC Clients from Cloud** option is selected, and there is a newer version of PC clients available on the server and not on Cloud, the end-users will receive a notification pop-up for upgrading their PC Clients. The end-users will not have any back-end information regarding the notifications that they receive, whether the upgrade is getting done from the Cloud or from the server.



Note:

With MiCollab Release 9.7 onward, MiCollab Client for Windows Desktop (Legacy Client) will not be a part of MiCollab Client Service build and the users cannot download Legacy Client in their system from the MiCollab server. This change will not impact the existing users of Legacy Client, as they continue to use the same feature as before.

If you try to upload Legacy Client rpm, the following error message will be displayed.



Note:

The feature to Upgrade Clients from Cloud is only applicable for PC Clients.

The MiCollab Client software stored on this server may be upgraded or downgraded without requiring an upgrade of the MiCollab Client service.

To perform an upgrade or downgrade of a supported MiCollab Client:

1. Under **Applications**, click **MiCollab Client Service**.
2. In the New Client Package field, click the **Browse**button and navigate to the MiCollab Client package to be uploaded.
3. Click **Upload MiCollab Client**.
4. The list of installed MiCollab Client software will automatically be refreshed with the updated version information.

Note:

The MiCollab Client Service Administration page accepts only .rpm format when uploading MiCollab Client software.

- **Diagnostics**:

  The Diagnostics section of the page provides access to diagnostics tools. Click **Perform Server Diagnostics**to access diagnostics tools.

  Note:

  Do not use the MiCollab Client Service Diagnostic tools unless you are instructed to do so by Mitel technical support personnel.

- **Import Data**:

  Allows you to import MiCollab Client Service data from an already backed-up file. If you have a backup file generated on a MiCollab Client Service, use this form to restore the data.

Note:
MSL configuration information (network information, hostname, and so on) contained in the backup file will be ignored.

Importing data using this option will overwrite all MiCollab Client Service configuration information and reinitialize the MiCollab Client Service database to the values stored in the specified backup file.

To import the data file:

1. Under **Import Data File**, click **Browse**.
2. Navigate to the backed-up form file, select the file and click **Open**.
3. Click **Import MiCollab Client Service Data**.

- **Reinitialize System**:

Selecting the Reinitialize MiCollab Client Service Configuration, reinitializes the configuration of the MiCollab Client Service.

Note:
Selecting this option will remove all MiCollab Client Service configuration information and reinitialize the MiCollab Client Service database.

To reinitialize MiCollab Client Service configuration:

1. Click **Reinitialize MiCollab Client Service Configuration**.
2. Click **OK**.

- **RC4 Setting**:

Rivest Cipher 4 (RC4) is a stream cipher that protects confidential data messages sent to and from secure URLs. However, RC4 has multiple vulnerabilities and the Payment Card Industry Data Security Standard (PCI DSS) recommendation is to disable it.

For MiCollab 8.1 or later, by default, RC4 is disabled. For earlier releases, RC4 is enabled by default and the administrator must disable it to be compliant with Payment Card Industry Date Security Standard (PCI DSS). Enabling or disabling this option may impact presence and ongoing chats, so change this setting outside of business hours. To change the setting:

1. Clear the box to disable or check the box to enable.
2. Click **Save RC4 Setting**.

Note:
If MBG is acting as a gateway for connections from a MiCollab server, there may be a requirement to enable RC4.

- **MiVB (MiXML/MiTai) Security Setting**:

  Enable **MiVB (MiXML/MiTai) Security Setting**to support public and corporate certificate for MiXML and MiTai connections towards MiVoice Business .

  Before enabling security setting, make sure prerequisites are met and take note of limitations.

  Prerequisites:

  - MiVB version is 8.0 or higher.
  - Public certificate or corporate certificate **signed by same authority**is installed on both MiVB and MiCollab Server.
  - MiVB FQDN or IP address must be included in subject or subject alternate name in the certificate.

Note:
If prerequisites are not met, PBX synchronization and MiTai connection will fail.

Limitations:

- Wild card domain names are supported in common name only.
- Self signed certificate is not supported.

By default, MiVB (MiXML/MiTai) setting is disabled. To enable the setting:

1. Check **Enable MiXML MiTai Security Setting**checkbox.
2. Click **Save MiXML MiTai Security Setting**.

Note:
In public certificate, IP address is not supported. If public certificate is used, administrator must program MiVBs with MiVB FQDN in MiCollab.

Note:
For MiVB 8.0 release, web server certificate signed by same authority needs to be installed.

Note:
For MiVB 9.0 release, web server certificate and device certificate, signed by same authority needs to be installed.

- **Federation Service Setting**:

  Click **Enable Federation Service Setting** to enable the federation service in MiCollab Client Service.

  Note:
  Enabling or disabling the federation service will restart MiCollab Client Service.

  By default, the Federation Service Setting is disabled. To enable the setting:

  1. Check **Enable Federation Service Setting** checkbox.
  2. Click **Save Federation Service Setting**.
  3. Click **OK** on the prompt to restart MiCollab Client Service.

- **MiTAI UTF-8 Support**:

  Enable MiTAI UTF-8 Support to get UTF-8 characters in CDRs (name fields) from MiVB. Before enabling this setting, make sure all MiVBs connected to this server are running on version 9.0 or later.

  By default, MiTAI UTF-8 support setting is disabled. To enable the setting:

  1. Check MiTAI UTF-8 Support checkbox.
  2. Click Save MiTAI UTF-8 Setting.
  3. Click OK on the prompt to restart PBX Proxy. PBX Proxy will automatically restart in the background.

Note:
If the configured MiVB version is not available or lower than 9.0, administrator cannot enable the MiTAI UTF-8 Support setting.

Note:
If the MiTAI UTF-8 support setting is enabled and the administrator provisions MiVB (lower than MiVB 9.0), the server will raise a critical alarm during next PBX sync. The administrator must disable this setting or upgrade MiVB version to 9.0 or later. After the configuration is updated, clear the alarm from the event log.

26.197.1 What's New in MiCollab Client

For a list of new functionality, see MiCollab What's New Guide in the Mitel Customer Documentation site, the Document Center.

Note:
For additional details about end-user MiCollab Client's new features and enhancements, refer to the *online Help* for the specific interface or the *Mitel MiCollab Client Administrator Guide* available on the Mitel Document Center Web site.

26.197.2 Requirements

This topic provides basic requirements for the MiCollab Client product. For additional details, refer to the *Mitel MiCollab Client Administrator Guide* available on the Mitel Document Center Website.

Server Requirements

The MiCollab Client Service resides as either a stand-alone application on a Mitel Standard Linux (MSL)-approved hardware platform or an integrated application in the MiCollab. There are three options for the MiCollab Client Service component:

- Purchase an approved MSL hardware platform, download, install, and configure the required MSL operating system and MiCollab Client Service blade on site.
- Purchase and install the Virtual MiCollab Client software package to run on a VMware-approved hardware platform.

The information below lists the server requirements:

Component	Requirement	Version
Hardware Platform	An approved Mitel Standard Linux (MSL) hardware platform.	
Operating System	Mitel Standard Linux (MSL)	Latest released version
Virtualization	VMWare® ESXi™ version 7.0	Refer to the Virtual Appliance Deployment Guide
	VMWare vSphere™ version 7.0 and 8.0	
	Nutanix AOS version 6.5.4	
Software Blade	MiCollab Client Service	Latest version

Note:
Virtualization:

- For information about installing and configuring VMware ESXi on the hardware platform, refer to the VMware documentation supplied with the product.

Communication Platforms Requirements

To use MiCollab Client , users must be configured with a desk phone, softphone, or both on one of the following Mitel communication platforms and versions:

- MiVoice Business v9.4 SP or higher
- MiVoice Office 250 v6.3 SP5
- MiVoice Office 400 v7.0 SP1 or higher
- MiVoice 5000 v8.1 SP1 or higher
- MiVoice MX-ONE v7.5 or higher

When deployed in a MiCollab environment, MiCollab Client can be integrated with MiVoice 5000 6.1 SP2 or later and MiVoice MX-ONE Release 6.0 SP2 or later. Refer to the *MiCollab Installation Guide* for more information.

MiCollab Client Requirements

MiCollab Desktop Client

The MiCollab Desktop Client provides the full suite of MiCollab Client features. To install and use the MiCollab Client Desktop Client, users must have a computer that meets the documented computer requirements.

Component	Requirement	Version
Central Processing Unit (CPU)	Dual Core, 1.6 GHz minimum	
Hard Disk Space	100 MB free hard disk space	

Component	Requirement	Version
Random Access Memory (RAM)	2 GB minimum (4 GB or more recommended)	
Network Interface Card (NIC)	10/100/1000 Mbps full duplex required (100 Mbps full duplex recommended)	
Sound Card	Full Duplex	
Digital Media Player	Windows Media® Player	6 or later
Operating system (OS)	Microsoft Windows 10 and 11	32 or 64-bit
Microsoft Office Application(s)	Office 365	
Thin Clients	Citrix XenApp 7.23 VMware Horizon – 7.11 or later	
Remote Desktop Services (formerly Windows Terminal Services)	Windows Server 2022	
Microsoft Add-on	Microsoft .NET ™ Framework	4.7 and 4.8.1

* The thin client environment does not support the embedded softphone and video call feature.

A USB headset or handset is required to use the MiCollab Client embedded softphone.

Supported USB handsets include:

- VoipVoice® Cyberphone 654

Supported USB headsets include (see MiCollab Client Engineering Guidelines for a complete list of Plantronics supported headsets):

- Jabra® GN 2000 USB
- Jabra GN 2100 USB
- Plantronics® CS50-USB
- Plantronics Blackwire C610

Note:
Supported Headsets and Handsets were tested with the MiCollab Client product. However, there are known limitations:

Volume adjustments made on a Plantronics headset during an active call are not reflected in the active call window.

Jabra GN 2000, 2100 and Plantronics Blackwire C610: Mute button is not functional even if configured.

Jabra GN 2000: While on an active call, the Audio does not automatically recover if the headset is unplugged and plugged back in.

Note:
Effective in MiCollab Client 6.0 SP2, when selecting Plantronics headsets under Softphone Settings (Desktop Client configuration), some functionality are pre-defined: Call Answer, Call End, Mute and Unmute.

MiCollab Client inter operates with the following software:

- **Supported Personal Information Managers**

  The following Personal Information Managers (PIMs) are supported for use with MiCollab Client :

  - Act! 2008 & 2011
  - Lotus Notes R8.0, R8.5, 8.5.2 and 9.0
  - Outlook 2013, 2016, 2019 and O365 (32 and 64 bit)
  - Google Calendar and contact integration
- Supported Instant Messaging Applications

  The following Instant Message (IM) clients are supported for use with MiCollab Client :

  - Lync 2013

MiCollab Client integrates with Google (Calendar and Contacts), Microsoft Exchange Server, or Microsoft Graph Server.

MiVoice for Skype for Business

MiVoice for Skype for Business is an application that integrates with Skype for Business and allows Skype for Business users to use Mitel telephony features through its feature rich MiCollab Client infrastructure.

MiCollab Client Web Portal

The MiCollab Client Web Portal provides remote access to a subset of MiCollab Client features from one of the following supported Web browsers :

- Microsoft Edge 115 or higher
- Mozilla Firefox 115 or higher
- Apple® Safari 15.5 or higher
- Google Chrome 115 or higher

MiCollab for Mobile for Android

MiCollab for Mobile for Android is a stand-alone client that users install on their Android mobile phones. The client provides automatic Dynamic Status updates based on the user's current location. Location options include GPS and Bluetooth. In addition, the client provides access to call logs, messages, and Corporate Contacts.

MiCollab for Mobile for iPhone client application provides Dynamic Status updates based on time and GPS location. In addition, MiCollab for Mobile provides an integrated environment in which you can communicate with corporate contacts, and access and manage visual voice mail and call history.

MiCollab Audio, Web and Video Conferencing Collaboration Product

When integrated with MiCollab Client, MiCollab Audio, Web and Video Conferencing (formerly known as Audio and Web Conferencing - AWC) provides users with conferencing, chat, annotation, document transfer, desktop and application sharing, and other collaboration features in real time. Collaboration is a licensed feature and must be purchased for MiCollab Client .

MiCollab UC-Client

MiCollab UC-Client (previously known as MiCollab Mobile) is still available.

Note:
Refer to the *MiCollab Client Engineering Guidelines* for supported versions.

26.197.3 About Licensed Features

Below are the list of licensable features for MiCollab Client. Two of the features are server-level licensed features:

- **Federation**: Considered to be "in use" at all times.
- **Peering**: Considered to be "in use" at all times.

The below table provides descriptions for all licensed features.

Feature	Description
Auto Answer	Incoming calls are answered at the first ring by the selected device (Desk Phone or Softphone). Users enable and disable this feature from the Dynamic Status dialog box on the Desktop Client. **Note**: Auto Answer conflicts with the Dynamic Extension Express feature on the MiVoice Office 250 PBX. **Note**: Auto answer is not supported on SIP soft phones.
Call Forwarding	The Call Forwarding feature allows users to: • forward to any non-PRG destinations. • add preferential routing. • send calls to dynamic extensions. When users are not licensed for Call Forwarding, they can still send calls to their desk phones, softphones, and voice mail. In addition, users can set Do-Not-Disturb and Auto Answer options.
Chat	Users can participate in online chat sessions with other MiCollab Client users also licensed for chat. Users access the **Chat** sub menu from the Corporate Contacts context menu.
Collaboration Integration	Users can access MiCollab Audio, Web and Video Conferencing (formerly known as Audio and Web Conferencing - AWC) features from the **Collaboration** submenu (available from the main menu) and the **Start Collaboration** option from the Corporate Contacts context menu.

Feature	Description
Compact Mode	Users can switch between the full mode and compact mode Desktop Client interfaces.
Console Option	Users have access to the Console from the Desktop Client main menu. The Console provides access to attendant functions such as answer, transfer, hold, and the ability to view and change another user's status. By default, console users run in Universal presence mode. **Note**: This feature must be purchased. Also, users who are licensed for the Console Option automatically have Universal Presence enabled for all local corporate contacts. This excludes contacts from peered MiCollab Client Services and external IM servers.
Desk Phone	Users' desk phone extensions, as programmed on the PBX, are integrated with MiCollab Client. **Note**: This feature must be purchased. Also, purchasing x licenses of this features automatically provides x number of all of the non-purchasable features.

Feature	Description
Desktop client SDK	This license is required for MiVoice for Skype for Business feature. **Note**: MiVoice for Skype for Business Deskphone only users: those users only require the Desktop client SDK feature. MiVoice for Skype for Business Softphone only users OR those users with a Softphone and an associated Deskphone will require the Softphone feature in addition to the Desktop client SDK feature.
Do-Not-Disturb (DND)	Users can enable and disable DND for each type of Dynamic Status. When DND is enabled, callers receive a busy tone and a Do-Not-Disturb message and incoming calls are not logged in the call log. Users enable and disable this feature from the Dynamic Status dialog box on the Desktop Client.

Feature	Description
Dynamic Status	Users can add statuses and configure the following Dynamic Status elements: • Status Name (for example, **In the office** or **Gone for the day**) • Optional custom text • Instant Message availability and Instant Message availability and auto reply • Preferential Routing • Phone Settings (DND and Auto Answer) Users can manually change their Dynamic Status at any time using the MiCollab Client interface. The new status is then communicated to other MiCollab Client users. In addition, Dynamic Status is also automatically updated in response to the user's Outlook calendar entries. **Note**: This feature must be purchased.
External Dial	Users can dial an external number from an integrated application such as Microsoft Word, Outlook, and Internet Explorer. The user may need to complete some configuration in the application to enable external dialing.

Feature	Description
Federation	The Federation feature provides MiCollab Client users with expanded IM capabilities. When the MiCollab Client Service is licensed for this feature, you can configure federation for the Enterprise on the Federation Tab, and users can view IM presence and chat with federated IM contacts using the Desktop Client's Chat window. **Note**: This feature must be purchased and is a server-level license. Therefore, it will not appear in any feature profiles. Also, MiCollab Client 4.0 IM server support is limited to Microsoft Office Communicator Server (OCS) 2005, and 2007 R2, and IBM Lotus Same time Server 8.5 and 8.5.1.
Knowledge Management	Users can index computer files and documents associated with a contact. When the user receives and incoming call, the Knowledge Management popup window appears presenting the user with a list of files associated with the caller including e-mail messages, contact entries, and documents (Microsoft Word, Excel ®, PowerPoint ® , Outlook and Adobe ® Portable Document Format).
Launchpad	Users can access the Launchpad view, which provides quick access to frequently completed actions, from their Desktop Client. Actions include dialing a number, browsing to a URL, running a program, and exploring a folder. **Note**: This feature is only compatible to legacy clients.

Feature	Description
Mobile Handoff	Users on Mobile device can use the Call Handoff feature (ability to push a call to other devices within the Personal Ring Group). This feature is limited to users on MiVoice Business communication platforms only. **Note**: **Handoff Feature Code**: As a prerequisite, the MiVoice Business Feature Code for Handoff must be programmed. If this feature is added to an existing server, the PBX need to be synchronized with MiCollab Client before the feature can be used (also see Synchronization Tab).
Mobile SIP Softphone	Allows user to have SIP-Based Softphone on Android and iOS clients. This feature is supported on MiVoice Office 250 and MiVoice Business systems only (MiVoice Business 5.0 SP2 and later release). **Note**: You must have the " MiCollab Mobile Client for Smart Devices" license enabled before you can enable the "Mobile SIP Softphone" license.
Office Communicator Integration	Users can send and receive instant messages using the Microsoft Office Communicator IM client, from the Desktop Client. Similar to the Chat feature, users can access the Office Communicator submenu from the Contacts context menu.

Feature	Description
Peering	The Peering licensed feature allows you to configure communication paths with other MiCollab Client Services for the purposes of sharing presence information and providing communication features between Enterprises. **Note**: This feature must be purchased and is a server-level license. Therefore, it will not appear in any feature profiles.
Phone Button Programming	Users can configure the buttons on their IP phone from the Mitel Integrated Configuration Wizard. This feature is limited to users on MiVoice Business communication platforms only.

Feature	Description
Presence	MiCollab Client Service uses **Dynamic Presence** (which is a replacement for Universal and On-Demand Presence) for telephony presence. The Desktop client will display presence for the contacts in the current view. **Note**: Console users will see presence information for all your corporate contacts. **Note**: An account with a Deskphone, Softphone, Stand-alone Web Portal, or Mobile Client for Smart Devices license has telephone presence even when the Presence feature is not selected in the feature profile. **Note**: With the introduction of MS Teams integration with MiCollab, a new Presence state, called as the External Presence State has been introduced. MS Teams will have fixed External Presence Status and when the dynamic status is enabled, the External Status will be set to either, Away, Busy, or Default.
Presence on Mitel Sets	Users can configure presence information for multiple contacts on their Desktop Client. This feature is limited to users on MiVoice Business communication platforms only.

Feature	Description
Presence on Mitel InAttend	InAttend Users can view presence* information for contacts associated with MiCollab Client. **Note**: This feature is limited to users on MiVoice MX-ONE and MiVoice 5000 communication platforms only.
Softphone	Users' softphone extensions, as programmed on the PBX, are integrated with MiCollab Client. **Note**: This feature must be purchased.
Stand-alone Mobile Web Portal	The Mobile Web Portal provides users with remote access to a subset of MiCollab Client features, such as configure and change their Dynamic Status, access call history data, view corporate contacts, accessing voice mail messages, and configure account options.
Stand-alone Web Portal	The Web Portal provides users with remote access to a subset of MiCollab Client features, such as configure and change their Dynamic Status, access call history data, view corporate contacts, access voice mail messages, and configure account options.

Feature	Description
MiCollab Mobile Client for Smart Devices	Users can install and use the MiCollab Mobile Client application on their Android, iPad, or iPhone mobile device. The MiCollab Mobile Client application provides Dynamic status updates based on location, time, WiFi, GPS and/or Bluetooth (depending on the device). The application also provides an integrated environment in which users can manage Dynamic Status, communicate with corporate contacts, and access visual voice mail and call history. The MiCollab Mobile Client for Smart Devices was formally known as the Locator.
Video Calls	Users have access to video presence for Corporate Contacts and can participate in point-to-point and multi-party video sessions. Video services for the MiCollab Client Desktop Client are provided by Mitel MiCollab Audio, Web, and Video Conferencing.
Visual Voice Mail	Users have access to the following NuPoint UM voice mail features from the Visual Voice Mail view: • Receive message waiting indications • Play, forward, and delete voice mail messages • View, forward, and delete fax messages • Change the voice mail PIN **Note**: This feature requires the user's mailbox to be configured on the NuPoint UM voice mail system.

* MiCollab Telephony Presence is not supported in InAttend.

26.197.4 Teamwork Mode

Teamwork Mode provides the ability for a user to have certain MiCollab Client functions without having a Mitel phone. In other words, a user will still be able to use certain non-telephony based features within the client even though the user does not have a desk phone or softphone.

Note:
Prior to release 5.1, a MiCollab Client user without any devices online and a hot desk user that was not logged in would go into offline mode. However, as of MiCollab Client 5.1 if the user has no devices associated with their account, they automatically go into Teamwork Mode.

Licensing: There are no new or additional licenses required specific to the Teamwork Mode feature. Licenses for individual features such as Chat, Visual Voicemail, etc...are still required.

26.197.5 Provisioning MiCollab Client

After you install and configure the MiCollab Client blade on the MSL server, you must provision the MiCollab Client system using the MiCollab Client Service administrator interface.

Follow the steps below, in order, to provision the MiCollab Client system using the MiCollab Client Service administrator interface:

1. Create an Enterprise.
2. Add Feature Profiles.
3. Add PBX nodes.
4. Add collaboration servers (*optional*).

Note:
The Unified Communicator Express/YA Collaboration Module is no longer a supported collaboration product for MiCollab Client .

5. Configure the Enterprise fields and options.
6. Add user accounts using one of the following methods:
   - Add user accounts automatically by configuring an AD/LDAP Synchronizer, and then completing a manual synchronization. Refer to the Licensed Features and Synchronization topic for details.
   - Add user accounts automatically by configuring a PBX Node Synchronizer, and then completing a manual synchronization. Refer to the Licensed Features and Synchronization topic for details.
   - Add user accounts manually by clicking Add Account from the Accounts tab. Accounts that you create manually are not affected if you later configure an AD/LDAP or PBX Node Synchronizer and then complete a synchronization.
7. Configure Automatic Call Distribution (ACD) settings (*optional*).
8. Configure Peering with other MiCollab Client Services or external servers (*optional*).
9. Configure IM and presence Federation (*optional*).
   - When you configure federation from the Peering tab, federated contacts are displayed in a separate list in the user's corporate directory from the Desktop Client's Contacts View.
   - When you configure federation from the Federation tab, instruct users to manually add the federated contacts to the Desktop Client. Users should create a new personal contact, and then add the IM

login information (for example, john_smith@ocs.com) for the contact using the **MiCollab Client Login** option.

10. Send a Welcome E-mail Message to MiCollab Client users.

The procedure above covers the configuration required in the MiCollab Client Service Administrator Interface ***only*** . It ***does not*** cover the additional configuration required at the site. Click here to read more.

The MiCollab Client product is integrated with the site's communication platform and network. In addition, this product can be integrated with other Mitel applications. Therefore, configuring and deploying the entire system requires access to network and telephone equipment, communication system software, and peripheral software products. The entire deployment process involves the following high-level tasks:

1. Configure the PBX for MiCollab Client .
2. Install and configure the integrated Mitel applications.
3. Install and/or configure the MiCollab Client Service component. (Procedure varies based on MiCollab Client Service deployment type.)
4. Access the MiCollab Client Service Administration page.
5. Provision MiCollab Client as documented in this topic.
6. Install MiCollab Client software.
7. Configure access for remote users.

For comprehensive information about all of the tasks required for MiCollab Client deployments, refer to the *MiCollab Client Administrator Guide*, available on the Mitel Document Center Web site.

26.197.6 Maintaining MiCollab Client

MiCollab Client administrator maintenance tasks are described briefly below. For comprehensive maintenance information, refer to the *MiCollab Client Administrator Guide* available on the Mitel Document Center Web site.

Server and Client Upgrades

To upgrade MiCollab Client , download and install a new MiCollab Client Service software blade. The blade contains the client software `.msi` file. This file must be deployed to users to complete the upgrade.

MiCollab Client Service Administration

To access the MiCollab Client Service Administration page, click **MiCollab Client Service** under Applications in the MSL Server Manager navigation panel. This page provides access to MiCollab Client Service administrator tasks.

MSL Server Manager Administration

The MSL Server Manager Administration menu provides options for the following server-related tasks :

- **Backup**: Performs a backup of the MSL server (and MiCollab) data.
- **View log files**: Allows you to view log files. Select a log file from the Choose a log file to view list, and then click **Next**.

- **Event viewer**: Shows the current alarm state for the system, followed by a number of events recorded depending on the current age setting for the page.
- **System information**: Allows you to set access privileges to the system information about your server. After enabling the service, click the link to view the information.
- **System monitoring**: Allows you to view monitoring graphs, which can help you analyze the system's performance.
- **System users**: Allows you to add, modify, or remove administrator users for the server.
- **Shutdown or reconfigure**: Allows you to reboot the server, shut down the server, or perform a full system reconfiguration.

Note:
These tasks are covered in the *Mitel Standard Linux Installation and Administration Guide,* available on the Mitel Document Center Web site.

26.197.7 Troubleshooting MiCollab Client

MiCollab Client includes various error messages, utilities, and logs to help troubleshoot issues. All the available troubleshooting information for MiCollab Client , including Calendar Integration troubleshooting, is documented in the Troubleshooting chapter of the *MiCollab Client Administrator Guide*.

If you encounter a problem with the product, you can download this document from the Mitel Document Center Web site and troubleshoot the issue.

If you cannot resolve the issue yourself, contact Mitel Technical Support for assistance.

26.197.8 Contacting Technical Support

Contact Mitel Technical Support if you require technical assistance. Before you call, check this Help system for tips and solutions. If you are unable to find a solution, please have the following information ready when you call:

- The MiCollab MSL software revision
- The nature of the problem
- What you were doing with the application when the problem occurred
- Troubleshooting results

For information about contacting Mitel Technical Support, access Mitel Online at http://www.mitel.com.

26.198 Enterprise Tab

The **Enterprise** tab includes fields and options for an Enterprise or a Company.

The first step to provisioning MiCollab Client is to create an Enterprise. To do so, click **Create Enterprise**.

After you have created an Enterprise, select it from the list box and then configure the fields and options for the Enterprise from the **Settings** area.

Note:
Some configuration settings do ***not*** apply to MiCollab Client standalone Web and Mobile Portal users (see table for details).

Note:
You cannot change the fields in this area after you have created an the Enterprise if PBX nodes have been defined. If PBX nodes have been defined, you must first delete all PBX nodes to change the values in these fields.

Settings

The **Settings** area includes fields for specifying basic Enterprise information.

To configure Enterprise Settings:

1. To configure Enterprise settings, you can specify values or edit the following fields.
   - **Description**: (Required) Type a description for the Enterprise, for example, **Acme Company-Phoenix Arizona**. By default this field is blank. The description:
     - must contain 1-128 characters.
     - must contain alpha-numeric characters (dashes included).
     - cannot contain vertical bars (|).
   - **Enterprise domain**: (Required) Type a domain for the Enterprise. The Enterprise domain need not be a resolvable DNS name or a registered domain name; however, it must follow the DNS suffix format. The Enterprise domain must be unique to the Enterprise so that peered servers do not have the same Enterprise domain. Mitel recommends that you use the site location or Enterprise ID as part of the Enterprise domain (for example, **Phoenix.xyzcompany.com**, where **Phoenix** is the Enterprise ID).

Note:
When the FQDN of the MiCollab Server is changed, the **Enterprise ID**, **Description**, and **Enterprise Domain** do not change automatically. The administrator must change them manually.

- **Voice mail server**: (Optional)
  - When **NuPoint** is selected, the Voicemail server field displays the FQDN of the NuPoint server. The field is "read-only" in this case.
  - When **Embedded** is selected, the Voicemail server field is hidden.
  - When **MiCollab Advanced Messaging** is selected, the Voicemail server field is enabled and the administrator needs to provide the URL for clients accessing MiCollab Advanced Messaging Web Client.

    MiCollab Advanced Messaging (MAM) integration

    The integration of MiCollab Advanced Messaging provides the user access to the responsive Web-interface for managing Voicemails.

    The user needs to provide the access credentials to the MiCollab Advanced Messaging Web Client on MiCollab Clients. The credentials to access MiCollab Advanced Messaging are not stored by the MiCollab Client but cached by the web interface (depending on user's browser settings on the device).

    Precondition:

    - The user needs to have a valid Visual Voicemail license.
    - The server hosting for MiCollab Advanced Messaging must have a valid, trusted certificate. Refer to the MiCollab Advanced Messaging documentation for details.
    - The MiCollab Advanced Messaging Web Client must be enabled for HTTPS and have a valid trusted certificate.
    - For information about PBX platforms that support MiCollab Advanced Messaging, see the *MiCollab Client Administrator Guide > Table 20: Voice Mail Server Types*.
    - The MiCollab Advanced Messaging must have the MiCollab Advanced Messaging Web Client installed.

Note:
The MAM Client URL must be resolvable and accessible from the internet for the MiCollab Client to be used outside the LAN.

Enabling MiCollab Advanced Messaging for a new MiCollab installation

The type of Voicemail for the installation must be selected in the Server Manager on the following page: **MiCollab Client Service** > **Configure MiCollab Client Service** > **Enterprise** > **Settings** > **Voice mail server type**.

Enabling MiCollab Advanced Messaging for an existing MiCollab installation

An existing MiCollab user does not get the new roles or templates automatically when MiCollab upgraded to version 8.0. The administrator must manually create the role or template to remove NuPoint and to change the MiCollab Client feature profile. This is required for the Client to display MiCollab Advanced Messaging in the **Voicemail** tab.

- **Administrator e-mail**: (Optional) Type the e-mail address for the MiCollab Client Service administrator. An e-mail message is sent to this address when On-Demand presence is enforced. This field can contain a maximum of 255 characters.
- **Switch type**: This field is editable when there are no PBX nodes defined on the PBX nodes tab. Once the **Switch type** field is set, all PBX nodes created will be of that type. After a PBX node is created, the **Switch type** field cannot be changed unless all PBX nodes are deleted.

  When creating a new enterprise that will not have any PBX nodes but only Teamwork Mode accounts, the switch type can be left at the default value of “Mitel Communications Director” (the value will be ignored).
- **Collaboration server type**: (Optional) Select a collaboration server to use with MiCollab Client. Options include:

  - None (default)
  - MiCollab Audio, Web and Video Conferencing

  If you do not intend to use collaboration features, set this field to **None** (default). If you have already added and configured a collaboration server, you cannot configure the option here.

Note:
The Mitel Your Assistant Collaboration Module is no longer supported as a collaboration server type. See the Collaboration tab topic for more information.

- **Avatar URL**: To enable MiCollab Avatars for Aquarius 69xx Sets (6920, 6930, and 6940), configure the avatar URL displayed in this field on MiVoice Business in the Online Services URL Form.
- **Language**: (*Required*) Select a language for the Enterprise from this list. You can configure the language parameter at the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts of the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. A user's language setting determines the language in which the Welcome E-mail Message is generated for that user.
- **Time zone**: (*Required*) Select the time zone where the Unified Communications server is physically located from the list box. The time zone where the Unified Communications server is located may be different from the time zone where the Enterprise is located.

2. Click **Apply** to save the changes. Clicking **Reset** clears the changes.

Calendar Integration

This feature enables the MiCollab Client administrator to configure a Google Server, Office 365, or an Exchange Server from which the MiCollab Clients can fetch calendar availability information and update their Dynamic Statuses. Exchange Integration supports Exchange 2016 and Exchange 2019.

From the **Calendar Type** drop-down menu, select **Google, Office 365,** or **MS Exchange**.

The following user permissions are mandatory:

1. When Calendar Integration is done with Office 365 using OAuth 2.0:
   - API Permissions - The Office 365 administrator must grant **full_access_as_app** application permissions for Office 365 Exchange Online API.
   - URL Access required - Client's firewall must allow the following URLs:
     - **outlook.office365.com** - Access for URL *outlook.office365.com* is also required when Calendar Integration is done with Office 365 using Basic authentication
     - **login.microsoftonline.com**

   To enable Calendar Integration, select the check box.
2. When Calendar Integration is done with Office 365 using OAuth 2.0 (Microsoft Graph):

- API Permissions - The Office 365 administrator must grant the following API permissions from Microsoft Graph:

  Delegated Permissions:

  - Calendars.Read
  - Calendars.Read.Shared
  - Calendars.ReadWrite
  - Calendars.ReadWrite.Shared

  Application Permissions:

  - Calendars.Read
  - Calendars.ReadWrite
- URL Access Required - Client's firewall must allow the following URL:

- **login.microsoftonline.com**
- **graph.microsoft.com**

Note:

If test connection is performed without granting the required permissions, the following error message is displayed:

"***Invalid calendar server credentials.: Invalid credentials.***"

To resolve this, the administrator must provide all the required API permissions.

If MS Exchange or Office 365 is selected then: (if Google is selected, skip steps 1 to 3 and go to step 4; see Settings required on Exchange Server for MiCollab Meeting Center)

1. Enter the URL of your Exchange Server. The URL corresponds to Exchange Web Services (EWS). The exact URL depends on how your exchange server is configured but is usually in the format *https://<hostname>/EWS/exchange.asmx*. For Office 365, refer to https://outlook.office365.com/ews/exchange.asmx.
2. The version of the Exchange Server is entered automatically during a successful test connection.

Note:
When XXX is connected to a 2010 SP3 Exchange Server, the version might still be shown as SP2 on the MiCollab Client Server Manager.

3. Enter the user name and password used to log in to the Exchange Server. For Azure Active Directory, the user name and password must be with **Application Permissions** to the **App ID/Secret key** issued for connection to the Azure AD. In this case, the user need not have administrative privileges on the Exchange Server. The user need only be able to view other users' calendar availability information.

   a. If you want to use Impersonation, select the appropriate radio button. If Impersonation is enabled, then MiCollab Client users need not provide their exchange password to use Calendar Integration. However, they still need to provide their Exchange user name and primary e-mail address.
   b. Enabling Impersonation can have security implications and requires administrative privileges on the Exchange Server.
   c. If you want to use Delegation, select the appropriate radio button.

   Refer to the following Microsoft websites for Microsoft Exchange version details:

Note:
Exchange 2019: https://docs.microsoft.com/en-us/Exchange/new-features/new-features?view=exchserver-2019

Settings required on Exchange Server for MiCollab Meeting Center

- Exchange Subscription Type selected to be either Impersonation or Delegation.
- For Impersonation, users need to have ApplicationImpersonation as Management Role and Access Rights as LimitedDetails.
- For Delegation, users need to have Access Rights as LimitedDetails.

Use the following command to change Management Role on Exchange Management Shell, where serviceAccount is the user name: New-ManagementRoleAssignment –Name:impersonationAssignmentName –Role:ApplicationImpersonation –User:serviceAccount

Use the following command to change Access Rights on Exchange Management Shell: Add-MailboxFolderPermission -Identity user1@mitel.com:\Calendar -User user2@mitel.com -AccessRights LimitedDetails

where,

- user1: user ID of the mailbox or calendar you want to access.
- user2: user ID of the service account you use or configure on the Admin portal.

Note:
Only Basic Authentication is supported on MiCollab while communicating with the Exchange Server.

4. You can access the Advanced Calendar Integration Settings. The default values for these settings work appropriately under most circumstances, and therefore, normally, need not be changed. Change them only if you have any particular needs, such as a requirement for high network latency. Be aware that changing these values affects calendar integration across ALL enterprises.
5. Test your connection to ensure that MiCollab Client can connect to either Google Server or Exchange Server and communicate with it properly. If on clicking the **Test Connection** button, you receive an error stating "**Invalid calendar server credentials**", you need to troubleshoot the issue.
6. Click **Apply** to save the changes. Clicking **Reset** clears the changes.

Calendar Integration for Office 365

The authentication protocol for Calendar Integration with Office365 can be Open Standard for Authentication 2.0 (OAuth 2.0), OAuth 2.0 (Microsoft Graph), or the Basic Authentication protocol.

A service account with a valid Office365 user license is required to enable the mailbox.

In Basic Authentication, the user name and password are used for authentication whereas in case of OAuth 2.0 authentication, tokens are used for authorization.

OAuth 2.0 (Microsoft Graph) also uses the OAuth 2.0 tokens, with the difference that instead of the Exchange Server, it uses Microsoft Graph Server APIs to fetch the calendar details.

Prerequisites OAuth 2.0:

- To use OAuth 2.0, an application must have an application ID issued by Microsoft Entra ID. On the **Request API** page, select **Exchange** under **Supported Legacy APIs** followed by **Application Permissions** and then select **full_access_as_app.** Then click **Add Permissions.**

  For more details about the configuration, see the **MiCollab Users and Services Provisioning** > **Configuration > Cloud Service Provider** section.

  Note:
  Any changes in API permission made from Microsoft Graph and EWS OAuth2.0 in Office 365 will be reflected in MiCollab after 60 minutes.

  To use OAuth 2.0 (Microsoft Graph), an application must have an application ID issued by Microsoft Entra ID. On the **API Permissions** page, select **Microsoft Graph** then **Delegated Permissions** and allow **Calendars.Read, Calendars.Read.Shared, Calendars.ReadWrite, and Calendars.ReadWrite.Shared**permissionsfollowed by **Application Permissions** with **Calendars.Read**, **Calendars.ReadWrite** permissions. Then click **Add Permissions** and **Grant Admin consent.**

After successfully configuring the Cloud Service Provider, the MiCollab administrator can enable Calendar Integration from MiCollab Client Services.

Perform the following steps under MiCollab Client Services:

1. Navigate to the **Applications** > **MiCollab Client Service** > **Enterprise**.
2. Under **Calendar Integration**, select the **Calendar Type** as **MS Office365**.
3. Select the **Authentication Protocol** for Office 365 as one of the following:

   - Basic,
   - OAuth 2.0
   - OAuth 2.0 (Microsoft Graph)

   To enable OAuth 2.0 or OAuth 2.0 (Microsoft Graph) as the Authentication Protocol, select the corresponding radio button.

4. For Exchange Subscription Type:

   - the default option selected is **Impersonation** if **OAuth 2.0** is selected as the Authentication Protocol. It will be applicable for all 9.2 servers including newly deployed and upgraded servers.
   - the default option selected is **Impersonation** if **OAuth 2.0** (Microsoft Graph) is selected as the Authentication Protocol. It will be applicable for all 9.6 servers including newly deployed and upgraded servers.

Note:
The default Authentication Protocol selected is Basic.

Note:
After a backup restore, the client credentials will not be restored as part of the MiCollab backup. Therefore, after a backup restore, the administrator must reconfigure OAuth 2.0 settings in the**Cloud Service Provider** section and then enable Calendar Integration.

Note:

No default subscription type is supported in Calendar Integration for Office 365 with OAuth 2.0 Authentication Protocol.

In the Default subscription type, the MiCollab users must provide their Exchange or Office 365 password from the client (Web, PC, or Mobile client) to use Calendar Integration.

No default subscription type is supported in Calendar Integration for Office 365 with OAuth 2.0 (Microsoft Graph) Authentication Protocol.

For more information about different calendar sharing options, refer to the following Microsoft links:

- Outlook
- Outlook Web Access

Trusted Servers

This area provides a table of trusted servers for MiCollab Client. After you configure peering with one or more MiCollab Client Services, they are automatically added to this table.

Note:
If the peered server IP address is changed, add or edit the IP address in the **Trusted Server Details** page, to view the presence state of the users.

The table includes three columns:

- **Description**: Shows the description you provide for the trusted server.
- **IP address/hostname**: Shows the server's IP address or hostname.
- **Type**: Indicates one of the following trusted as the server type:
- *Presence Proxy*: Presence proxy servers are required to provide presence information such as status and login notification to remote users. If you do not have any remote users (all users are located at the site where the Unified Communications server is located), you need not add presence proxy servers.
- *IM*: An IM trusted server provides Instant Messaging presence to MiCollab Client users on the local Enterprise.
- *Peer*: A peer trusted server provides presence information for corporate contacts on peered MiCollab Client Services.

You can perform the following tasks for trusted servers:

- Click the **Add Server** link to add a new trusted server.
- Click the **server name link** to edit the corporate location.
- Delete a trusted server.

  If you delete a peered server, you can also delete it as a trusted server, as part of your cleanup activities.

  To delete a trusted server:

  1. Select the server you want to delete from the **Trusted Servers** table.
  2. Click the **Delete Server** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the server. Clicking **Cancel** cancels the deletion.

Launchpad Settings

The Launchpad is an area on the MiCollab Legacy Client interface where the user can quickly navigate to a URL, dial a phone number, run a program, or explore a folder. The Launchpad entries that you configure here apply to every user that is licensed for the Launchpad feature.

Note:
This feature is compatible only with legacy clients.

This area of the **Enterprise** tab provides a table that lists the Launchpad entries you add for MiCollab Client. The table has three columns:

- **Label**: Indicates the label or description that you provide for Launchpad entry.
- **Action**: Indicates what occurs when the user accesses the Launchpad item. There are two actions that you can configure for the user: **Dial a number** and **Browse to a URL**.
- **Value**: Indicates the phone number or URL that corresponds to the action you selected.

You can Add, **Edit**, and **Delete** Launchpad entries. Any changes you make to Launchpad settings will not be displayed in the Desktop Client until the user restarts the client.

USB Devices

The MiCollab Client Desktop Client supports several headsets and handsets (see list under Requirements).

To use a USB device with MiCollab Client , users must create a USB device profile using the MiCollab Client Desktop Client. If the user's account includes the **User can manage USB device profiles** option (Account Details Page – Account Settings – **USB Devices**), the user can upload the profile to the Unified Communications server.

The USB devices displayed in this area include the device information from the profiles created and uploaded by users. The device information is read-only and cannot be edited. You can, however, **Sort** the information and **Delete** USB devices from the server.

Plus Dialing Settings

This area of the **Enterprise** tab includes fields for specifying plus dialing settings.

Note:
Starting with MiCollab Client 5.1, some of the dialed digit processing happens locally within MiCollab Client. Because of this, if some dialing settings are changed in the server-manager, all clients within that enterprise (or for that PBX) mustbe restarted. Following are the settings affected by this:

- At the enterprise level:
  - Plus Dialing settings > Country code
  - Plus Dialing settings > International access code
  - Plus Dialing settings > Long distance access code
- At the PBX nodedetails level:
  - Plus Dialing settings > Country code
  - Plus Dialing settings > International access code
  - Plus Dialing settings > Long distance access code
  - Extension length
  - Dialing prefix

The plus dialing settings include:

- **Country code**: This field must be set to the country code of the country where the PBX resides. If an E.164 call is placed to a number within the user's "home" country, MiCollab Client will strip off the digit string from the country code.
- **International access code**: This field indicates the international dial code that must be dialed for international calls from the country where the PBX resides. If the MiCollab Client determines that the call is being placed outside of the user's country (based on the PBX country code), MiCollab Client prepends the International Prefix.
- **Long distance access code**: This field indicates the Toll digit for the country where the user's PBX resides. For any E.164 dialed calls within the user's home country, MiCollab Client prepends the toll digit.

Note:
Sites using E.164 (plus dialing) settings must have ARS set up on the PBXs to strip the Toll Digit for local calls.

Note:
During an avatar search, the CLID translation string is stripped off from the directory number.

CLID Translation

CLID Translation: For details about this field, refer to the help for CLID translation field in the PBX Node Details page.

Note:
If CLID Translation is explicitly specified at the PBX node level, that setting will override the CLID Translation setting at the Enterprise level.

Default Account Settings

This area of the **Enterprise** tab includes the default values that will apply to MiCollab Client accounts whilethey are created. The values you configure here apply to all accounts whether you create them manually (Adding and Editing Accounts), or you create them automatically by configuring an AD/LDAP or PBX Node synchronizer (Synchronization tab).

If required, you can edit the values for any account from the **Account Details** page.

To configure default account settings

1. Specify the following settings under Default Account Settings:

   Login Settings

   - **Country**: Select the country that the MiCollab Client users reside in. By default, this option is set to United States.
   - **PBX node**: Select the PBX node that services users from the list box. The list includes all the PBX nodes you have configured on the **PBX Nodes** tab. If you have not configured PBX nodesyet, the list box will be empty.
   - **Account code length**: Account codes provide a way to track phone usage. Select the account code length from the list box. The code length is in the range 0-12. You can configure account code details by using the **ACD Settings** tab.
   - **Sort Order**: Select the order type you want for displaying the names on MiCollab Clients.
     - Select **First Name** to display contacts' first name in the directory and in search results. By default, **First Name** is selected as sort order.
     - Select **Last Name** to display contacts' last name in the directory and in search results.

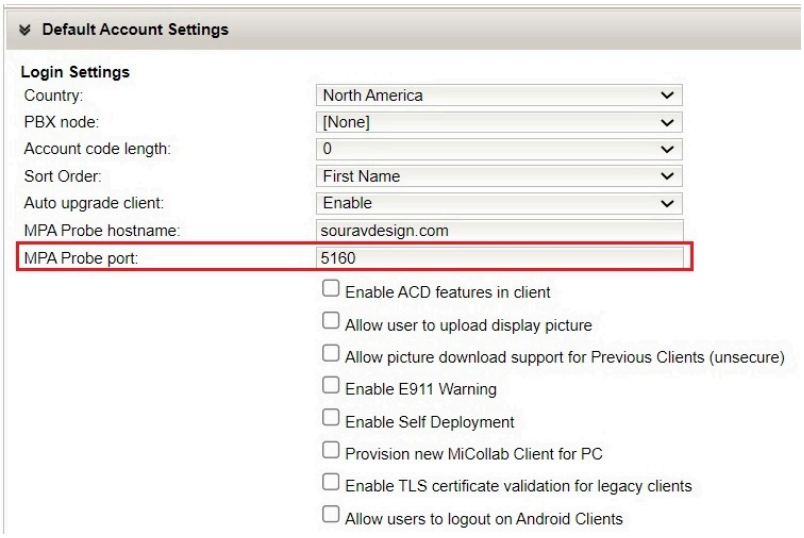
   Note:
   Changing the sort order value at the server does not impact the setting of existing users. Sort order value is applicable only for new users.

Note:
If an existing server is upgraded to include this setting, the server will have First Name as the default value. It will not have any impact on the Client setting.

Note:
If the sorting value is changed to Last Name, this value will persist after an upgrade or backup restore.

- **Auto Upgrade Client**: Auto Upgrade Client provides an option to control automatic client upgrades.
  - Select **Enable** to push the client upgrade pop-up notification (if there is a new version of the client available) for all users under the Enterprise (provided that **Default** or **Enable** is set in **Accounts**

> **Account Settings**). By default, this option is enabled. Users will get a client upgrade pop-up notification.
    - Select **Disable** to disable client upgrade notification for all users under the Enterprise (provided that **Enable** is not set in **Accounts** > **Account Settings**).
- **MPA Probe hostname**: Enter the MPA Probe hostname details, which are used to collect the softphone voice quality reports from the Clients.
- **MPA Probe port**: The default value is 5160. The MPA Probe port is used to collect the softphone voice quality reports from the Clients.
- **Enable ACD features in client**: Select this option to provide users with Automatic Call Distribution (ACD) features in the MiCollab Client Desktop Client.
- **Allow user to upload display picture**: Determines whether users can upload their own display picture from the Desktop Client.
- **Allow picture download support for Previous Clients (unsecure)**: Allows users to download *picture for previous MiCollab Clients.*
- **Enable E911 Warning**: Displays a warning whenever the user launches the softphone client. The warning states that the softphone may not be able make calls to the appropriate emergency 911 public safety authorities in some locations. By default, this option is enabled.
- **Enable Self Deployment**: Allows the user to self-deploy MiCollab Client.
- **Provision new MiCollab Client for PC**: Select to provision MiCollab Client for PC for all users under the Enterprise. By default, this option is disabled.
- **Enable TLS certificate validation for legacy clients**: Select to enable validation of TLS certificate for legacy clients. By default, this option is disabled.
- **Allow users to logout on Android Clients**: By default, this setting is disabled and users will not be able to log out of the Android clients. The administrator needs to enable this flag to allow users to log out from the Android clients.



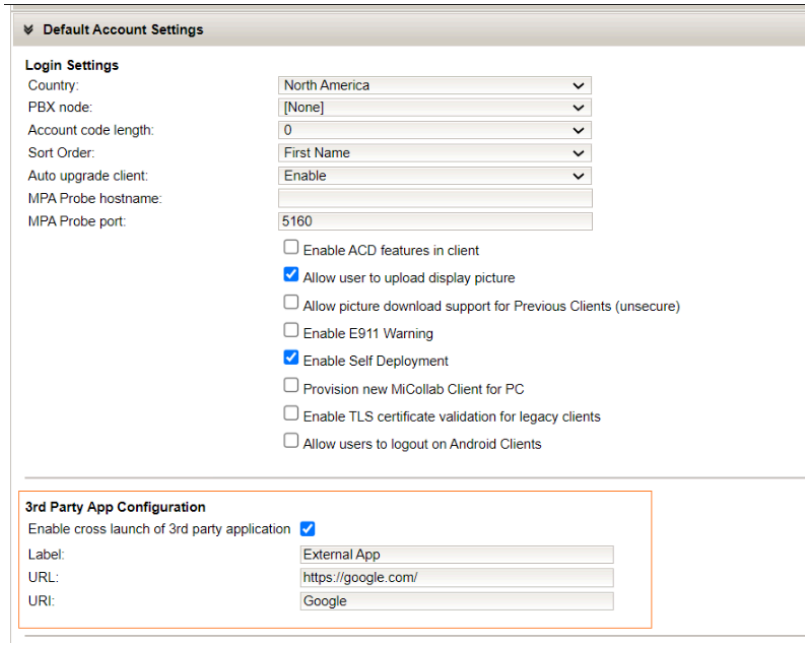
3rd Party App Configuration

By enabling the **3rd Party App Configuration**, the administrator has the ability to configure a third-party application to be launched from MiCollab Client. Once enabled, all MiCollab users can launch the third-party application from their Clients. To enable cross-launch of the third-party application in their Clients, users need to refresh or restart their clients.

Note:
The Clients are not updated dynamically with the new information updated nor the server notified when the settings are changed in this **3rd Party App Configuration**. The Clients must be restarted for the changes to show up or take effect.

To set up the cross launch of any third-party application for all users, perform the following changes:

- **Enable cross launch of 3rd party application**: Select the check box to enable cross launch of a third-party application from MiCollab Client. This check box is cleared by default. The **Label**, **URL**, and **URI** fields are available to edit only if the check box is selected.
- **Label:** Type the name of the third-party application. The default value is **External App**. The Label that is added here as the name of the third-party application is displayed in the Navigation panel of the client. This field can contain a maximum of 20 alpha-numeric characters. This field is mandatory.
- **URL:** Type the URL of the application. The URL must start with http:// or https://. Note that the system does not validate the URL during the setup. This field is mandatory.
- **URI:** Type the URI of the application. The URI must end with ://. This field is optional.



Note:
The **3rd Party App Configuration** setting is also available under **MiCollab Client Service Configuration** > **User Profiles** tab > **Existing user profile** / **New user profile**. The following conditions apply:

- if the setting is enabled under the **Enterprise** tab and disabled in all the user profiles, all the users on that server can cross launch the third-party application from their Clients.
- if the setting is disabled under **Enterprise** tab and enabled in any of the user profile, the users who are assigned to that user profile can cross launch thethird-party application from their Clients.
- if the setting is enabled from both **Enterprise** and user profile, the user profile settings will override the **Enterprise** settings for the users who are assigned to that user profile.

Corporate Directory Settings

- Download limit
- The (Really Simple Syndication) **RSS Window** is an optional embedded window that provides RSS feeds from a selected URL to the user's Legacy Desktop Client. Configure the following **RSS Window** settings:
  - *URL*: Type the URL to use as the default RSS Window location.
  - *Always On*: Select this option if you want the RSS Window to always appear on the user's Desktop Client.
  - *User modifiable*: Select this option if you want to allow users to change the default URL.
- Select a **Collaboration Server** from the list. The list includes all the collaboration servers you have configured on the Collaboration tab. If you have not configured collaboration servers yet, this field displays the message, "No collaboration servers defined."
- (Optional) Enable **Users can manage MiCollab corporate locations**. This field allows users to manage Corporate Locations from their MiCollab Mobile Client and upload the information to the MiCollab Client Service. By default, this option is disabled.
- The MiCollab Client Desktop Client supports various USB devices. Configure account **USB Devices** options:
  - *User can configure local USB devices*: Select this option to allow users to configure USB devices in the MiCollab Client Desktop Client.
  - *User can manage USB device profiles*: Select this option to allow users to manage (upload, edit, and delete) USB device profiles on the Unified Communications server from their desktop client. When you enable this option, the *User can configure local USB devices* option is automatically enabled.

2. Click **Apply** to save the changes. Clicking **Reset** clears the changes.

Corporate Locations

This area of the **Enterprise** tab allows you to manage corporate locations for use on the MiCollab Client Mobile client. The corporate locations table includes the following information:

- **Name**: The name that you provided for the location.
- **Radius**: The circular area surrounding the location.
- **Latitude**: The latitude of the location.
- **Longitude**: The longitude of the location.

You can complete the following tasks for corporate locations:

- Click the Add Location link to add a new corporate location.
- Click the **location name link** to edit the corporate location.
- Click  to show the corporate location on Google Maps ™ .
- Delete a corporate location. **To delete a corporate location:**

1. Select the corporate location that you want to delete from the table.
2. Click the **Delete Location** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the server. Clicking **Cancel** cancels the deletion.

Call Log Settings

This field allows the option to **Show Missed Calls for Key Line**. Once enabled, the Call History displays missed calls for key line numbers.

This feature is disabled by default.

For details about enabling the Centralized Call History feature for MX-ONE, see the **Adding and Editing PBX Nodes** > **Subscribing Centralized Call History from MiVoice MX-ONE** section.

Reset Password Settings

The **Reset Password on Login** check box under **Reset Password Settings** allows Non-SSO users to reset their MiCollab Client password from MiCollab Client. This check box is cleared by default. When the **Reset Password on Login** check box is selected, the following pop-up screen notification appears:

```
Activating this feature affects all users who are not using single sign-on or
Active Directory authentication. Mitel recommends that all users be notified
of this security enhancement prior to it being activated.

The efforts of this feature are as follows:

• Upon the user's next logout from the MiCollab client (including computer
  restarts), users shall see a prompt to change their MiCollab password when
  they start the MiCollab client.
• Part of that password change process requires users to enter their current
  password. Users who do not recall their current password can click the
  "Forgot password" button to receive an email with a temporary password. The
  users shall use this password to login to MiCollab, and the system shall
  prompt them to change this temporary password to a permanent password of
  their choice.

Prior to activating this feature, please alert all users who are not using
single sign-on or Active Directory authentication of this pending action.
```

External Ldap Search Settings

External Ldap Search Settings is used to enable external search feature at the Enterprise level. To enable/disable external LDAP search:

1. Select the **Enable external Ldap search** check box. By default, this check box is not selected. Clear the check box to disable the external LDP search.

   The **Enable external LDAP lookup for call history** check box is selected by default. This makes the server go to the Meta directory to look up for names for the call history. If this check box is cleared, the server does not look up for Call history names in the Meta directory and users will see numbers instead of names in their **Call History** menu.
2. Click **Apply** to save the setting.

Jetty Configuration Settings

To enable/disable the jetty process:

1. Selectthe **Enable Jetty Process** check box. By default, this check box is selected. Clear the check box to disable the jetty process.
2. Click **Apply** to save the setting.

MiTeam Classic Configuration

Post Release 9.7, the MiTeam Classic feature will be removed from MiCollab. For enterprises that have disabled the MiTeam Classic before the upgrade, the **MiTeam Classic Configuration Settings** panel will not be displayed in the **Enterprise** tab.

The enterprises that have enabled MiTeam Classic before the upgrade will continue to see the **MiTeam Classic Configuration Settings** panel. If they disable it, then the **MiTeam Classic Configuration Settings** panel will be removed permanently from this **Enterprise** tab.

MiTeam Classic provides Cloud-based collaboration features for UCC Premium users. Note that MiTeam Classic is supported only for MiCollab Clients in Integrated mode. See the *MiCollab Client Administrator Guide* for MiTeam Classic integration requirements.

Email Notification Settings

The text box contains the default **from** email address for sending email notifications. The default value is uca.no.reply@<servername>.<domain name>.

The email address can be updated for email messages to be sent from the updated address.

Presence Privacy Configuration Settings

This setting controls whether the user's presence information (dynamic status, telephony status, video availability, and calendar advisory) is displayed to other users or not. The user's IM availability is not controlled by this setting.

Presence Privacy Service: By default this setting is **Disabled**.

- Set the **Presence Privacy Service** value to **Disabled** to disable the presence privacy feature.
- Set the **Presence Privacy Service** value to **Enabled** to enable the presence privacy feature.

Show Presence for all users: This setting is available only if **Presence Privacy Service** is **Enabled**. By default the **Show Presence for all users** setting is selected.

- If this setting is selected, the presence information of all users on local and peered servers is displayed.
- If this setting is not selected, presence status of users on local and peered servers are not shown to a user unless those users are added to the presence allowed list of the user.

Limitations

- The server will not send updated presence packet on toggling presence **Presence Privacy Service** setting at the server. Presence will be updated only when there is change in the presence status or when the user logs out and then logs in.
- **Presence Privacy Service** is not supported in Co-located mode.
- On peered servers, the Presence Privacy setting at the local server takes priority. For example, if the setting on peered server A is **Enabled** and the setting on peered server B is **Disabled**, peered user's presence will be displayed based on the local server setting and not the server where the user actually exists.
- Telephony presence status of other users does not turn off immediately. It changes only when the user logs in again to the Client. When user logs in to the Client, telephony presence will turn off from the corporate directory, call history, search tab, and from legacy console.
- Video call functionality does not work when the presence privacy setting is enabled.

Note:
After you create an Enterprise, you cannot edit the **Enterprise ID** field. However, you can delete the Enterprise.

You can also do the following from this page:

- Click the Add an Enterprise link to create a new Enterprise.
- Click the Delete This Enterprise link to delete an Enterprise.

To delete an Enterprise:

1. Select the Enterprise from the list.
2. Click the **Delete this Enterprise** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the Enterprise. Clicking **Cancel** cancels the deletion.

26.198.1 Adding and Editing Corporate Locations

You can add and edit corporate locations for use on the MiCollab Mobile Client if you know the latitude and longitude coordinates for the location.

Note:
You can obtain longitude and latitude coordinates from Google Maps ™ if you log into your iGoogle account. Google Maps provides tools to account holders that display latitude and longitude coordinates as a tooltip and mark the coordinates for a specified location.

The MiCollab Mobile Client displays the corporate location in the client interface. Users can then associate the corporate location with one of their Dynamic Statuses. Then, when users enter the corporate location, the MiCollab Mobile Client automatically updates their Dynamic Status.

To add or edit a corporate location:

1. Type a **Name** for the corporate location. The Name is limited to 32 characters in length and must contain alpha-numeric characters, dashes, and/or spaces.
2. Type the **Radius** for the corporate location and then select feet or meters. The radius is the circle that surrounds the location. The default radius is 1000 feet.
3. Type the **Latitude** of the location. Latitude is limited to 16 characters in length, including numeric characters, the minus sign (-) and period (.). The valid range is -90.0 to 90.0.
4. Type the **Longitude** of the location. Longitude is limited to 16 characters in length, including numeric characters, the minus sign (-) and period (.). The valid range is -90.0 to 90.0.
5. Click **Create** or **Save**. You are returned to the Enterprise Tab.

After you create Corporate Locations, you can edit the associated fields at any time.

Note:
MiCollab Mobile Client users must restart the client to see recently-added corporate locations.

26.198.2 Adding and Editing Trusted Servers

The trusted servers table identifies servers that can connect to the local MiCollab Client Service without authentication.

Note:
If the peered server IP address is changed, add or edit the IP address in the **Trusted Server Details** page, to view the presence state of the users.

To add or edit a trusted server:

1. Type a **Description** for the trusted server. The Description is limited to 64 characters in length and must contain alpha-numeric characters, dashes, and/or spaces.

2. Type the **IP address/hostname** for the server. The IP address must be a valid IP address or fully qualified domain name.
3. Select one of the following server types:

   - **Presence**: Trusted presence servers are permitted to receive presence information from the contacts on this MiCollab Client Service .
   - **IM**: Trusted IM servers are permitted to exchange Instant Messages with contacts on this MiCollab Client Service .
   - **Peer**: Trusted peer servers are permitted to exchange communication information with contacts on this MiCollab Client Service .
4. Click **Create** or **Save**. You are returned to the Enterprise Tab.

After you create a trusted server, you can edit the associated fields at any time.

Note:
The following procedure must be done on MiCollab Client 5.1 to resolve peering on a server which had a changed IP address, failure to do so will cause peering not to work. Go to the Enterprise Tab, expand Trusted Servers, select the peered server whose IP address changed and in the Trusted Server Details page edit the field "IP address/hostname" with the correct IP address.

Note:
Whenever the peered server address is changed, the server address must also be updated in the peer trusted servers list.

26.198.3 Creating an Enterprise

Creating an Enterprise is the first step to provisioning MiCollab Client.

On this page, configure basic information about a company to create an Enterprise.

To create an Enterprise

1. Configure the following Enterprise Settings.

   - **Enterprise ID**: (*Required*) Type a unique identifier for the Enterprise, for example, **Phoenix**. By default this field is blank. The Enterprise ID:

     - is limited to 4-32 characters in length.
     - must contain alpha-numeric characters (dashes included).
     - cannot contain spaces, vertical bars, commas, semicolons, or colons (| , ; :).

Note:
You cannot change this field after you create the Enterprise if PBX nodes have been defined. Once PBX nodes have been defined, this field cannot be deleted unless all PBX nodes are deleted first.

- **Description**: (*Required*) Type a description for the Enterprise, for example, **Acme Company-Phoenix Arizona**. By default this field is blank. The Enterprise Description:
  - is limited to 1-128 characters in length.
  - must contain alpha-numeric characters (dashes included).
  - cannot contain vertical bars (|).
- **Enterprise domain**: (*Required*) Type a domain for the Enterprise. The Enterprise domain does not need to be a resolvable DNS name or a registered domain name, however, it does need to follow the DNS suffix format. The Enterprise domain should be unique to the Enterprise so that peered servers do not have the same Enterprise domain. Mitel suggests using the site location or Enterprise ID as part of the Enterprise domain (for example, **Phoenix.xyzcompany.com**, where **Phoenix** is the Enterprise ID).
- **Voice mail server**: (*Optional*) Type the IP address or the hostname of the Enterprise's NuPoint UM voice mail server, for example, **phx-acme-Nupoint**. If you do not have a NuPoint UM voice mail server, leave this field blank.
- **Administrator e-mail**: (*Optional*) Type the e-mail address for the MiCollab Client Service administrator. An e-mail message is sent to this address when On-Demand presence is enforced. Maximum length for this field is 255 characters.
- **Switch type**: (*Required*) Select the communications system (switch) that the Enterprise currently uses from the list box.

  By default, MiVoice Business is selected.

Note:
You cannot change this field after you create the Enterprise if PBX nodes have been defined. Once PBX nodes have been defined, this field cannot be deleted unless all PBX nodes are deleted first.

- **Collaboration server type**: (*Optional*) Select a collaboration server to use with MiCollab Client. Options include:
  - None (default)
  - MiCollab MiCollab Audio, Web and Video Conferencing

  If you do not intend to use collaboration features, set this field to **None** (default). If you have already added and configured a collaboration server, you cannot configure the option here.

Note:
The Mitel Your Assistant Collaboration Module is no longer supported as a collaboration server type. Refer to the Collaboration tab topic for more information.

- **Language**: (*Required*) Select a language for the Enterprise from the list. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. The user's language setting determines which language the Welcome E-mail Message is generated in for that user.
- **Time zone**: (*Required*) Select the time zone where the MiCollab Client Service is physically located from the list box. The time zone where the MiCollab Client Service is located may be different than the time zone where the Enterprise is located.

2. Click **Create** to create the Enterprise.

After you create the Enterprise, you are returned to the Enterprise tab where you must complete additional Enterprise-related settings.

26.198.4 Advanced Calendar Integration Settings

The Advanced Calendar Integration settings enable you to adjust calendar integration settings specific to your network.

Note:
The default calendar integration settings are optimal in most cases. You should only modify them if you have some special requirements, such as high network latency. These settings are applied globally, across all enterprises.

Google

- **Calendar duration per fetch**: Determines how much calendar information is retrieved each time a fetch is performed. The recommended value is 24 hours worth of information - see Note 3.
- **Calendar onpeak fetch Interval**: Determines how often the calendar information is fetched during the onpeak time period. The recommended value is to poll calendars every 45 minutes. The range is 5 to 480 minutes - see Note 4..
- **Calendar offpeak fetch interval**: Determines how often the calendar information is fetched during the offpeak time period. The recommended value is to poll calendars every 240 minutes. The range is 5 to 1440 minutes - see Note 4.
- **Start peak time:** Peak period start time, default is 0700 hours. The allowed range is 0000 to 2359 - see Note 4.
- **End peak time:** Peak period end time, default is 1730 hours. The allowed range is 0000 to 2359 - see Note 4.
- **Request accumulation delay**: Determines the delay to accumulate free/busy requests. The range is 1 to 300 seconds; the default is 30. Lower values may result in unnecessary duplicate event fetches

from the Google server – as the server can send multiple event notifications for a single calendar event creation or deletion.

- **Maximum users per fetch:** Fetch at most 20 calendars per poll request (recommended). The range 1 to 20. Higher values will result in fewer (but larger) network requests. Lower values will result in more (but smaller) network requests.

Common Settings:

- **Parallel connections**: Determine the number of parallel connections to the server. The recommended value is 6. Higher values can be useful in the case of high network latency. Higher values also result in higher network loads.
- **Connection timeout**: Determines how long the connection can be lost before a timeout is flagged. The recommended value is 30 seconds.
- **Error limit:** Determines how many timeouts can occur while communicating with the Google server before the MiCollab Client Service temporarily suspends communication with the Google server. The recommended value is 5 timeouts. Higher values cause the MiCollab Client Service to tolerate more timeouts from the Google server - see Notes 1 and 2.
- **Error duration:** Determines the time interval within which timeouts are considered. For example, if the Timeout Duration is 5 minutes (which is the recommended value), then timeouts that happened before 5 minutes are not considered when determining whether or not to temporarily suspend communication with the Google Server - see Notes 1 and 2.
- **Retry delay after errors**: Determines how long MiCollab Client suspends communication with the Google server before retrying. This applies to most errors caused due to admin configuration, or some issue with MiCollab Client -Google server communication. The default value is 15 minutes - see Notes 1 and 2.

Note:
The **Error limit, Error duration**, and **Retry delay after errors** parameters are used for timeout error throttling. In other words, when <Error Limit> timeouts happen within <Error Duration>, then the MiCollab Client Service waits for <Retry delay> before re-initiating communication with the Google server. Before MiCollab Client retries, the administrator can at any time test the connection with the Google server from the Enterprise tab, apply the settings, and cause MiCollab Client to immediately start communicating again.

Note:
Similar to the above note, non-timeout errors (such as incorrect authentication credentials, network reachability issues, etc.) will cause the communication with the Google server to be disabled and retried after <Retry delay> interval. When the communication is disabled, the MiCollab Client administrator can change settings, apply the changes and cause MiCollab Client to immediately retry the communication again.

Note:
By default, the Calendar Integration Module retrieves 24 hours of calendar information for a user, starting at the present time. Once the first 15 hours elapse, the Calendar Integration Module once again retrieves information for the next 24 hours. If, during those first 15 hours, any calendar events are created/delete/modified, then the Calendar Integration Module will again retrieve 24 hours of information starting at the current time.

Note:
Google calendar imposes a daily limit (10,000 requests by default) on how many requests can be made to it. To conserve the number of Google requests, MiCollab Client allows the Administrator to setup an onPeak interval during which time, the polling is done frequently. Outside of this time (for example, outside of normal office hours), the polling frequency is reduced, thus reducing the number of requests. If you need a bigger quota (more than 10,000 requests per day), please login to the console at https://code.google.com/apis/console#access and request more Quota.

MS Exchange

- **Calendar duration per fetch**: Determines how much calendar information is retrieved each time a fetch is performed. The recommended value is 24 hours worth of information - see Note 3.
- **Calendar fetch Interval**: Determines how often the calendar information is fetched. The recommended value is 15 hours - see Note 3.
- **Event subscription notification frequency**: Determines how often subscription information is sent. The recommended value is 90 minutes. Lower values result in more subscription traffic and processing. Higher values will reduce processing but delay the detection of possible subscription losses on the exchange server.
- **Subscription delay**: Determines the delay after each subscription is performed. The recommended value is 50 milliseconds. Lower values result in spikes of traffic and CPU. Higher values increase the amount of time taken to subscribe all users.
- **Request accumulation delay**: Determines the delay to accumulate free/busy requests. The range is 1 to 10 seconds; the default is 10. Lower values may result in unnecessary duplicate event fetches from exchange server – as the exchange server can send multiple event notifications for a single calendar event creation or deletion.
- **Maximum users per fetch:** Fetch at most 100 calendars per poll request (recommended). The range 10 to 100. Higher values will result in fewer (but larger) network requests. Lower values will result in more (but smaller) network requests.

Common Settings:

- **Parallel connections**: Determine the number of parallel connections to the server. The recommended value is 6. Higher values can be useful in the case of high network latency. Higher values also result in higher network loads.

- **Connection timeout**: Determines how long the connection can be lost before a timeout is flagged. The recommended value is 30 seconds. Higher values will wait longer for the calendar server to respond, but can delay the detection of unresponsiveness.
- **Error limit**: Determines how many timeouts can occur while communicating with the Exchange server before the MiCollab Client Service temporarily suspends communication with the Exchange server. The recommended value is 5 timeouts. Higher values cause the MiCollab Client Service to tolerate more timeouts from the Exchange server - see Notes 1 and 2.
- **Error duration**: Determines the time interval within which timeouts are considered. For example, if the Timeout Duration is 5 minutes (which is the recommended value), then timeouts that happened before 5 minutes are not considered when determining whether or not to temporarily suspend communication with the Exchange Server - see Notes 1 and 2.
- **Retry delay after errors**: Determines how long MiCollab Client suspends communication with the Exchange server before retrying. This applies to most errors caused due to admin configuration, or some issue with MiCollab Client -Exchange server communication. The default value is 15 minutes - see Notes 1 and 2.

Note:
The **Error limit, Error duration**, and **Retry delay after errors** parameters are used for timeout error throttling. In other words, when <Timeout Limit> timeouts happen within <Timeout Duration>, then the MiCollab Client Service waits for <Retry delay> before re-initiating communication with the Exchange server. Before MiCollab Client retries, the administrator can at any time test the connection with the Exchange server from the Enterprise tab, apply the settings, and cause MiCollab Client to immediately start communicating again.

Note:
Similar to the above note, non-timeout errors (such as incorrect authentication credentials, network reachability issues, etc.) will cause the communication with Exchange server to be disabled and retried after <Retry delay> interval. When the communication is disabled, the MiCollab Client administrator can change settings, apply the changes and cause MiCollab Client to immediately retry the communication again.

Note:
By default, the Calendar Integration Module retrieves 24 hours of calendar information for a user, starting at the present time. Once the first 15 hours elapse, the Calendar Integration Module once again retrieves information for the next 24 hours. If, during those first 15 hours, any calendar events are created/delete/modified, then the Calendar Integration Module will again retrieve 24 hours of information starting at the current time.

MS Office 365

The authentication protocol for Calendar Integration with Office365 can be either Open Standard for Authentication 2.0 (OAuth 2.0), OAuth 2.0 (Microsoft Graph) or Basic Authentication protocol.

A service account with a valid Office365 user license is required to enable the mailbox.

Basic Authentication mechanism is a process where the username and password are provided for authentication purposes, whereas in case of OAuth 2.0, tokens are being used for authorization.

OAuth 2.0 (Microsoft Graph) also uses the OAuth 2.0 tokens with difference being instead of Exchange it uses Microsoft Graph Server APIs to fetch the calendar details.

For initial details on configuration, refer to **MiCollab Users and Services Provisioning** > **Configuration > Cloud Service Provider** section.

Once the configuration under **Cloud Service Provider** is successful, the MiCollab Administrator can enable Calendar integration from MiCollab Client Services.

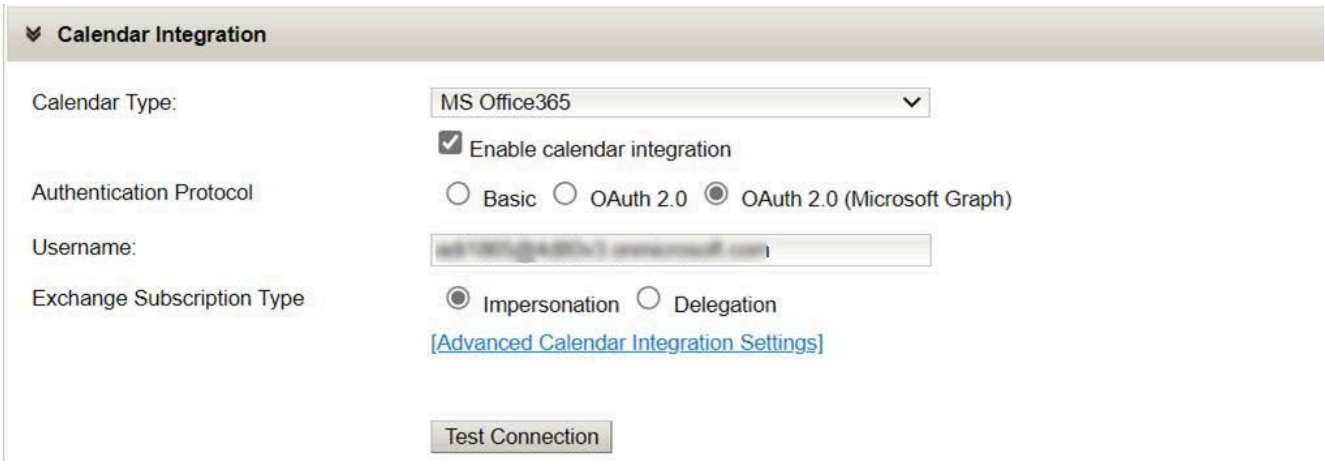
Perform the following steps under MiCollab Client Services:

1. Navigate to the **Applications > MiCollab Client Services > Enterprise.**
2. Under **Calendar Integration,** select the **Calendar Type** as **MS Office365.**

3. Select the **Authentication Protocol** for Office 365 as:

   - **Basic**,
   - **OAuth 2.0**, or
   - **OAuth 2.0 (Microsoft Graph)**

   In order to enable OAuth 2.0 or OAuth 2.0 (Microsoft Graph), the administrator must select the respective Authentication Protocol's radio button.



Note:

The API permission for MS Graph must be given to app in Microsoft Entra ID.

Note:

The administrator must test the connection to switch between OAuth 2.0 (Microsoft Graph) and OAuth 2.0

Note:

The **Username** field is mandatory to configure the calendar integration with Office 365 using OAuth 2.0 protocol.

The **Username** should be a primary SMTP address.

4. For **Exchange Subscription Type**, the default option selected is **Impersonation** if OAuth 2.0 (Microsoft Graph) is selected as Authentication Protocol. It will be applicable for all 9.6 servers including the new deployed and upgraded servers.

Note:
After a backup restore, the client credentials will not be part of the MiCollab backup. Therefore, the admin must reconfigure OAuth 2.0 settings at the Cloud Service Provider section and then enable Calendar Integration.

Note:
Default subscription type is not supported in Calendar Integration for Office 365 with OAuth 2.0 Authentication Protocol.

26.19 Synchronization Tab

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab -integrated mode.

Using synchronization, you can quickly populate the MiCollab Client accounts list based on your existing PBX node, Active Directory (AD), or Lightweight Directory Access Protocol (LDAP) corporate directory. In addition, you can schedule periodic synchronizations to keep your MiCollab Client accounts and corporate directory synchronized.

From the Synchronization tab, select the Enterprise from the list box, and then select a synchronization type .

Synchronization Type

To select a synchronization type:

1. Select one of the following synchronization options:

   - **None**: Select this option if you do not want to populate your account list using a corporate directory synchronizer. If you select this option, you will need to add all MiCollab Client accounts manually.
   - **Active Directory/LDAP Synchronizer**: Select this option if you want to populate the MiCollab Client accounts database using the company AD or LDAP directory. You will then need to add an AD/LDAP synchronizer. To provide ongoing synchronization between MiCollab Client and the AD/LDAP directory, you can schedule automatic synchronizations. You can also complete manual synchronizations. When you click the **Sync Now** button, the AD/LDAP directory is synchronized with the MiCollab Client Service. Refer to the Common AD/LDAP Field Mappings topic for information about field mappings between AD and LDAP.
   - **PBX Node Synchronizer**: Select this option if you want to populate the MiCollab Client accounts database using the user/extension information programmed for the PBX node database. To provide ongoing synchronization between MiCollab Client and the PBX node database, you can schedule automatic synchronizations. You can also complete manual synchronizations. When you click the **Sync Now** button, all of the PBX nodes are synchronized with the MiCollab Client Service .

   Note:
   After you complete phone extension configuration changes (add, delete, move, change) on the PBX, perform a manual synchronization (**Sync Now**) to *immediately* update the affected MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization.

   In addition, for those MiCollab Client users whose extensions are affected by the configuration changes you make on the PBX, instruct the users to exit and then restart their MiCollab Desktop Clients to refresh extension information.
2. Click **Apply**.

After you select a synchronizer, you can complete the following tasks:

- Perform a manual synchronization .

  To perform a manual synchronization, click **Sync Now**. The MiCollab Client accounts database is synchronized with the AD/LDAP directory or the PBX Node database.

- Schedule a day and time to perform automatic synchronizations.

  Schedule automatic synchronizations for the MiCollab Client accounts database and the AD/LDAP directory or the PBX node database.

  To schedule automatic synchronizations:

  1. Specify the following to schedule the synchronization:
     - The frequency (in days) the synchronization should occur.
     - The hour the synchronization should start.
     - The minute the synchronization should start.
     - Whether the synchronization should occur in the AM or PM.
  2. Click **Apply** to save the information, or click **Reset** to clear your changes.
- *For Enterprises configured for AD/LDAP synchronizers only*, you can also do the following:
- Click Add to add an AD/LDAP synchronizer and configure the settings.
- Click an AD/LDAP Synchronizer link to edit it.
- Delete an AD/LDAP synchronizer. When you delete an AD/LDAP synchronizer, all the accounts associated with the synchronizer are also deleted.

  To delete an AD/LDAP synchronizer:

  1. Select the AD/LDAP synchronizer you want to delete from the list.
  2. Click the **Delete** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the synchronizer, or click **Cancel** to cancel the deletion.
- Check the status of the last AD/LDAP synchronization.

> **Note**:
> For synchronization failures, refer to the Synchronization Error Messages topic.

- *For Enterprises configured for PBX Node synchronizers only*, you can also do the following:
- Check the status of the last PBX Node synchronization on the PBX Nodes tab.
- View PBX Node synchronization details on the PBX Node Details page.
- Specify a feature profile to use for all accounts created during the PBX node synchronization.

Note:
Before specifying a Feature Profile, refer to the Licensed Features and Synchronization topic.

To specify the feature profile to use for PBX node accounts:

1. Create the feature profile for the PBX node on the Features tab.
2. On the Synchronization tab, select the appropriate feature profile from the list box.
3. Click **Apply** to save the information, or click **Reset** to clear your changes.

- Enable or disable the Synchronize Dynamic Extensions only option.

  This option specifies if new accounts are created or not during the synchronization process. By default, this option is disabled. Options include:

  - **Disabled**: When this option is disabled (not selected) the synchronization process pulls data (including Dynamic Extension information) from the PBX nodes and creates MiCollab Client accounts.
  - **Enabled**: When this option is enabled (selected) the synchronization process does not create new accounts. It does however, pull Dynamic Extension data from the PBX node to update existing MiCollab Client accounts. When you enable this option, you must manually create the accounts first.

Note:
The following are valid character ranges for LDAP synch. Anything outside of these is invalid character for LDAP synch:

0x9, 0xA, 0xD, 0x20 to 0xD7FF, 0xE000 to 0xFFFD, 0x10000 to 0x10FFFF

Synchronization Rules for MiVoice Business:

Note:
On MiVoice Business , PRG stands for - **Personal Ring Group**. MDUG - stands for **Multi Device User group**.

1. After creating users with MDUG/PRG, perform a manual PBX synchronization (**Sync Now**) to *immediately* update the MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization.
2. Starting from MiCollab Client 5.1, user can have either a MiNet Softphone or a SIP softphone, but not both.
3. The MiCollab Client will recognize numbers on MiVoice Business with device type as 'App Server Port' or '5020 IP' with MAC address starting with A1:21:00 as MiNet Softphone. Numbers on MiVoice Business with device type as 'MiCollab Client Endpoint' will be recognized as 'UC Endpoint', if user does not have a MiNet Softphone. If user has both number types, then MiCollab Client will assign the MiNet Softphone as User softphone.
4. If user has deskphone and softphone , and no PRG or MDUG on MiVoice Business , then the first name, last name and department fields in MiVoice Business has to match exactly (including case) for the deskphone and softphone for MiCollab Client PBX sync to associate the two phones for same user. This restriction does not apply if user has PRG or MDUG on MiVoice Business and the deskphone and softphone are part of the PRG.
5. When user has PRG or MDUG on MiVoice Business , the first name,last name and department of PRG pilot is used to identify the account in MiCollab Client. The PRG pilot will be assigned as user deskphone or as user softphone.
6. If user has multiple deskphones or SIP phones or MiNet softphones, then PRG or MDUG has to be defined in MiVoice Business and all the user devices have to be part of the group for MiCollab Client to pull in all the phone numbers for that user.
7. When a phone number is deleted in MiVoice Business then it will still show up in MiCollab Client for that account when one or more of the following is true:

   a. The number was manually added in MiCollab Client by the administrator.
   b. Some of the user's dynamic statuses are still pointing to that number for call routing purposes.

   To remove the number from MiCollab Client database, the user has to login to the desktop client and update the dynamic statuses pointing to the deleted number. User has to update the Make Call from setting within each status to point to a different number. Once all the references are removed, the user can delete the number from MiCollab Client database.

Note:
Rule 6 also applies to MiVoice Office 250.

26.199.1 Adding and Editing AD/LDAP Synchronizers

Adding an AD/LDAP synchronizer is a two-step process: configure Connection Settings, and then configure Field Mappings.

To help you generate the LDAP path, which is a required field under Connections, use the LDAP Path Assistant.

LDAP Path Assistant

The LDAP Path Assistant can make it easier to formulate the LDAP URL for a synchronizer, provided that the synchronizer is connecting to an Active Directory server. The Assistant may not work with other kinds of LDAP servers.

To use the assistant, enter the fully qualified domain name (FQDN) of the domain controller in the Assistant. The Assistant will then create an LDAP URL with the format ldap://<*domain-controller-name*>/<*DC= separated top level domain controller name components*>

For example:

- **Domain controller name**: test-controller.mitel.com
- **Resulting LDAP path**: ldap://test-controller/DC=mitel,DC=com

Note:
The path assistant is only intended to assist you in the creation of LDAP URL. Path assistant may ***not*** always work depending on how your LDAP server is configured.

The **Search context** is an LDAP path relative to the absolute path specified in the **LDAP path** field. Together, the values you configure for the **LDAP path** and **Search context** fields determine which LDAP object is the starting point for the search query. For example, if you use the following hierarchy in your LDAP database:

XYZ Company

-> New York Branch

-> Sales Department

-> US Sales

-> Eastern US

To synchronize all accounts from the Eastern US Organizational Unit, you would specify the LDAP fields as follows:

- **LDAP path**: ldap://ldap.example.com/DC=example,DC=com
- **Search context**: OU=NewYork Branch, OU=Sales Department, OU=US Sales, OU=Eastern US

If your search should begin at the root object (for example, the XYZ Company object), you can leave the Search context blank.

To add an AD/LDAP Synchronizer:

1. Configure the AD/LDAP **Connection Settings**.

   Connection Settings allows MiCollab Client to connect to the AD/LDAP directory and import information. Add or edit the following Connection Settings:

   - **Description**: (*Required*) Type a short description for the AD/LDAP synchronizer. This field has a maximum length of 64 characters.
   - **Domain name**: (*Required*) Type the domain name for the AD/LDAP synchronizer. The value can be any unique value. This field has a maximum length of 128 alphanumeric characters, and supports dashes, and periods.
   - **Show LDAP Path Assistant**: Click **Show LDAP Path Assistant**, enter the fully qualified domain name (FQDN) of the domain controller, and then click **Generate Path**. The LDAP path field is populated. Click **Hide LDAP Path Assistant**.

     Note:
     The LDAP Path Assistant is only intended to assist you in the creation of the LDAP URL. Depending on how your LDAP server is configured, it may not always work.

   - **LDAP path**: (*Required*) Type the full LDAP path of the synchronizer will use when connecting to the directory server. This field has a maximum length of 255 characters. Example: ldap://directory.mitel.com/DC=mitel,DC=com
     - **Server supports paging results**: Clear this setting if the LDAP server does ***not*** support paging results extension (refer to IETF rfc2696). Windows Server® 2003 Active Directory and ApacheDSTM servers do support paging results.
     - **Do not import disabled accounts from AD**: This setting is applicable only when connecting to an Active Directory server. DO NOT check this for other kinds of LDAP servers. If checked, MiCollab Client will not import disabled accounts from Active Directory. To find out if an account is disabled or not, on ActiveDir server, open the "Active Directory Users and Computers" tool, navigate to the account, right-click on the account, and select Properties. Under the Account tab -> Account Options, the "Account is disabled" field will show the account status.
   - **Search context**: (*Optional*) This field points to the LDAP object on the sub-tree where the search query is run. If you complete this field, the value MUST be relative to the initial context specified by the **LDAP path** parameter. If you leave this field blank, then the query search is performed on the LDAP root object pointed to by the "LDAP path" parameter. This field has a maximum length of 255 characters. Example: (ou=Sales).
   - **User query**: (*Optional*) If specified, this field should be a valid LDAP query string, which is used to selectively query for and import user accounts. If your leave this field blank, the query string (|(objectClass=person)(objectClass=user)) is used. This field has a maximum length of 255 characters.
   - **Username**: (*Optional*) Type the username for the directory server. The username can be an LDAP distinguished name. Example: CN=Administrator,OU=engineering,DC=directory,DC=mitel,DC=com. If the directory server is Active Directory, it can be the qualified Active Directory username. Example: engineering\jsmith.

Note:
The specified user must have privileges to read information relevant to all accounts that expect to be synced into MiCollab Client .

- **Password**: (*Optional*) Type the password for the directory server.
- **Default feature profile**: (*Required for Account AD/LDAP Synchronizers only. This field is not displayed for external server AD/LDAP Synchronizers*) Select the feature profile you want to apply to the accounts created by the synchronizer. By default, the **Default Feature Profile** is selected.

Note:
The Default Feature Profile does not include any features. To assign features to users when you create accounts during the initial synchronization, you must first create a Feature Profile that includes the features you want to use, and then you can select it here. Refer to the Licensed Features and Synchronization topic before selecting a Feature Profile.

- **Timestamp**: MiCollab Client Service uses the modification timestamp on LDAP objects to optimize processing. This is mainly used for display picture importing and MiCollab Client tries to import only those display pictures which have changed on the LDAP server since the last time MiCollab Client did a successful sync.
  - **Timestamp attribute**: This is the attribute name of the LDAP field which contains the modification timestamp. In case of Active Directory, the attribute is ***whenChanged***. If your LDAP server has some other attribute name, specify that instead.

Note:
If this attribute is left blank, MiCollab Client Service will try to import display pictures for all eligible accounts, regardless of when they were modified. While a blank timestamp attribute is not a recommended configuration for regular use (because display picture import can consume substantial cpu/ memory), it can be used to force a re-import of all display pictures if required for troubleshooting, error recovery, etc. To do this, blank out the timestamp attribute and perform a sync. After the sync, set the timestamp attribute back to its original value and sync again.

  - **Timestamp syntax**: The format of the timestamp value contained in the timestamp attribute. For Active Directory, this is X680 format. Some older LDAP servers may use the X208 format.

2. Do one of the following:

- If you are adding a new AD/LDAP synchronizer, click **Next**.
- If you are editing an existing synchronizer, click **Save**.

3. Configure the **Field Mappings** between the directory and the MiCollab Client accounts.

   Field Mappings specify how AD/LDAP database fields are mapped to MiCollab Client account fields when the information is synchronized.

   a. If required, edit the default values in the **Account Information** field. The table below defines the field mappings from AD/LDAP objects to MiCollab Client accounts. Based on the fixed label and description provided for each field, determine if you need to edit the default values. To edit a field, delete the existing value and type a new value in the text box.

Field	Default Value	Description
Directory key	objectGUID	This is the unique key that identifies the account in the directory. If the directory object does not have a value for this field, it is not imported.
PBX node	facsimileTelephoneNumber	Identifies the PBX node, or switch, that the user's phone is configured on. If the directory object does not have a value for this field, it is not imported.
First name	givenName	The user's first name. This field can be blank.
Middle name	initials	The user's middle name. This field can be blank.
Last name	sn	The user's last name. This field can be blank.
Login ID	sAMAccountName	The login ID that the MiCollab Client Desktop Client uses to authenticate with the MiCollab Client Service. This field can be blank.
Desk phone extension	ipPhone	The user's desk phone extension. This field can be blank.

Field	Default Value	Description
Soft phone extension	otherIpPhone	The user's soft phone extension. This field can be blank.
Company name	company	The user's company name. This field can be blank.
Address	streetAddress	The user's street address. This field can be blank.
City	l	The user's city. This field can be blank.
State/Province	st	The user's state. This field can be blank.
ZIP/Postal code	postalCode	The user's ZIP/postal code. This field can be blank.
Display picture	jpegPhoto	The user's display picture. This field can be blank.

b. Add, Edit, or Delete **Phone Numbers**, **E-mail Addresses**, and **Instant Message (IM) Addresses** from the existing tables.

c. Do one of the following:

- If you are adding a new AD/LDAP synchronizer, click **Done**.
- If you are editing an existing synchronizer, click **Save**.

After you create an AD/LDAP synchronizer, you can edit the associated fields at any time.

Refer to the Common AD/LDAP Field Mappings topic for information about field mappings between AD and LDAP.

26.20 PBX Nodes Tab

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab-integrated mode.

The PBX Nodes tab provides a table for the PBX nodes you have added to the Enterprise.

Select the Enterprise from the list box and the following information is displayed for each PBX node configured:

- **IP Address**: Indicates the IP address for the PBX server.
- **Description**: Indicates the description that you provide for the PBX node.
- **Version**: (MiVoice Business only): Indicates the software version the PBX is currently running.
- **Extension Length**: Specifies the number of digits used for extensions on the PBX node.
- **Voice Mail Number**: Specifies the voice mail extension for NuPoint UM on the PBX node.
- **Last Sync**: Specifies the date of the last PBX node synchronization.
- **Sync Status**: Specifies the status of the last PBX node synchronization. Results include **In Progress**, **Success**, **Success with Info** and **Failure**. You can view synchronization details from the PBX Node Details page.

Note:
For synchronization failures, refer to the Synchronization Error Messages topic.

CSTA settings

The following fields are only displayed when MiCollab Client is integrated with MiCollab and MiVoice MX-One or MiVoice 5000.

- Port: Type the port MiCollab Client uses for MiVoice MX-One or MiVoice 5000. This setting should remain at default. If the PBX port number changes, the PBX administrator needs to inform you so you can modify this setting.
  - MiVoice MX-One : Default value is 8882.
  - MiVoice 5000 : Default value is 3211. In rare instances, there may be multiple ports for the MiVoice 5000. Type the port numbers, up to three, separated by a semi-colon.

Note:

If you change the Feature Access Code on UCA, you need to restart the client.

- Extended checking of the phone device: Default is Off. Turn on only when directed by support.
- Print PDU: MiVoice 5000 only. Default is Off. Turn on only when directed by support.
- Number of log files: MiVoice 5000 only. Type the number of log files to store. Default value is 10.
- Maximum file size: MiVoice 5000 only. Type the maximum log file size. Default value is 3 MB.
- Protocol file: MiVoice 5000 only. Type the name of the file used for the trace. Default is pdutrace.
- XML trace active: MiVoice MX-One only.
- Use phone number block: Type the device range to handle devices only in this range. For MiVoice 5000 the range is 2001 to 3001
- Group Call Pickup Feature Access Code: This option is visible to both PBX types, MX-One and MiVoice 5000. This option helps to store the feature access code which is provisioned in MX-One for Group Call Pickup in the UCA database.

Note:

If the Group Call Pickup Feature Access Code (FAC) is changed in the administrator portal, then no notification is sent to the clients. Clients will need to re-login to get the updated FAC details.

Note:

MiVoice 5000 : PDU log files are stored in the default log folder for CSTAProxy / UCA: /opt/intertel/log. View and retrieve PDU log files using the default MiCollab log file viewer.

You can complete the following tasks for PBX nodes:

- Sort the information in the table.
- Select one or more entries in the table.
- Click the Add Node link to add a PBX node.
- Click the PBX node link in the **IP Address** column to edit the PBX node.

- Delete a PBX node.

  To delete a PBX node:

  1. Select the node you want to delete from the PBX node list.
  2. Click the **Delete Node** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the node, or click **Cancel** to cancel the deletion.
- Synchronize specified PBX nodes.

  To synchronize one or more nodes:

  1. Select the nodes you want to synchronize.
  2. Click the **Synchronize** link. A dialog box appears prompting you to confirm the synchronization.
  3. Click **OK** to start the synchronization, or click **Cancel** to cancel the synchronization.

  Note:
  The **Synchronize** link only appears when the PBX Node Synchronizer has been enabled on the Synchronization tab. The **Synchronize** link does not apply to multi-node Mitel MiVoice Office 250 sites that are configured for synchronization with a CT Gateway. For this type of configuration, all of the nodes can be synchronized using the **Sync Now** button on the Synchronization tab.

- Click  to open the PBX Administration Tool .

  Using the PBX administrator's Web window, you can complete configuration, maintenance, and diagnostic tasks for the PBX node, without logging out of the Unified Communications administrator interface. Close the PBX administrator's Web window when you have finished updates to the PBX node.
- Click  to complete a Line Monitor Cache refresh (*MiVoice Business only*).

  During a Line Monitor Cache refresh, the MiCollab Client Service requests updated information for the MiVoice Business phone lines configured for MiCollab Client. On average, the refresh takes one second per single-line set and two seconds per three or four-line set.

  Note:
  System Performance . During a line monitor cache refresh, clients are taken offline temporarily, and then automatically returned to service with the new line configuration. Schedule line monitor cache refreshes during low traffic periods. No server reboot is required.

- Refresh the information on the page.

26.200.1 Adding and Editing PBX Nodes

You can add new PBX nodes and edit existing PBX nodes on the PBX Node Details page.

Note:
The fields on the PBX Node Details page vary between MiVoice Business, MiVoice Office 250, MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400 PBX nodes. Some fields are PBX-specific and do not appear if they are not required for the PBX.

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab -integrated mode. MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400 are only supported in MiCollab integrated mode. Refer to the MiCollab Administrator Help for more information.

If you are configuring multiple MiVoice Office 250 nodes, click here to review information about using a CT Gateway.

For multiple MiVoice Office 250 nodes, you can streamline the synchronization process by configuring synchronization between the Unified Communications server and a single CT Gateway supporting the multi-node configuration.

After you configure the CT Gateway for synchronization, you do not need to complete synchronizations for each PBX node. When the MiCollab Client Service synchronizes with the CT Gateway, the required data for all of the associated PBX nodes is updated on the Unified Communications server.

To configure CT Gateway synchronization:

1. Add each PBX node in the multi-node configuration to the MiCollab Client Service (Adding and Editing PBX Nodes).
2. Add the CT Gateway as the final PBX node in the configuration (Adding and Editing PBX Nodes).
3. Configure PBX Node synchronization (Synchronization tab).

Remember the following guidelines when configuring a CT Gateway for multiple MiVoice Office 250 nodes:

- You cannot synchronize individual PBX nodes. However you can synchronize all nodes using the **Sync Now** button on the Synchronization tab.
- All PBX-node level settings, including **Voice mail server** and **Voice mail public number**, should be configured for the actual PBX node, and not the CT Gateway node.
- Each node's Session Manager must have a DB Programming account with a password that matches the password set for the single CT Gateway node.
- The CT Gateway must be running software version 4.4.01 or higher.
- All nodes configured on the CT Gateway must be communicating (up and working) so that the PBX synchronizer will synchronize all of the accounts. If one or more of the MiVoice Office 250 nodes are not

communicating with the CT Gateway, the node will not be synchronized as indicated by the message that is generated under the PBX Nodes tab.

- All nodes connected to the CT Gateway must be using OAI protocol version 10.0 or later (MiVoice Office 250 v3.2 or later). Node connections to the CT Gateway that are not running protocol version 10.0 or later must be removed from the CT Gateway, or the nodes must be upgraded to v3.2 or later.
- It is recommended that all duplicate extensions between nodes be removed before installing the CT Gateway. If this is not done, one of the accounts with the duplicate extension information will be deleted during the synchronization.

Note:
You are not required to configure the resilient node.

To add or edit a PBX node:

1. Configure the PBX node Settings.

   - **Description**: (*Required*) Type a name for the PBX node. By default, this field is blank. The Description field is limited to 1-64 characters in length, and must contain alpha-numeric characters (dashes and spaces included).
   - **Hostname**: (MiVoice Business Only - *Required*) Type the IP address or hostname for the MiVoice Business PBX node in this field. By default, this field is blank.

     Note:
     The values for the following read-only fields apply to MiVoice Business PBXs only and are generated after the MiCollab Client Service synchronizes with the PBX.

     - **Version**: Indicates the software version that the MiVoice Business PBX is currently running.
     - **Handoff feature code**: Indicates the feature code programmed for the Handoff feature on the MiVoice Business PBX.

     As a prerequisite, the MiVoice Business Feature Code for Handoff must be programmed. If this feature is added to an existing server, the PBX need to be synchronized with MiCollab Client before the feature can be used.
   - **Internal IP address/hostname**: (*MiVoice Business only - Required*) Type the internal IP address or hostname for the Mitel MiVoice Business PBX node in this field. If your PBX configuration includes an expanded Processing Server (PS1), type the IP address of the base server in this field and type the IP address of the PS1 in the OAI IP address/hostname field.
   - **External IP address/hostname**: (*Mitel MiVoice Business / Mitel MiVoice Office 250 Only - Optional*) Type the external IP address or hostname for the PBX node. This field applies to remote

MiCollab Client softphones in teleworker mode. The External IP Address/Hostname provides a communication path between remote users and the PBX. By default, this field is blank.

- **Extension length**: (*Required*) Extension length is the maximum length that can be configured for a PBX DN. The DN extension can range from 1 to the maximum extension length. Select the number of digits used for internal extensions on the PBX. Options include 3-7 digits. By default, this field is set to 4.
- **Registration code**:(*MiVoice Business Only-Required*) Type the registration code as configured on the MiVoice Business PBX. The valid length is 1-10 digits, and valid characters include 0-9, *, and #.

  The registration code corresponds to the Set Registration Access Code or Set Replacement Access Code, programmed in the MiVoice Business System Administration Tool (Systems Options Assignment form). These codes, typically 3 characters in length, can be a maximum of 10 characters long. A single Set Registration and Set Replacement Access Code applies to all IP devices on the system. Set Registration and Set Replacement Access Codes make up the first part of an IP device Personal Identification Number (PIN). The second part of the PIN is the IP device extension. For example, if an IP device has a PIN of 9991000, 999 is the Set Registration/Replacement Access Code and 1000 is the extension number.

  The registration code can be one to 10 characters in length, and can include digits 0-9, *, and #. By default, this field is blank.
- **Dialing prefix**: (*Optional*) Type the number that the user dials to obtain an outside line on the system. The dialing prefix is inserted automatically when the user makes a call from the History view, or from an imported contact. The prefix can be dialed even while manually entering the digits. The dialing prefix can be 1-32 digits in length, and can include digits 0-9. By default, this field is blank.

  The dialing prefix is not inserted by MiCollab Client when the number dialed starts with the '-' character (a hyphen). For example, if the number dialed by the MiCollab Client is -4809619000, then the number dialed by the PBX is 4809619000 (without the hyphen). If the number dialed by the MiCollab Client is 4809619000, then the number dialed by the PBX is 94809619000, where 9 has been defined as the PBX node outgoing prefix.
- **Voice mail server:** (*Specific to NuPoint voice mail only - Optional. If an embedded voice mail is in use, then do not enter it.*) Type the IP address or hostname for the node's voice mail server. The voice mail server configured here serves all accounts assigned to this node. If this field is left blank, all accounts assigned to this node will use the voice mail server configured on the Enterprise tab. If required, you can configure a different voice mail server on a user's account, which will override the voice mail server you configure here and on the Enterprise tab. The voice mail server can be 1-128 characters in length.
- **Voice mail number**: (*Required*) Type the voice mail extension for NuPoint UM. If required, you can configure a different voice mail extension on a user's account, which will override the extension you configure here. The voice mail number can be 1-32 digits in length, and can include digits 0-9. By default, this field is blank.

  If MiCollab Client is running in integrated mode and you change the voice mail number, it is applied to all MiCollab Client accounts on the PBX. If MiCollab Client is running in co-located mode, it is just applied to new accounts (see following option).
- **Apply voice mail number to all accounts**: (*Optional*) This option is only present when MiCollab Client is running in co-located mode. It allows you to quickly change the **Voice mail number** for all accounts on the node configured for the same voice mail number. After you change the Voice mail number, select this option, and then click **Save**. All accounts that were configured for the previous Voice mail number are updated to the new Voice mail number.
- **Voice mail public number**: (*Optional*) Type the voice mail public number for NuPoint UM. If required, you can configure a different voice mail public number on a user's account, which will

override the voice mail public number you configure here. The voice mail public number can be 1-32 digits in length, and can include digits 0-9. By default, this field is blank.

- **No answer timer**: (*Optional*) Type an amount of time, in seconds, slightly less than the amount of time that will elapse before an incoming unanswered call is directed to voice mail. This setting is used by MiCollab Client for call forwarding. The No answer timer can be 0-60 seconds in length. By default, this field is set to 16 seconds.
- **Username**: (*Required only for* MiVoice Business) Type the username of the preconfigured account on the PBX node that will be used by the MiVoice Business PBX node synchronizer. The username field can be 1-64 characters in length. By default, this field is blank.

  To configure an MiVoice Business PBX node synchronizer, an administrator user account must exist on each MiVoice Business node (User Authentication Profiles in the MiVoice Business System Administration Tool). This account must have System Access enabled. The MiVoice Business user name and password must be specified in the properties of each switch that will be synchronized.

> **Note**:
> For security reasons, you can create an administrator user account that has System Access enabled, with No Access as the assigned Access Type using the System Administrator Policies form.

- **Password**: (*Required only for* MiVoice Business) Type the password of the preconfigured account on the PBX node that will be used by the PBX node synchronizer. This is the password for the MiXML, and MiTAI connection to the node. The password can be 1-64 characters in length. By default, this field is blank.

> **Note**:
> Make sure that you enter the correct MiVoice Business System login credentials. If the credentials are incorrect, the ***PBX_PROXY_MitaiOpenPBXFailed*** alarm is triggered. If this occurs, reenter the correct credentials, and restart the ***PBX_PROXY*** module from the *MiCollab Client Service Diagnostics* page or perform a **Line Monitor Cache** refresh from the *PBX Nodes* page. The login credentials that you reenter take effect only after you perform either of these two operations.

Note:
MiTAI authentication is supported on MiVoice Business release 9.0 and later. It is recommended to turn OFF the authentication for earlier releases of primary and secondary MiVoice Business versions.

- **Internal OAI IP address/hostname:** (*Mitel MiVoice Office 250 Only)* This field is only required when the Mitel MiVoice Business PBX node includes an expanded Processing Server (PS-1). Type the internal IP address of the PS-1 in this field. Type the IP address of the base server in the Internal IP address/hostname field.
- **External OAI IP address/hostname:** (Mitel MiVoice Office 250 Only -Optional) This field is only required when the Mitel MiVoice Business PBX node includes an expanded Processing Server (PS-1). Type the External IP address of the PS-1 in this field. This field applies to remote MiCollab Client SIP softphones in teleworker mode. The External IP Address/Hostname provides a communication path between remote users and the PBX. By default, this field is blank.
- **OAI port** (*Mitel MiVoice Office 250 Only - Required)*: Type the port number used for the OAI connection to the MiVoice Business node. The range for this field is 1-65,535. By default, this field is 4000.
- **OAI password**: (*Mitel MiVoice Office 250 Only - Optional)* Type the password of the preconfigured account on the PBX node that will be used by the PBX node synchronizer. This is the password for the OAI connection to the node. The password can be 1-64 characters in length. By default, this field is blank.
- IP/Digital Telephone Database Programming Password: (*Mitel MiVoice Office 250 Only – Optional*) Type the password required by Administrator phones, when programming the Mitel MiVoice Business system through the phone. The password can consist of up to eight numeric characters. By default, this field is blank. In Mitel MiVoice Business Database Programming, this field is located under System\Phone-Related Information\IP/Digital Telephone Database Programming Password \Edit Password.
- Language: (*Optional*) Select a language from the list if you want to override the Enterprise language settings for the PBX. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. The user's language setting determines which language the Welcome E-mail Message is generated in for that user.
- Reload Dialed Digits Processing Template Files: Select the dialed digits processing logic to be used when a MiCollab Client user enters a phone number from the client. Once the dialed digit processing files are modified, clicking on this button will reload the files into the MiCollab Client system. This will update the processing logic for all PBXs across all enterprises on that MiCollab Client Service .

Note:
The dialed digits processing logic should not be modified unless instructed to do so by Mitel support personnel. Since this affects the very way numbers are dialed from MiCollab Client , incorrect processing may render useless large parts of the system.

2. Configure the Plus Dialing Settings.

   This area of the PBX Node Details page includes fields for specifying plus dialing settings.

   Note:
   Starting with MiCollab Client 5.1, some of the dialed digit processing happens locally within MiCollab Client. Due to this, if some dialing settings are changed in the server-manager, all clients within that enterprise (or for that PBX) should be restarted. Following are the settings affected by this:

   - At the enterprise level:
     - Plus Dialing settings -> Country code
     - Plus Dialing settings -> International access code
     - Plus Dialing settings -> Long distance access code
   - At the PBX Node details level:
     - Plus Dialing settings -> Country code
     - Plus Dialing settings -> International access code
     - Plus Dialing settings -> Long distance access code
     - Extension length
     - Dialing prefix

   The plus dialing settings include:

   - Country code: This field should be set to the country code of the country where the PBX resides. If an E.164 call is placed to a number within the user's "home" country, the country code will be stripped off of the digit string by MiCollab Client .
   - International access code: This field indicates the international dial code that must be dialed for international calls from the country where the PBX resides. If the MiCollab Client determines that the call is being placed outside of the user's country (based on the PBX country code), MiCollab Client will pre-pend the International Prefix.
   - Long distance access code: This field indicates the Toll digit for the country where the user's PBX resides. For any E.164 dialed calls within the user's home country, MiCollab Client will prepend the toll digit.

   Note:
   It is important that sites using E.164 (plus dialing) settings set up ARS on the PBXs to strip the Toll Digit for local calls.

Note:
The Plus Dialing Settings on the PBX Node tab override those on the Enterprise tab.

Note:
starting with + and strips the (0) from the digit string before processing the dialed digit string for insertion of the international access code and the long distance code. This change addresses the needs of European customers who have numbers such as +44(0)<number> in their contacts. The (0) in the number is optional, based on the location from which the user is calling the number. For example, if the number +44(0)6665544 is dialed from the MiCollab Client by a user in the United States SA, then the number dialed by MiCollab Client is 011446665544 where 011 is the international access code and 44 is the country code of the United Kingdom. If the same number is dialed from the MiCollab Client by a user within the United Kingdom, then the number dialed by MiCollab Client is 006665544, where 0 is the dialing prefix, the dialing prefix, and also the long distance code defined for the PBX node under the Plus Dialing settings.

3. Configure the CLID Translation.

CLID Translation: This field is only applicable to 3300 type PBX. This field should be set to a list of comma separated digits (such as 0, 00). The MiCollab Client Service will them remove these leading digits from incoming numbers before generating call records and call history information.

At most, one digit string (the first one that is applicable) will be applied to any given number. For example, suppose the incoming number is 001143476276 and the CLID translation is specified as 00, 11. The MiCollab Client Service will translate that number into 1143476276, due to the fact that the first CLID translation string (00) matched the leading digits of the incoming number. The fact that the next CLID translation string (11) matches the now leading digits of the incoming number is inconsequential because the CLID translation has already been done once.

Note:
This feature is only applicable to 3300 type PBX.

Note:
Whitespaces in the field are ignored.

Note:
If the field is empty, then the CLID translation settings at the enterprise level will take effect. If the enterprise level CLID translation string is empty as well, then no translation is done.

4. Configure the default Dynamic Status Phone Settings. Set the defaults according to the PBX node type: MiVoice Business or MiVoice Office 250.

   These default settings are used on the Dynamic Status page in the desktop client.

   - Forward my calls to:
     - Use PBX Default *(default)*
     - Voice Mail

     Note:
     The Under these conditions option is available only if Forward my calls to is set to Voice Mail.

   - Under these conditions:
     - Busy *(default)*
     - No Answer
     - Busy and No Answer

   These default settings are used on the Dynamic Status page in the desktop client.

   - When I am on the phone:
     - Use PBX Default *(default)*
     - Voice Mail
   - If I do not answer:
     - Use PBX Default *(default)*
     - Voice Mail

5. *For MiVoice Business PBX nodes*, schedule Line Monitor Cache refreshes.

   During a Line Monitor Cache refresh, the MiCollab Client Service requests updated information for the MiVoice Business phone lines configured for MiCollab Client. On an average, the refresh takes one second for a single-line set and two seconds for three and four-line sets.

   Note:
   System Performance During a line monitor cache refresh, clients are taken offline temporarily, and then automatically brought online to the service with the new line configuration. Schedule line monitor cache refreshes during low-traffic periods. No server reboot is required.

   To schedule line monitor cache refreshes:

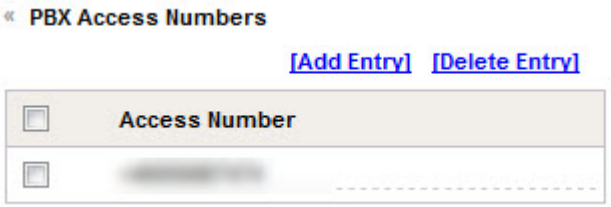
   a. Select a day or days of the week to perform the refresh.
   b. Select an hour, minute, and specify AM or PM to schedule the refresh.
6. *For MiVoice Office 250 PBX nodes,* skip to the step 4.
7. Configure the **PBX Access Numbers**.

   This number is used for Call Through feature and should match the DID number (DID number terminating on the Hot Desking Access Number) configured on MiVoice Business and the R3 number configured on MiVoice MX-ONE. Multiple access numbers can be configured depending on the PBX configuration.

Note:
Call Through feature is supported on MiVoice Business 8.0 SP3 and later and MiVoice MX-ONE 7.0 and later.

To configure the PBX access number in MiCollab:

a. Go to **MiCollab Client Service** > **PBX Nodes** and select the node to be used.
b. Under **PBX Access Numbers**, click **Add Entry**.



c. Enter the Access Number in the **Add value** text box.

Note:
It is recommended that you configure the PBX access numbers in E.164 format so that these numbers can be dialed from any country. For example, the Country Code for India is +91, and the PBX Access Number will be +91xxxxxxxx.

d. Click **Save**.

To add multiple access numbers, repeat steps 2 through 4.

To delete an access number, select the number and click **Delete Entry**.

Note:
For Call Through feature to work, configure the PBX and MiCollab for Mobile Client as mentioned in the below sections.

PBX configuration for Call Through feature MiVoice Business configuration

- **T1 PRI and Hot Desking Access Number configuration**

  T1 PRI Trunk must be configured. For information on Trunk Configuration, see *MiVoice Business System Administration Tool Online help*.

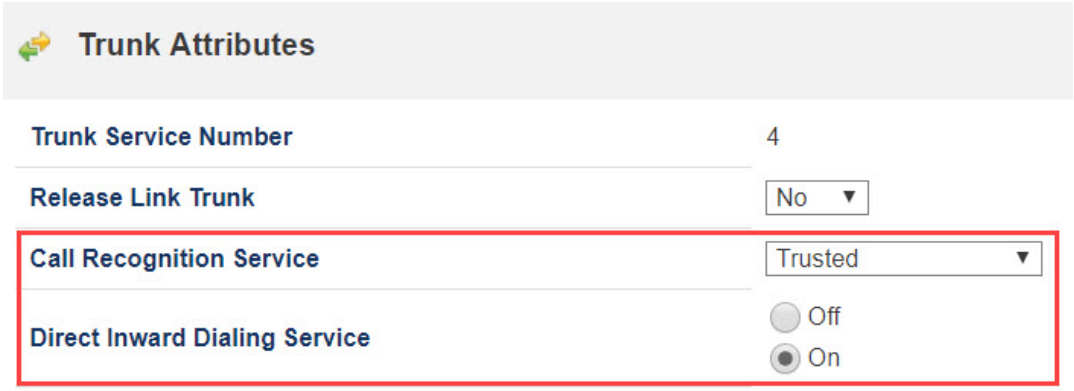
  The Hot Desking Access Number must be configured on MiVoice Business and a corresponding PSTN access number (DID) must be configured on the MiVoice Business and the PSTN gateway. This PSTN access number must be configured to route the calls to the Hot Desking Access Number.

For more information about configuring the Hot Desking Access Number and the DID number, see *MiVoice Business System Administration Tool Online Help*.

- Call Recognition Service (CRS) configuration

To define trunk attribute parameters:

a. Go to **MiVoice Business System Administration Tool** > **Trunk Attributes** form.
b. Select the configured **Trunk Service Number** (for the above T1 PRI Trunk) and click **Change**.
c. Select **Trusted** against **Call Recognition Service** and select **On** against **Direct inward Dialing Service**.



d. Click **Save**.

- Suppress Dial Tone configuration

When the called party ends the call, the calling party (initiating the Call Through call) receives a dial tone. This can be turned off from the **Hot Desk External User – Dial Tone on Call Complete** setting in *MiVoice Business System Administration Tool* > *Class of Service Options* form.

- DTMF Tone configuration

Call Through feature is dependent on CRS being activated. For added security, a Class of Service feature must be enabled for users to be able to have their DTMF tones acted on by the call manager.

This can be enabled from the **Hot Desk External User – Allow DTMF Dialing** setting in *MiVoice Business System Administration Tool*> *Class of Service Options* form.

MiVoice MX-ONE configuration

- **T1 PRI configuration**

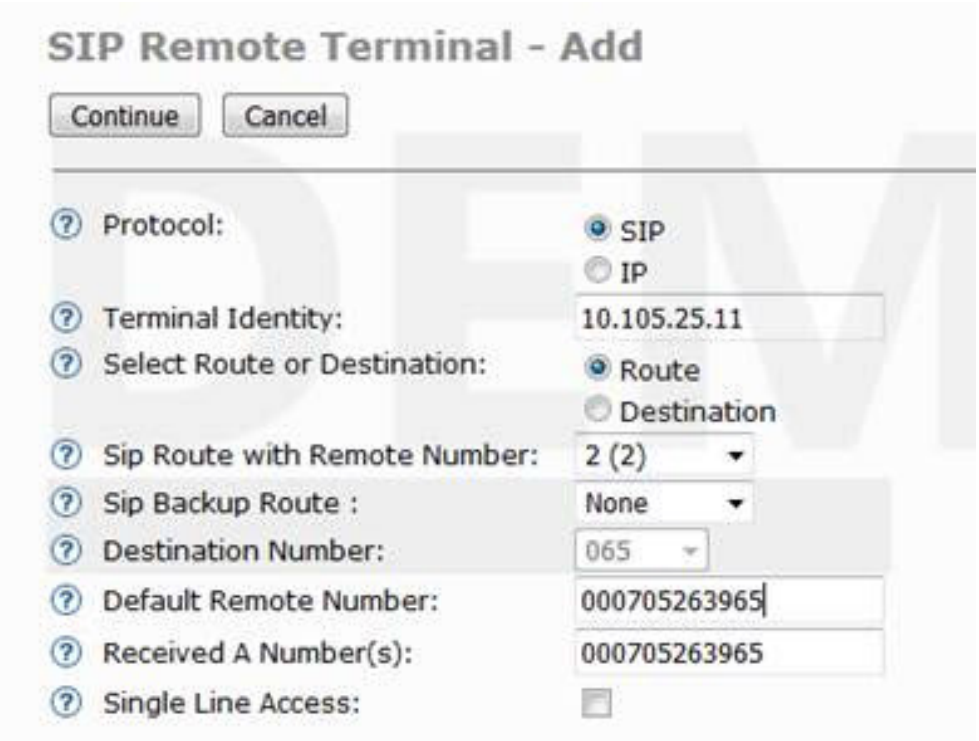
  T1 PRI number must be configured on MiVoice MX-ONE. For more information about creating a trunk code and configuring the PRI Trunk, see *MiVoice MX-ONE Provisioning Manager User Task* > *Users* section.
- **Remote Number R3 configuration**

  a. Create the Remote Number R3 for the user.
  b. Configure the user in MiVoice MX-ONE Provisioning Manager:
  c. Provision the Remote Extension number.

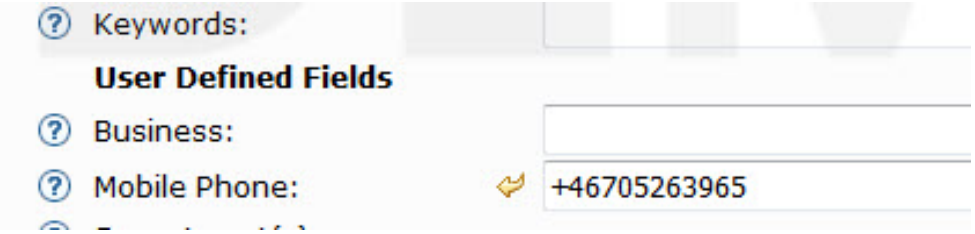
  i. Initiate a remote extension for ISDN Trunks(under **Services**> **Extension**).



  ii. Initiate a remote extension for SIP trunks.



iii. Enter the mobile number for the user (under **Users**> **User**).



Note:
Make sure that the mobile number is configured for the user in MiCollab Server Manager (Users and Services).

- **Subscribing Centralized Call History from MiVoice MX-ONE**

  In the **Enterprise** tab under **Call Log Settings** tab, you can enable or disable the Centralized Call History feature on MiCollab. If you enable this feature, MiCollab Server synchronizes Call History logs for all its users from the interfacing MX-ONE. MiCollab does this by subscribing to the MX-ONE for Call History events for all configured phone numbers of its users.

Note:

If this feature is disabled, MiCollab Client Service shall not subscribe to the MX-ONE for Call History events and will behave as earlier, that is, it will create its own Call History entry in its database whenever any user completes any incoming, outgoing, or missed call.

Note:

This feature is available on MiCollab version 9.5 onward and shall only work with MX-ONE version 7.4 SP1 or above.

It is necessary that you configure the appropriate settings on MX-ONE and MiCollab to enable the Call History feature.

Configuration on MX-ONE:

a. Must enable the **Enable Centralized Name And Number Log** for all MX-ONE CSPs for which this feature is required. There are two ways to do this:

- **Using SNM User Interface:** From the **SNM** tab, select **Telephony**> **Extension**> **Common Service Profile**. Select the CSP that is required to be modified, and then select the **Service Category**tab. After this, click on the **Enable Centralized Name And Number Log** checkbox to enable it for the selected CSP. Do these steps for all CSPs for which this feature needs to be enabled. Refer to the MX-ONE document on SNM GUI for more details.
- **Using the command line:** Set attribute **cnnlog** to **1x** for all the extension profiles of MX-ONE for which this feature is required. Refer to MX-ONE documentation [Section 6.1.2 of Document ID 38_15431-ANF90114] for details on how to set this attribute.

Note:

Without enabling **Enable Centralized Name And Number Log** settings for all the required CSPs, MX-ONE will send empty responses preventing MiCollab Client users from viewing the updated Centralized Call History entries on the Client UI.

b. FQDN of MiCollab Client Service must be reachable from MX-ONE. This is done using 'sudo -H mxone_maintenance' on MX-ONE and then select **DNS settings** > **Forwarders** > **Change setting for DNS forwarding**. Alternatively, you can provide an entry of MiCollab Service's hostname and IP address in the /etc/hosts file of MX-ONE. Refer to MX-ONE documentation for details on DNS forward settings.

c. Valid SSL certificates must be deployed on the MX-ONE so that MiCollab server communicates with MX-ONE over HTTPS. Without a valid certificate on MX-ONE, the feature would not work, and enabling this feature on MiCollab shall fail.

d. It is recommended to create a new DN (Directory Number) on the MX-ONE system, and then specify the same DN and password for the **Username** and **Password** fields under **Enable Centralized Call History** checkbox on the MiCollab Client Service Admin Portal. This **Username** and **Password** must be created in MX-ONE with the command `user_authentication`. For more information about the command, see MX-ONE documentation [Document IDs 1_19082-ANF90114 and 201_19082-ANF90114].

Note:

If you modify the DN and (or) password on the MX-ONE, you must also update the **Username** and **Password** fields for the **Centralized Call History feature** on the MiCollab Client Service Admin Portal.

Refer to below **Configuration on MiCollab** section for more details.

Configuration on MiCollab:

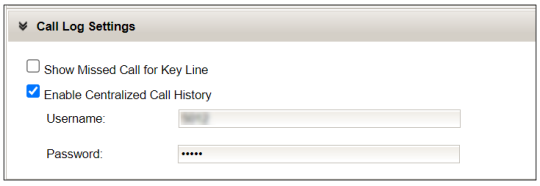
a. Valid SSL certificates must be deployed on MiCollab → Web Server so that MX-ONE can send Call history events securely over HTTPS.

b. To enable the Centralized Call History feature on MX-ONE, go to **MiCollab Client Service** > **Configure MiCollab Client Service** > **Enterprise** tab > **Call Log Settings**, and configure the settings for the **Centralized Call History** feature.

- Select the **Enable Centralized Call History** check box, and then provide correct values in the **Username** and **Password** fields.

Note:

For **Username** and **Password** fields, provide the same DN and password that were created initially as specified in the step (**d**) of **Configuration on the MX-ONE**section.



c. After configuring the above-listed settings, click **Apply**. The server will validate the credentials (user name and password). If the credentials are valid, the feature will be enabled and the server will be subscribed to MX-ONE for the Centralized Call History feature for all users.

Note:

If the DN and (or) password are incorrect, the validation fails, in which case, the settings made will not be saved, and the Centralized Call History feature will remain disabled on the MiCollab.

Note:

Clicking the **Apply** or the **Reset** button will save or clear all the settings provided in the **Enterprise** tab.

Below are the possible failure scenarios when the admin tries to enable the **Centralized Call History** feature in the MiCollab Client Service Admin Portal:

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
I class="- topic/p ">Invalid Call History Username or Password	Admin has provided an incorrect user name and (or) password to enable the **Enable Centralized Call History** in the **Call Log Settings** tab.	Verify that the correct DN (Directory Number) and password are specified in the **Username** and **Password** fields. It must match the DN and password created on MX-ONE, as specified in step (d) of **Configuration on MX-ONE** section.
Server Error occurred during fetching of certificate from MX-ONE PBX: Unable to retrieve SSL certificate.	MiCollab Client Service Admin Portal is unable to communicate with MX-ONE over HTTPS because the SSL certificate on MX-ONE is either not installed or is invalid or expired.	Check and correct the SSL certificate deployed on MX-ONE by referring to the MX-ONE documentation.
Server error during call history credentials authentication: connection refused or connection time out.	Due to network issues, a Timeout occurred while communicating with MX-ONE.	Try again after some time. If the problem persists, check the network connection between MiCollab and MX-ONE. Check whether all services are running appropriately on MX-ONE.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
Error from MX-ONE PBX while validating Call History credentials - received 500 Internal Server Error.	MiCollab Client Service is unable to communicate with MX-ONE due to some 5xx response code from MX-ONE.	Check with the MX-ONE administrator to verify and solve the problem.
class="- topic/p ">Server error during call history credentials authentication: <error message>	MiCollab Client Service is unable to communicate with MX-ONE due to an error code.	Contact the MX-One administrator with the error message.

Below are the possible failure scenarios after the **Centralized Call History** feature is enabled on the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
MiCollab Client Service subscribes to MX-ONE for the Call History events for all the users. **Note**: The subscription request is sent in below three instances,	Subscription to MX-ONE failed for one or more DN's due to the 4xx or 5xx response code. **Note**: The user DN for which subscription failed shall not be able to view the	Carry out the appropriate steps according to the response code: **a.** For the 401 or 403 response code, check and correct the **Username**and (or) **Password**field of the **Client Log Settings** tab on the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
• immediately after the Call History feature is enabled on the MiCollab Server,		

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
• after the restart of the MiCollab Client Service,		**b.** For the 408 (or request timeout) response code, check and correct the network connection between MiCollab and MX-ONE.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
• and periodically after every 12 hours upon expiration of the subscription.	latest Call History logs from MX-ONE.	c. For any other 4xx response code, check the problem with the DN and take necessary action to correct its configuration on MX-ONE. d. For any other 5xx response code, check and confirm that MX-ONE and all its services are up and running. After taking the above remediation steps, try again by either disabling and enabling the feature or by restarting the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
After the MX-ONE user completes any incoming, outgoing, or missed call, the MiCollab Client Service requests MX-ONE for the latest Call History records.	The request sent by the MiCollab Client Service to MX-ONE fails due to any other error response code. **Note**: Corresponding Call History entry will not be visible on MiCollab Clients.	Carry out the appropriate steps according to the response code: **a.** For the 401 or 403 response code, check and correct the **Username**and (or) **Password**field of the **Client Log Settings** tab on the MiCollab Client Service Admin Portal. **b.** For the 408 (or request timeout) response code, check and correct the network connection between MiCollab and MX-ONE. **c.** For any other 4xx response code, check the problem with the DN and take necessary action to correct its configuration on MX-ONE. **d.** For any other 5xx response code, check and confirm that MX-ONE and all its services are up and running. After taking the above remediation steps, try again by either disabling and enabling the feature or by restarting the MiCollab Client Service Admin Portal.
After the MX-ONE user completes any incoming, outgoing, or missed call, MX-ONE sends a Call History event to the MiCollab Client Service.	MiCollab Client Service did not receive the event sent by MX-ONE, due to which the corresponding Call History record is not visible on MiCollab Client.	To retrieve the unlisted Call History entries, either restart the MiCollab Client Service from the admin portal Or Try to disable **and** enable the feature again from the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
MiCollab Client end user deletes single, multiple, or all Call History entries from any MiCollab Client.	The request for deletion sent from MiCollab Client Service to MX-ONE fails, due to which the MiCollab Client end user will not be able to delete the Call History entries. **Note**: An appropriate error message is displayed on the MiCollab Client UI.	Carry out the appropriate steps according to the response code: **a.** For the 401 or 403 response code, check and correct the **Username**and (or) **Password**field of the **Client Log Settings** tab on the MiCollab Client Service Admin Portal. **b.** For the 408 (or request timeout) response code, check and correct the network connection between MiCollab and MX-ONE. **c.** For any other 4xx response code, check the problem with the DN and take necessary action to correct its configuration on MX-ONE. **d.** For any other 5xx response code, check and confirm that MX-ONE and all its services are up and running. After taking the above remediation steps, try again by either disabling and enabling the feature or by restarting the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
MiCollab Client end-user attempts to delete some Call History entries of MX-ONE while the admin has disabled the **Centralized Call History** feature in the MiCollab Client Service.	Cannot delete the MX-ONE Call History entries if the **Centralized Call History** feature is disabled. **Note**: Displays **Unable to remove Call History Records** on the MiCollab Client UI.	NONE - This is a known limitation.
The MiCollab Client Service is down, during which any MX-ONE user configured on MiCollab completes a call (incoming, outgoing, or missed) using a desk phone.	As a result, both the MiCollab Client Service and the MiCollab Client will not update the Call History entry for this MX-ONE call made by the user during the downtime.	During the startup of the MiCollab Client Service, the MiCollab Client Server fetches all the missed Call History entries for all users from the last updated date or time. If the Call history entries for the latest date or time for any DN are unavailable, the Server will retrieve Call History entries for the past 24 hours.

For all the failure scenarios described above, a Warning Alarm will be triggered, providing the details of the DN, error response code, and error message in the MiCollab Client Service Admin Portal.

Note:

In the MiCollab Client Service Admin Portal, the admin will be able to view the alarms (like Major, Critical, and Clean) based on the type of error. Go to the **Event log** page to view the relevant error details.

From a MiCollab Client end-user perspective, there will be no perceptible change in the MiCollab Client Call History tab. When you enable the MX-ONE call history feature, the Client will seamlessly work as earlier.

MiCollab for Mobile Client settings

To enable Call Through functionality in MiCollab for Mobile Client:

a. In MiCollab for Mobile Client, go to **Settings** > **General**.
b. Select **My Numbers** and tap **Mobile** or **Remote Extension** if configured.

- For **Mobile**, tap **Call Through** to enable the setting.
- For **Remote Extension**, tap **Call Through** and select the configured mobile number from the prompt to enable the setting.

c. Tap **Save**.

Note:
For more information on Call Through feature for end-users, refer to *MiCollab for Mobile Client Quick Reference Guide* > *Call Through* section.

8. For MiVoice MX-ONE only: Configure the **MX-ONE Status Settings** for the selected PBX node.

- Select the **Disable MX-ONE Statuses** check box to disable the additional MX-ONE statuses and diversion profile integration for all users in the selected PBX node. The default status **In the Office** will be selected for all users having an additional MX-ONE status.
- Clear the **Disable MX-ONE Statuses** check box to enable the additional MX-ONE Statuses and diversion profile integration for all users in the selected PBX node.

Note:
A confirmation is displayed after the settings are saved or created. Click **Ok** to apply the settings.

Click **Refresh** to view the current status of the operation:

- NONE
- FAILED
- SUCCESS
- Enabling In Progress
- Disabling In Progress

9. Do one of the following:

- Click **Create** to create the PBX node.
- Click **Save** to save the updated information for the PBX node.
- Click **Cancel** to return to the PBX Node tab without making changes.

You are returned to the PBX Nodes tab.

After you add a PBX node, configure the PBX node synchronizer, and perform a synchronization, you can view read-only synchronization details for the last synchronization completed.

To view synchronization details

Click **Synchronization Details** to expand the page. The details displayed include:

- Start Time
- Stop Time
- Status
- Details

To add System CLI Number

System CLI Number

Note:
This setting is applicable only for MiVoice Business Communication Platform. The system CLI number requires MiVoice Business version 10.0.1.18 or higher to operate.

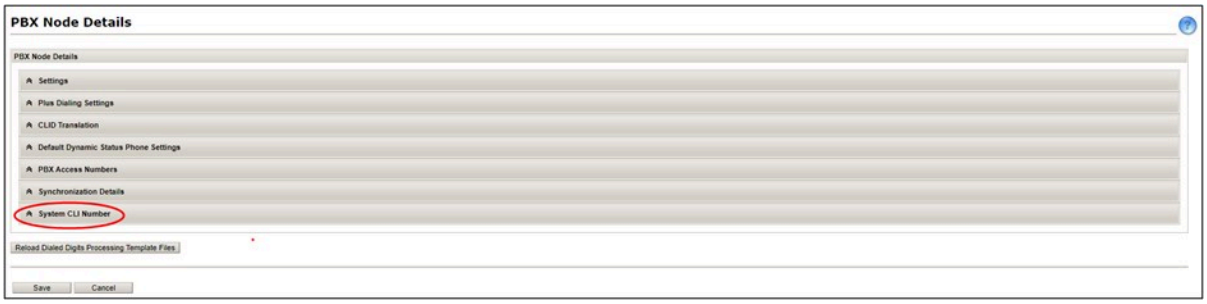
Note:
System CLI Number is applicable for calls made to external numbers only (for Softphone and Desktop calls). This feature is not applicable for internal calls.

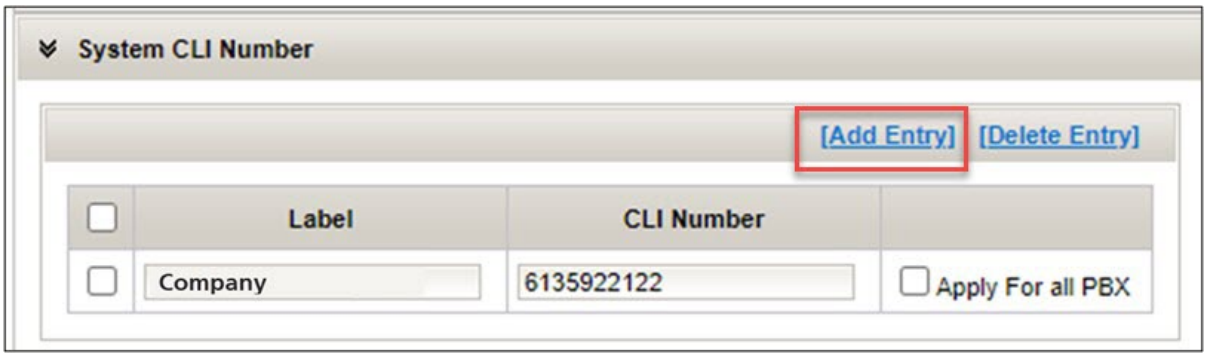
System Calling Line Identification (CLI) Number feature enables the caller to select which phone number must be displayed to the called party. The caller can select the preferred number from the**Settings > Manage Status > Edit status** > **Show my outgoing number** dropdown menu in the MiCollab client. For each Dynamic Status, the users will have the option to select the preferred CLI Number for outgoing calls.

The administrator configures the CLI Numbers for users, that the MiCollab Client user can select to be displayed on External party phones when in a call. The selected CLI Number will be displayed during outgoing CTI and Call Through (FMC) calls.

To configure the CLI Number in MiCollab:

1. Go to **MiCollab Client Service** > **PBX Nodes** and select the node to be used.
2. Under **System CLI Number**, click **Add Entry.**





Note:

If the **Apply For all PBX** checkbox is checked, the CLI number will be applied to all PBXs listed under the PBX tab.

3. Enter the CLI Number in the **CLI Number** and a name to the **Label**text box.
4. Click **Save**.

To delete a CLI Number, select the number and click **Delete Entry**.

Note:
If a CLI Number is applied to all PBXs and the administrator deletes the CLI Number entry, the number will be automatically removed in all PBXs.

Note:
Privacy numbers cannot be used as CLI number. This is a limitation on MiVoice Business Communication Platform.

Note:
The Ring groups, Hunt Groups, Personal Ring Groups, and Multi Device User Groups having an associated DID number will be added automatically in CLI Number list on performing PBX sync.

Note:
Non-DID numbers MUST NOT be used as a CLI Number.

ONS Feature Settings

One Number Service feature will be disabled by default on MiCollab 9.2 server. To enable the feature, the administrator must clear the **Pre 7.3 MX-ONE** option.

Reload Dialed Digits Processing Template Files

Once the dialed digit processing files are modified, clicking the **Reload Dialed Digits Processing Template Files** button reloads the files into the MiCollab Client system. This will update the processing logic for all PBXs across all enterprises on that MiCollab Client Service .

Note:
The dialed digits processing logic should not be modified unless instructed to do so by Mitel support personnel. Since this affects the very way numbers are dialed from MiCollab Client , incorrect processing may render useless large parts of the system.

26.20.1 Accounts Tab

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab Integrated mode.

The Accounts tab provides a table that lists all of the MiCollab Client accounts for each Enterprise.

Select the Enterprise from the list box and the following information is displayed for each account configured:

- **Type**: There are two types of accounts as indicated by the accounts icons:
- *Synchronized accounts*  : These accounts are created automatically during synchronizations between the MiCollab Client accounts database and the AD/LDAP directory *or* PBX node database.
- *Manually-created accounts*  : These accounts are created manually using the add or copy functions (see below).

- **PRG**: **Yes** indicates that the account has a Personal Ring Group (PRG) configured on the PBX. **No** indicates the account does not have a PRG.

Note:
For MiVoice Business 5.0 and later only, this field also enables Multi-Device User Groups. Note that with MDUG, once a user is busy in a call, any attempt by that user to originate a new call from another device within the MDUG group, using the MiCollab Client OR physically going off-hook from that device, results in a call failed indication.

- **Active:** Indicates if the account is active. This column is only shown if there is at least one account that is not active. Inactive accounts indicate that the account is not properly licensed.
- **Last Name**: Indicates the user's last name.
- **First Name:** Indicates the user's first name.
- **Desk Phone**: Indicates the extension for the user's desk phone.
- **Soft Phone**: Indicates the extension for the user's UC Advanced softphone.

Mitel Phone Model	MiVoice Business PBX	MiVoice Office 250 PBX
5020 IP Phone	yes	no
AppServerPort	yes	no
5224 IP Phone	no	yes

Note:
Provision the 3300 with 5020 IP device type for resilient MiCollab Client softphones.

Note:

SIP Softphone connected to MiVoice Business PBX must be configured as:

- Device Type = MiCollab Client Endpoint
- Key with Line Type = Multicall
- Button Dir. Number matching the number of the device
- Ring Type = Ring.

Note:
If a user is configured as a Basic MiCollab Desktop Client user, Mitel recommends configuring one desk phone or one desk phone and EHDU device.

- **PBX Node**: Indicates the IP address for the PBX node server.

Note:
If the PBX Node column is blank, the account is considered to be in Teamwork mode and not associated with any PBX node.

You can complete the following tasks for accounts:

- Search for an account.

  The search function is not case sensitive and it is a "contains" type search versus a "starts with" type search. For example, if you search using the search string "br", the search will return all of the accounts that include "br" in either the first or last name.

  Searched fields include:

  - First Name
  - Last Name
  - Desk Phone
  - Softphone

  To search for an account:

  1. Type a search string in the Search text box. You can search accounts using:
     - Alphabetical characters: Type a name, a group of letters, or a single letter in the Search box.
     - Numeric characters: Type a full extension, a group of numbers, or a single number in the Search box.
  2. Click **Search**. The list of account names matching the search string is displayed.

  To clear the Search box, click Clear.
- Click Add Account to add a new account.
- Delete an account. **To delete an account:**

  1. Select the account you want to delete from the account list.
  2. Click the **Delete Account** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the account, or click **Cancel** to cancel the deletion.

- Send a welcome e-mail.

  Welcome e-mail messages provide the user with the following information and links:

  - MiCollab Client Login ID and Password (required to log in to MiCollab Client user interfaces)
  - Desk phone extension
  - Softphone extension
  - MiCollab End User Portal URL (provides access to the End User Portal)
  - MiCollab for PC Client (*micollab_pc.msi*) download URL, if MiCollab for PC Client is configured for the user
  - MiVoice for Skype for Business (*mivoice_sfb.msi*) download URL
  - MiCollab MAC Desktop Client download URL
  - MiCollab Mobile Client (iOS and Android) download URL
  - MiCollab Web Client download URL
  - MiCollab Client Quick Reference Guide URL (provides basic MiCollab Client installation and feature usage information)
  - Legacy Skype for Business Client (*MitelMiVoiceForLync.msi*) download URL
  - Local Android Client (*MitelUCAdvanced.apk*) download URL

  Before you send a welcome e-mail to the user, make sure you have programmed an e-mail address for the user's account in the **Contact Information** section of the Account Details page.

  To send a welcome e-mail:

  1. Select the account or accounts from the account list.
  2. Click the **Send Welcome E-mail** link. A dialog box appears prompting you to confirm the action.
  3. Click **OK** to send the e-mail message, or click **Cancel** to cancel.
- Sort the information in the table.
- Select one or more entries in the table.
- Activate an inactive account.

  To activate an account:

  1. Select the account you want to activate from the account list.
  2. Click the **Activate** link. A dialog box appears prompting you to confirm the activation.
  3. Click **OK** to activate the account, or click **Cancel** to cancel the activation.
- Click the First/Last Name link to edit account information.

- Click the copy icon  to quickly create a new account based on the values configured for the associated account.

  To copy account fields and create a new account:

  1. Select the account you want to copy and click the copy icon  . The Account Details page opens and the non-user-specific fields are populated with the values from the copied account.
  2. If required, edit the following pre-populated fields:
     - PBX node
     - Voice mail number
     - Language
     - Country
     - Feature Profile
  3. Complete the remaining user-specific account fields:
     - First name
     - Middle name
     - Last name
     - Login ID
     - Password
     - Desk phone
     - Soft phone
     - Mailbox number
  4. Click **Create**.
- Refresh the information on the page.

Note:
When adding an account manually the PBX node must be set to 'None' for account to be in Teamwork mode.

When using Active directory sync, the PBX node value in active directory should be set to <enterpriseId>.local and no deskphone or softphone number must be assigned to the user account in active directory.

26.201.1 About Login IDs

MiCollab Client credentials are communicated to the user via a Welcome E-mail Message that you can generate for each user after you provision the system.

MiCollab Client credentials include:

- Fully Qualified Domain Name (FQDN) for the MiCollab Client Service (required for the Desktop Client installation)

- MiCollab Client Login ID (simple, or fully qualified Login ID – used to log in to the MiCollab Client user interfaces)
- MiCollab Client Password (used to log in to the MiCollab Client user interfaces)

You can also log in to the MiCollab client using the UPN. The *UserPrincipalName* (UPN) attribute must be in the internet-style sign-in format where the username is followed by the @ sign and a domain name.

Note:
The UPN login is supported only in the integrated mode.

Note:
The presence of the peered users with the login ID as UPN will be seen only when both the peered servers are on MiCollab version 9.4 and above.

The value entered for the **Login ID** field on the Account Details page provides the simple Login ID for the user. If you are managing a single Enterprise deployment, users are provided with a simple Login ID (for example, john_smith) via the Welcome E-mail Message.

The Login ID:

- must be unique.
- supports ISO8859-1 characters.
- can be between 2 and 113 alphanumeric characters in length.
- can be numeric, but should not conflict with any other user's DN. The user can use his own DN as a Login ID.

The UPN login specifications are as follows:

- The userPrincipalName (UPN) attribute must be in the internet-style sign-in format where the user name is followed by the @ symbol and a domain name. For example, username@abc.com.
- The maximum number of characters for the UPN attribute is **113**. A specific number of characters are permitted before and after the @ symbol; the specifications are as follows:
  - maximum number of characters for the username, that is the characters before the @ symbol should not be more than 64
  - maximum number of characters for the domain name following the @ symbol should not be more than 48
  - the @ symbol is required in each userPrincipalName value
  - the @ symbol cannot be the first character in each userPrincipalName value
  - the username cannot end with a period (.), an ampersand (&), a space, or with the @ symbol
  - the username should not have spaces
  - routable domains must be used; for example, local or internal domains cannot be used
  - unicode is converted to underscore characters
  - userPrincipalName cannot contain any duplicate values in the directory

Note:

MiCollab does not support the @ character as the first or last character in the UPN value.

26.201.2 Adding and Editing Accounts

The **Account Details** page provides fields and options for creating and configuring an account. At a minimum, you must configure the **Login Settings** and **Licensed Features** sections of the **Account Details** page, when you create an account.

Then at a later time, you can edit the account information and provide additional details for the account.

Note:
Some configuration settings do not apply to MiCollab Client Stand-alone Web Client users (see table for details).

In addition, chat history is managed on this page.

Creating an account

To create an account, do the following:

1. Configure the account details on the **Create Account Details (Login Settings)** page.

   - **First name**: Type the first name for the account holder.
   - **Middle name**: Type the middle name for the account holder.
   - **Last name**: (*Required*) Type the last name for the account holder.
   - **Login ID** (case insensitive): (*Required*) Type the login ID that the account holder will use to log in to the Desktop Client (for example, <*first name_last name*>). You can use upper or lower case letters in this field.
   - **Password**: (*Required*) Type the password that the account holder will use to log in to the Desktop Client.
   - **PBX node**: (*Required*) Select the PBX node that provides phone service to the account holder. Select [**None**] if the account is in Teamwork Mode and not associated with any PBX node.

Note:
A Teamwork Mode account that is not associated with any PBX node can later be associated with a PBX node when the account is assigned a phone on a PBX. However, an account that is associated with a PBX node cannot be moved back to Teamwork Mode.

- **Mailbox number**: Type the extension number for the account holder's mailbox.
- **Voice mail server**: (*Optional*) This field can be used to override the **Voice mail server** field configured on the PBX Node Details page for the PBX node associated with an account. This field can contain a maximum of 128 characters, and must include a valid IP address or host name. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default.
- **Voice mail public number**: (*Optional*) This field can be used to override the **Voice mail public number** field configured on the PBX Node Details page for the PBX node associated with this account. This field can contain a maximum of 32 characters. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default.
- **Language**: (*Optional*) Select a language from the list if you want to override the Enterprise and PBX language settings for this account. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. The user's language setting determines the language in which the Welcome E-mail Message is generated for that user.
- **Country**: Select the country that the account holder resides in.
- **Refresh line monitors on save**: (MiVoice Business only) If the primary MiVoice Business was not running when MiCollab Client started, the MiTAI monitors for non-resilient devices are not set. Select this option to restart the MiTAI monitors and receive updated line configuration from MiVoice Business.
- **Reset dynamic statuses on save**: If there are PRG/MDUG provisioning changes, including the addition or deletion of phones from PRG/MDUG for the dynamic status to be created. Select this option to recreate dynamic statuses for this account.

  - A status reset removes all custom statuses and custom routing rules created by the end-user.
  - The account language setting determines the language in which the new statuses are created by the system.
  - Users need to log in back to MiCollab Client after dynamic statuses have been reset.
- **Presence Privacy Configuration Settings**: This setting controls whether a user's presence information (dynamic status, telephony status, video availability, and calendar advisory) is displayed to other users or not.

  Show Presence for User: This setting is available only if **Presence Privacy Service** is **Enabled** at the Enterprise level. By default, the **Show Presence for User** setting is enabled.

  - If the above setting is enabled, the presence information of the user is displayed to all users on local and peered servers.
  - If the above setting is disabled, the presence information of the user is displayed only to those users on local and peered servers who are in the presence allowed list of the user.

Note:
For this option, the setting specified at the Account level overrides the setting specified at the Enterprise level.

Limitations:

- **Presence Privacy Service** is not supported in co-located mode.
- On peered servers, the Presence Privacy setting at the local server will override that at the peered server.
- Telephony presence status of other users does not turn off immediately. To turn it off, the user must log out from the client and then log in again. When the user logs in again in to the client, the telephony presence status of other users from corporate directory, call history, search tab, and from legacy console is turned off.
- Video call functionality does not work for users for whom presence privacy setting is enabled.
- In the MiCollab peered server setup, if one of the server is at a version earlier than MiCollab 9.0, users on that server will see the presence information of all users on all the peered servers irrespective of whether the presence feature is enabled or disabled on the other servers.
- If MiVoice Business Controller is earlier than 9.0 and InAttend servers have SIP-based subscription, enabling the presence privacy setting will not impact the dynamic status and the telephony presence (presence status will not change to **status unknown**).

2. Configure the Licensed Features by selecting a feature profile to assign to the account. The following information is displayed for the Feature profile:

   - **Profile features**: A read-only list of features included in the selected profile.
   - **Add-on features**: The list of features available to select from that are *not* included in the selected profile.

   To add/remove features to an account:

   a. Select/deselect the features from the **Add-on features** list.
   b. Click **Save**.

3. Click **Create**. You are returned to the **Accounts** tab.

To complete the account configuration, click the account name from the Accounts tab, and edit the account information.

Note:
If you are creating a Teamwork Mode account through AD/LDAP synchronization, fill out all fields in the active directory as you would for a regular account except for the following:

- Set PBX node value to <enterpriseId>.local, where <enterpriseId> is the ID of the enterprise being created and can be found on **Enterprise** tab.
- Do not fill out fields for desk phone and softphone.

Editing an account

To edit an account, do the following:

1. Edit the account details **(Login Settings).**

- **First name**: Edit the first name of the account holder.
- **Middle name**: Edit the middle name of the account holder.
- **Last name**: (*Required*) Edit the last name of the account holder.
- **Login ID**: (*Required*) Edit the login ID that the account holder will use to log in to the Desktop Client (for example, <*first name_last name*>). You can use upper or lower case for this field.
- **Password**: (*Required*) Type the password that the account holder will use to log in to the desktop client.
- **Reset Password on Save**: Select this option to reset the account password to a random value. When you click **Save**, an e-mail message providing the new password is sent to the user. Make sure you have programmed an e-mail address for the account under the **Contact Information** section of this page. If the account does not have a programmed e-mail address, an error message is generated and the option is cleared.
- **PBX node**: (*Required*) Change the selected PBX node to edit the settings.
- **Primary Extension**: (*Required only for Priority Ring Group PBX synch only*) Type the primary extension for the account holder. Select the type of device of this primary extension (from drop-down menu select Deskphone, Softphone or SIP).
- **Mailbox number**: Type the extension for the account holder's mailbox extension.
- **Voice mail server**: (*Optional*) This field can be used to override the Voice mail server field configured on the PBX Node Details page for the PBX node associated with this account. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default. The maximum length is 128 characters, and must include a valid IP address or host name.
- **Voice mail public number**: (*Optional*) This field can be used to override the Voice mail public number field configured on the PBX Node Details page for the PBX node associated with this account. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default. The maximum length is 32 characters.
- **Country**: Select the country that the account holder resides in.
- **Allow user to upload display photo**: Select this option if you want to allow the user to upload and save a photo to the MiCollab Client Service. When the photo is uploaded to the server, it is displayed

on this page along with the user's other account information. The user's photo is then displayed in the MiCollab Desktop and Web clients.

- **Upload new photo**: You can also upload a photo of the user to the server if you have one available. Uploaded photos must adhere to the standard guidelines.

Standard guidelines to upload a photo:

- Supported photo file types are .jpg, .png, and .gif.
- The maximum file size for photos is 25600 bytes.
- The administrator's interface does not allow you to crop photos.
- All uploaded photos will be resized to 128 x 128 pixels.

To upload a photo:

a. Click **Upload New Photo**.
b. Browse to the photo location.
c. Select the photo and click **Open**.
d. Click **Upload**. The photo is uploaded to the page.

To cancel the upload, click **Cancel New Photo**.

Note:
Do not update the AWV password from the **MiCollab Client Service Configuration Account** tab when MiCollab is in integrated mode because doing so might cause authentication issues while you use MiTeam Classic features.

2. Edit the Licensed Features for the account.

a. Select a Feature profile to assign to the account.

The following information is displayed for the Feature profile:

- **Profile features**: A read-only list of features included in the selected profile.
- **Add-on features**: The list of features available to select from that are *not* included in the selected profile.

b. To add/remove features to an account:

i. Select/deselect the features from the **Add-on features** list.
ii. Click **Save**.

Note:
Both Web Portal features are set automatically when you select either one of them.

3. Edit the Phone Numbers for the account.

   a. Select **Add** to create a new device.

   The following information is displayed for adding a new device:

   - **Type**: The type can be **Desk Phone**, **MiNet Softphone**, **SIP Softphone**, **Phone**, **PRG**, **Voice Mail**, or **DID**.
     - **Phone**: Includes other devices programmed for the account. You can edit the **Label** and **Number** for these types of phone numbers.

       Note:
       By default, phone numbers are published to the Corporate Contacts list. Clear the **Published** option if you want the phone numbers to remain unpublished.

     - **PRG**: Includes Personal Ring Group (PRG) extensions programmed on the PBX. You can edit the **Label** only for these types of phone numbers.
     - **DID**: Includes the Direct Inward Dialing (DID) number configured for the user on MiVoice Business. You can edit the **Label** and **Number** for these types of phone numbers.
   - **Label**: Enter a label for each device created.
   - **Number**: Enter an extension number for each device created.
   - **Published**: The option to publish phone numbers.
     - On the MiVoice 5000 communication platform, if the **Published** option is not selected, the phone number of the user will be obfuscated. The Client also obfuscates the number in the **Call History** and **Voicemail** menu for the called party. The called party will not be able to call back or copy the obfuscated number.
     - If **Privacy Flag** is set to **On** in MiVoice Business communication platform and the **Published** option is not selected in MiCollab, then the number will not be visible in MiCollab incoming

calls, Search results, Call History, Contacts menu, contact card, activity tab, voicemail history, and notifications. Following are the limitations:

- If an unpublished number was previously recorded in the call logs before the feature was enabled, then the menus, **Search**, **Call History**, **Voicemail History**, **Contact Card (hover-over)**, and **Activity** will display the number.
- In the incoming call window, the **Decline with a chat** option will not be shown for the user with private DN.
- If the user publish/unpublish the number using their MiCollab Client, then the privacy feature is terminated and the number will be visible in the corporate directory and contact card.
- Contacts from the peered servers are automatically synchronized after an interval of 6 hours. For an immediate synchronization, users must restart their MiCollab Client manually.
- For voicemail with privacy DN, only the name of the party who sent the voicemail is displayed; chat functionality will be disabled. This feature is compatible with MiCollab Client Version 9.3 and earlier and with MiCollab 9.3 server and Privacy DN **ON**. Restart the MiCollab Client to see the changes.

- **Video Capable**: The option to indicate whether the SIP softphone is video capable.

Note:
On other communication platforms, the phone number will not appear in the contact card, but incoming calls, call history, and voicemail history will display the number.

Note:
Publishing MDUG non-prime numbers is not supported in MiCollab. Use PRG to publish non-prime numbers.

b. Select **Create**. When adding a MiNet softphone, a random, a unique MAC address is created and appears here. If MiCollab Client is in co-located mode, the field can be edited. If MiCollab Client is in integrated mode, the field is read-only.
c. To delete a device, select the device and click **Delete**.
d. To edit a device, select the device and click **Edit** beside the device.
e. When switching from SIP softphone to MiNet softphone, perform the following procedure to register the MiNet Softphone:

i. Delete the user name folder in "`C:\Users\\AppData\Roaming\Mitel\UC\`".

CAUTION:
Deleting the application folder will also remove all the existing settings for the user.

ii. Re-launch the Legacy MiCollab Desktop Client application.

iii. Switch from SIP softphone to MiNet softphone.

4. Configure the account **Contact Information**.

- **Company name**: Type the account holder's company name.
- **Address**: Type the street address for the company.
- **City**: Type the city where the company is located.
- **State/Province**: Type the state where the company is located.
- **ZIP/Postal code**: Type the zip code where the company is located.
- Add, Edit, and Delete the following for the account:
  - Phone Numbers
  - E-mail addresses
  - IM addresses

5. **Configure the Account Settings**

The **Account Settings** area on the Account Details page allows you to overwrite the Default Account settings (configured on the Enterprise Tab) for the specified account. *If necessary*, configure the following settings for the account:

- **Phone Settings**: Configure the following for the account holder's phone:
  - *Account code length*: Select the number of digits for account codes from the range 0-12. The default is 0.
  - *Auto Upgrade Client*: This option offers control over automatic client upgrades.
    - Select **Default** to retrieve the client upgrade information from the Enterprise setting. By default, this option is enabled.
    - Select **Enable** to push the automatic client upgrade (if there is a new version of the client available) for the user. The user will trigger a client upgrade pop-up notification.
    - Select **Disable** to disable the client upgrade for the selected user.
  - *Enable ACD features in client*: Select this option if you want the account holder to have access to the ACD view and corresponding features in the Desktop Client.
- **RSS Window**: Configure the following for the account holder's RSS window:
  - *URL*: Type the URL of the RSS Web page that you want to appear in the account holder's RSS window on the desktop client. For example, **http://www.mitel.com/RSSNewsRelease**. RSS feeds are formatted by a script on the Unified Communications server that provides an HTML scrolling interface to the user.
  - *Always On*: Select this option for the RSS window to be always visible in the account holder's Desktop Client.
  - *User Modifiable*: Select this option to enable users to modify the URL from the Desktop Client.
- **Collaboration**: Configure the following collaboration settings for the account holder:
  - *Username*: Type the user name that the account holder uses to log in to the collaboration Web interface.

Note:
Set the user name to be the MiCollab Audio, Web and Video Conferencing e-mail address.

- *Password*: Type the password that the account holder uses to log in to the collaboration Web interface.
- *Collaboration server*: Select the account holder's collaboration server, or select Default to use the collaboration sever configured for the Enterprise.

- **Mobile Settings**: Optionally, enable the **User can manage MiCollab corporate locations** option. Users for whom this option is enabled can manage Corporate Locations from their MiCollab Mobile Client and upload the information to the MiCollab Client Service. By default, this option is disabled.
- **Client Upgrade Settings**: Select the **Do not provision new MiCollab Client for PC** option to disable provisioning MiCollab for PC for the selected user.

Note:
Use this option in case of mixed deployment of MiCollab Clients (Desktop Client and MiCollab for PC for different users).

Note:
If the **Provision new MiCollab for PC** option under the **Enterprise** tab is disabled, then **Client Upgrade Settings** cannot be used to modify the default settings.

- **Group Presence Control Settings**: By default, the **Users can manage group presence** check box is not selected; select the check box to enable the settings that allow MiCollab Client users to update their group presence and retrieve the group list.

Note:
Support for group presence control is limited to MiVoice Business, MiVoice 5000, and MX-One PBXs. If you enable group presence control for other PBX types, you will receive the following error message:

Group presence control setting can't be enabled. It is supported with MiVoice Business, MiVoice 5000 and MX-ONE PBX only.

MiVoice Business

In MiVoice Business, both Ring Groups and Hunt Groups are supported. A user can be a part of multiple Ring Groups and Hunt Groups and this information is visible in their MiCollab Clients.

The administrator must configure a Ring/Hunt Group in MiVoice Business and add the user's DN (Directory Number) as a Ring/Hunt Group member. After synchronization between MiVoice Business and MiCollab Client Service, the **Ring Groups** menu will be displayed in the navigation pane of MiCollab Client under which both the Ring and Hunt Group details are also displayed.

Note:
After configuration, the administrator must select the **Users can manage group presence** check box under **Group Presence Control Settings**. Refer to Group Presence Control Settings section.

MiCollab Client users can mark themselves as present or absent (logged in/logged out) with regard to a Ring/Hunt Group by clicking the toggle switch corresponding to that Group or by clicking the global toggle switch to indicate their status as logged in/logged out from all Ring/Hunt Groups.

Note:
The **Group Presence Control COS** option must be enabled for extensions on MiVoice Business for the Group Presence feature to work.

MiVoice 5000

In MiVoice 5000, only Hunt Group is supported and each user can be a part of only one Hunt Group.

The administrator must configure a Hunt Group in MiVoice 5000 and add the user's DN as a Hunt Group member. After synchronization between MiVoice 5000 and MiCollab Client Service, the **Hunt Group** menu will be displayed in the navigation pane of MiCollab Client. In the Hunt Group menu, the configured Hunt Group will be displayed as **Enable Hunt Group**.

Note:
After configuration, the administrator must select the **Users can manage group presence** check box under **Group Presence Control Settings**. Refer to Group Presence Control Settings section.

MiCollab Client users can mark themselves as present or absent (log in/log out) in the Hunt Group. If the administrator has not selected the **Users can manage group presence** check box, the Hunt Group menu will be removed from the navigation pane of MiCollab Client.

Note:
In MiVoice 5000, when a user is added or removed from a Hunt Group, MiCollab Client does not receive any notification from MiVoice 5000. The user must log in to MiCollab Client again to get the latest group information.

MX-One

In MX-One, only Hunt Groups are supported and each user can be a part of a maximum of four Hunt Groups. This information is visible in their MiCollab Clients.

Note:
The log in/log out from Hunt Groups feature is supported from MX-One 7.5 version.

The administrator must configure a Hunt Group in MX-One and add the user's DN as a Hunt Group member. After the user logs in, the Hunt Group menu will be displayed in the navigation pane of MiCollab Client.

Note:
After configuration, the administrator must select the **Users can manage group presence** check box under **Group Presence Control Settings**. Refer to Group Presence Control Settings section.

MiCollab Client users can mark themselves as present or absent (logged in/logged out) of the Hunt Group. If the administrator has not selected the **Users can manage group presence** check box, the Hunt Group menu will be removed from the navigation pane of MiCollab Client.

Note:
In MX-One, when a user is added or removed from a Hunt Group, then the user on MiCollab Client will receive the latest group information in real time.

- **USB Devices**: Configure the following USB device options:
  - *User can configure local USB devices*: Selecting this option allows account holders to configure USB devices on their computer using MiCollab Desktop Client.
  - *User can manage USB device profiles*: Selecting this option enables account holders to manage (upload, edit, and delete) USB device profiles on the Unified Communications server from MiCollab Desktop Client. Mitel recommends that you enable this option for a limited number of users (1-2) on the system.

    Note:
    Enabling this option automatically enables the **User can configure local USB devices** option.

6. Click **Save** to save the account information.

Note:
Accounts synchronized with the PBX: After you complete phone extension configuration changes (add, delete, move, or change) on the PBX, perform a manual synchronization (**Sync Now** button on the Synchronization tab) to *immediately* update the affected MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization.

In addition, those MiCollab Client users whose extensions are affected by the configuration changes you make on the PBX must exit and then restart their MiCollab Desktop Clients to refresh extension information.

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab-integrated mode.

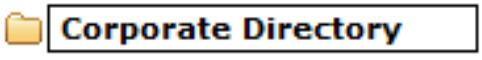
MiVoice Conference/Video Phone devices must be set to *video enabled* to allow video calls. See MiVoice Conference/Video Phone device for further details.

26.202 Corporate Directory Tab

The Corporate Directory tab provides a list of all the accounts for each corporate directory. When an account is included in the corporate directory, the user is listed as a corporate contact in the MiCollab Client Desktop Client Contacts view.

The directory structure for corporate directories varies based on how the corporate directory was generated.

Corporate directories generated from a PBX synchronization, or by manually creating the accounts include just one top level Corporate Directory folder .



All accounts are displayed in the Corporate Directory table, and there are no subfolders under the top-level Corporate Directory folder.

Corporate directories generated from an AD/LDAP synchronization typically include various organization groups and associated folders .

Subfolders, and the accounts that reside in them, correspond to the Organization Units present in the AD/LDAP Corporate Directory. If a folder is collapsed, you can expand it by doing one of the following:

- Click the arrow next to the folder.
- Click the name of the folder.
- Click the **Expand All** link.

If a folder is expanded, you can collapse it by doing one of the following:

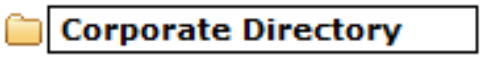
- Click the arrow next to the folder.
- Click the **Collapse All** link.

The corporate directory table provides the following information for the accounts in the directory:

- **Type**: There are two types of accounts as indicated by the accounts icons:
- *Synchronized accounts*: These accounts are created automatically during synchronizations between the MiCollab Client accounts database and the AD/LDAP directory *or* PBX node database.
- *Manually-created accounts*: These accounts are created manually using the add or copy functions.
- **Last Name**: Indicates the user's last name.
- **First Name:** Indicates the user's first name.
- **Desk Phone**: Indicates the extension for the user's desk phone.
- **Soft Phone**: Indicates the extension for the user's MiCollab Client softphone.

Local Corporate Directories

To see the list of accounts in the local corporate directory, click the top level **Corporate Directory** folder.



In some circumstances, you may not want to include all accounts as corporate contacts (for example, high-level company executives). You can remove individual accounts from the corporate directory, thereby removing the associated user from the list of MiCollab Client corporate contacts. Removing an account from the corporate directory group does not delete the account from the corporate directory. It merely removes the associated user from the list of corporate contacts in the MiCollab Client Desktop Client.

You can also **add** manually-created accounts to the corporate directory and include the associated users in the list of MiCollab Client corporate contacts.

For local corporate directories you can:

- **Sort** the information in the table.
- Select one or more entries in the table.
- **Refresh** the information on the page.
- Add accounts to the corporate directory.

- Remove accounts from the corporate directory.

  To remove one or more contacts from the corporate directory group:

  1. Select the contact you want to remove.
  2. Click the **Remove** link. A dialog box appears prompting you to confirm that you want to hide the contact from the corporate directory group.
  3. Click **OK** to remove the contact, or click **Cancel** to cancel the removal.

Peered Corporate Directories

To see the list of accounts for a peered server corporate directory, first expand the top-level Corporate Directory folder, and then click the sub-folder with the **Description** of the peered server (as configured on the Peer Server Details page).



When MiCollab Client Services are configured for peering, users are categorized by corporate directory in the MiCollab Client interfaces. Users between different corporate directories have equal access to presence information and communication features as they do with users from their own corporate directories. Users who have been removed from their corporate directory are not visible to other users.

For each peered server, the directory tree structure displayed under the local Corporate Directory folder mirrors the Corporate directory structure on the peer server itself. Because you do not have management access to peered corporate directories, the **Add** and **Remove** links will not appear when you click on a peered corporate directory folder.

For peered corporate directories you can:

- **Sort** the information in the table.
- **Refresh** the information on the page.

26.202.1 Adding Corporate Contacts

This page shows the list of accounts that are not currently included in the local MiCollab Client Service Enterprise's corporate directory group. When an account is not included in the corporate directory group, the associated user is not listed as a corporate contact in the MiCollab Client Desktop Client Contacts view.

You can add a synchronized account  or a manually-created account  to the local corporate directory group from this page.

Note:
You cannot add (or remove) accounts from a peered server corporate directory.

To add an account to the corporate directory group:

1. Select the account from the list.
2. Click **Add**. You are returned to the Corporate Directory tab, with the account added to the group.
3. Click **Cancel** to return to the Corporate Directory tab without adding accounts to the corporate directory group.

26.202.2 ACD Settings Tab

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

Automatic Call Distribution (ACD) is an optional feature for Enterprises using MiCollab Client. ACD is used by call centers to manage incoming calls to a single directory number. The calls are distributed among a group of logged in call center agents. When ACD is enabled for the agent, the Desktop Client provides an ACD view.

The ACD Settings tab includes fields and options used to configure ACD groups, account codes, and busy reasons. When an ACD agent starts his or her MiCollab Client , the MiCollab Client Service sends the ACD settings to the client and populates the ACD view.

Select the Enterprise from the list box and then configure the following areas for ACD settings.

ACD Groups (*MiVoice Business only*)

The MiVoice Business switch requires ACD agents to be included in ACD groups. The ACD Groups table contains the following column headings:

- **Group ID**: The Group ID should match the group ID of an ACD group configured on the MiVoice Business switch.
- **Switch IP**: The IP address of the MiVoice Business switch.
- **Agents**: The list of extensions included in the ACD group.

You can Add, Edit, or Delete ACD Groups.

In addition you can add and delete agent extensions to the groups.

To add agent extensions to the ACD group:

1. Click  . The ACD groups table expands to include an agent edit area.
2. Do one of the following:

   - To add a single extension, type the extension number in the first box and leave the second box blank.
   - To add a range of extensions, type the starting extension in the first box and the ending extension in the second box.
3. Click **Add**, and then click **Done**.

To delete agent extensions from the ACD group:

1. Click  . The ACD groups table expands to include an agent edit area.
2. Click  for the extension or range that you want to delete.
3. Click **Done**.

When you are finished configuring ACD Groups, click **Apply** to save the information, or click **Reset** to clear your changes.

Account Codes

To facilitate reporting, some call centers require account codes for ACD calls. At startup, account codes are sent to the desktop clients for the users (agents) who have been configured for the ACD feature. Agents can then apply the account code during the call from the Desktop Client's ACD view.

The Account Codes table contains the following column headings:

- **Code**: The numeric value for the account code (2-12 digits).
- **Label**: The description you provide for the account code.

You can Add, Edit, and Delete account codes.

When you are finished configuring Account Codes, click **Apply** to save the information, or click **Reset** to clear your changes.

Busy Reasons

The Busy Reasons section allows you to manage the ACD busy reasons provided by the switch. The number of busy reasons displayed is determined by the switch type (see table below).

The Busy Reasons table contains the following column headings:

- **Code**: The numeric value for the busy reason code.
- **Label**: The default description, (or description that you provide), for the busy reason code.

Code	MiVoice Business Default Label	MiVoice Office Default Label
0	No Reason	No Reason
1	At Lunch	At Lunch
2	Gone Home	Gone Home
3	Unavailable	Unavailable
4	Do-Not-Disturb	Do-Not-Disturb
5	In Meeting Until	In Meeting Until
6	On Vacation Until	On Vacation Until
7	Page Me	Page Me
8	Call Me At	Call Me At
9	Away from Desk	Away from Desk
10	Out of Town Until	Out of Town Until
11	Telecommuting	Telecommuting
12		Out Until
13		Leave Voice Mail
14		On Break
15		In Training

Code	MiVoice Business Default Label	MiVoice Office Default Label
16		Out of Office
17		Meeting Customer Until
18		Travelling
19		Off Site at

You cannot add or delete busy reason codes or labels. However, you can edit all of the busy reason labels except for the label for code 0 (No Reason). This busy reason code is predefined and cannot be changed.

When you are finished editing Busy Reason labels, click **Apply** to save the information, or click **Reset** to clear your changes.

26.203 Collaboration Tab

The Collaboration tab provides a table that lists all the collaboration servers that are configured for the Enterprise. Collaboration servers provide audio, video, web conferencing, and associated collaboration features to MiCollab Client users who are provisioned for the Collaboration Integration licensed feature.

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab -integrated mode.

Additional information about the MiCollab Audio, Web and Video Conferencing collaboration server:

The collaboration server is the central hub for all conference sessions. Audio and web conferences require a server where the conference sessions are hosted, and all conference information flows through the server before being distributed to the MiCollab Client Desktop Client.

Mitel supports the MiCollab Audio, Web and Video Conferencing product for collaboration features.

MiCollab Audio, Web and Video Conferencing provides an integrated application to create audio and Web conferences, create video calls, share documents and applications, chat, and use collaboration tools such as whiteboarding and annotation to share information between users in real time.

Like MiCollab Client , MiCollab Audio, Web and Video Conferencing is packaged on the MiCollab server, which is connected to the IP network. The MiCollab server provides access to a Web-based administrator interface for configuring MiCollab Audio, Web and Video Conferencing , scheduling conferences, viewing conference calls, and administering collaboration controls. You can access all interfaces through either HTTP or HTTPS.

Note:
MiCollab Client v5.0 requires MiCollab Audio, Web and Video Conferencing 4.0 or later running on MiCollab v4.0 or later.

Select the Enterprise from the list box and the following information is displayed for the Enterprise's collaboration servers:

- **Description**: The short description configured for the collaboration server.
- **URL**: The Web address for the collaboration server.

You can complete the following tasks for collaboration servers:

- Sort the information in the table.
- Select one or more entries in the table.
- Click the Add Server link to add a collaboration server.
- Click the collaboration server link in the **Description** column to edit the collaboration server.
- Delete collaboration servers.

Note:
To clean up your database you can delete previously-used UCX/YA Collaboration servers.

To delete a collaboration server:

1. Select the server you want to delete from the table.
2. Click the **Delete Server** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the server, or click **Cancel** to cancel the deletion.

- Refresh the information on the page.

26.203.1 Adding and Editing Collaboration Servers

On this page, you can add and edit information for the MiCollab Audio, Web and Video Conferencing collaboration servers you configure for the Enterprise.

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab -integrated mode.

To add or edit an MiCollab Audio, Web and Video Conferencing Collaboration server:

1. Type a **Description** (*Required*) for the MiCollab Audio, Web and Video Conferencing collaboration server. This field has a maximum length is 64 characters.
2. Type the **URL** (*Required*) for the MiCollab Audio, Web and Video Conferencing collaboration server. This field has a maximum length of 255 characters and must begin with " http://" or " https://."
3. Click **Sync Now**. The remaining fields are auto-populated by the collaboration server.

- **Dial-In phone number 1/2/3**: These fields have a maximum length of 32 digits (0-9), and correspond to the following fields as programmed on the MiCollab Audio, Web and Video Conferencing server:

  - The toll free number that user's can dial to join MiCollab Audio, Web and Video Conferencing audio conferences.
  - The public (non-toll free) number that user's can dial to join MiCollab Audio, Web and Video Conferencing audio conferences.
  - The extension number that user's can dial to join MiCollab Audio, Web and Video Conferencing audio conferences.
- Dial Out Allowed: When enabled under Default Account Settings in MiCollab Audio, Web and Video Conferencing , users can dial out to others using MiCollab Audio, Web and Video Conferencing (CO call). By default, this is enabled.

Note:
This option can also be enabled or disabled on a per-user basis in MiCollab Audio, Web and Video Conferencing.

- **Port Reservations Enabled**: When Port Reservations are enabled in MiCollab Audio, Web and Video Conferencing , the MiCollab Audio, Web and Video Conferencing server tracks how many audio and Web conferencing ports are scheduled for use at any given date and time.
- **Project Codes Required**: When this option is enabled in MiCollab Audio, Web and Video Conferencing , users must enter a project code when creating an MiCollab Audio, Web and Video Conferencing conference.
- Department Codes Required: When this option is enabled in MiCollab Audio, Web and Video Conferencing , users must enter a department code when creating an MiCollab Audio, Web and Video Conferencing conference.
- Project Codes: Provides a list of Project Codes configured for the MiCollab Audio, Web and Video Conferencing server.
- Department Codes: Provides a list of Department Codes configured for the MiCollab Audio, Web and Video Conferencing server.

Note:
Project and department codes are used to track conferences for billing purposes and to restrict conference usage.

- **MiCollab Audio, Web and Video Conferencing Internal Port**: Corresponds to the value for the Internal Port field (by default, port 4443) on the MiCollab Audio, Web and Video Conferencing Administrator Web Conferencing Settings page.
- MiCollab Audio, Web and Video Conferencing client version: Provides the current MiCollab Audio, Web and Video Conferencing Collaboration Client software version.
- **MiCollab Audio, Web and Video Conferencing server version**: Provides the current MiCollab Audio, Web and Video Conferencing server software version.
- **AWC External Port**: Corresponds to the value for the External Port field (by default, port 443) on the MiCollab Audio, Web and Video Conferencing Admin Web Conferencing Settings page.
- **Web Conferencing Name**: Corresponds to the value for the Web Conferencing Name field on the MiCollab Audio, Web and Video Conferencing Administrator Web Conferencing Settings page.

Note:
If you receive an IO Exception error message after you click **Sync Now**, refer to the Synchronization Error Messages topic.

4. Do one of the following:

   - Click **Create** to create the MiCollab Audio, Web and Video Conferencing collaboration server.
   - Click **Save** to save the updated information for the MiCollab Audio, Web and Video Conferencing collaboration server.
   - Click **Cancel** to return to the Collaboration tab without making changes.

You are returned to the **Collaboration** tab.

26.20 Features Tab

The Features tab provides fields and options used to configure feature profiles for each Enterprise and view current Licensed Feature Usage. Using feature profiles, you can quickly provision users with MiCollab Client features.

Select the Enterprise from the list box and the following information is displayed:

- **Feature Profiles**: The **Add Profile** link in the Feature Profiles section allow you to configure feature profiles for the selected Enterprise. A feature profile consists of a profile name and description, a list of licensed features included in the profile, and a list of members (users) assigned to the profile. You can create feature profiles based on basic user types: Integrated User, Stand-alone Web Portal User, and Stand-alone Mobile Portal User.

  Note:
  The Federation and Peering licenses are server-level licenses and therefore will not be included in any Feature Profiles. If the UC Server is licensed for Federation and Peering, the Federation and Peering tabs will appear on the UC Server Administrator interface. The tabs will not appear if the server is not licensed for these features. See the About Licensed Features topic for details about MiCollab Client licensed features.

- **Licensed Feature Usage**: The Licensed Feature Usage section provides read-only information about the current licensed feature usage on the system.

You can complete the following tasks from the Features tab:

- Click the Add Profile link to add a feature profile.
- Click the feature profile link in the **Name** column to edit the feature profile.
- Click the  icon to add or edit feature profile members.
- Delete a feature profile. **To delete a feature profile:**

  1. Select the feature profile you want to delete from the feature profile table.
  2. Click the **Delete Profile** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the feature profile, or click **Cancel** to cancel the deletion.

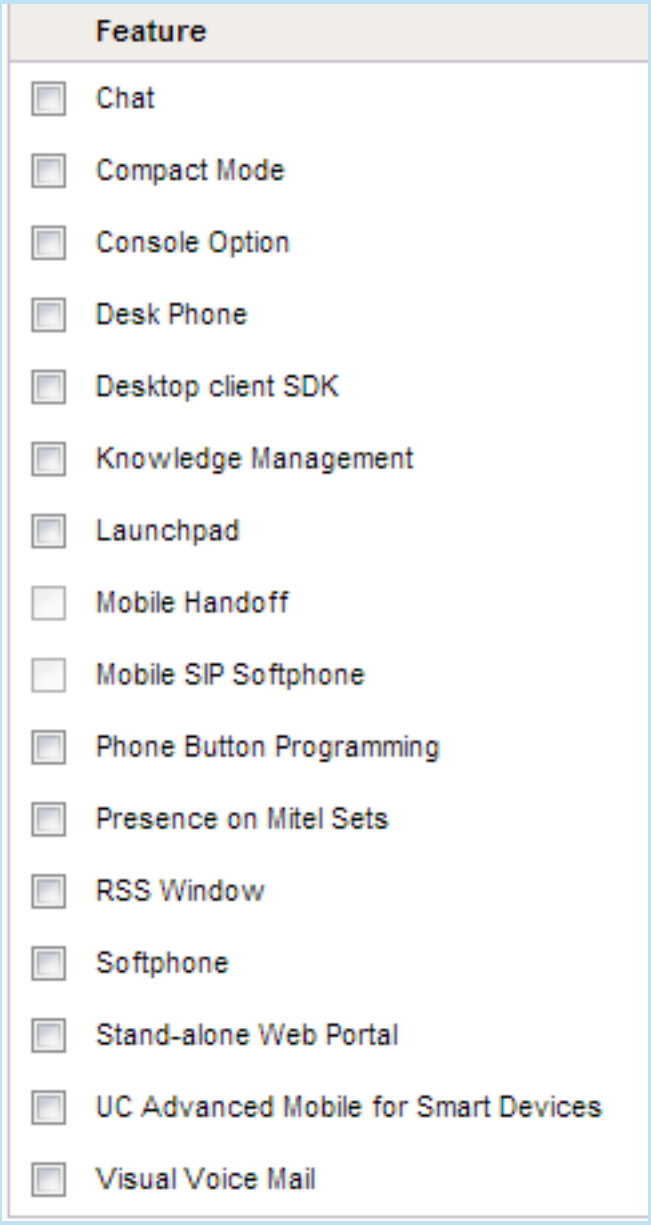
- View Licensed Feature Usage.

  The Licensed Feature Usage table provides the following information:

  - **Feature**: The name of the licensed feature. See the About Licensed Features topic for feature descriptions. Non-licensable features will not be visible in this list.
  - **Sys Allowed**: Indicates the total number of seats defined in the license for the entire system (all Enterprises combined).
  - **Sys Used**: Indicates the total number of seats in use for the entire system (all Enterprises combined).
  - **Allowed**: Indicates the number of seats defined in the license for the selected Enterprise.
  - **Used**: Indicates the number of seats in use for the selected Enterprise.
- Sort the information in the Licensed Feature Usage table.
- Refresh the information on the page.

Note:

The **Features Tab** - Licensed Feature Usage has been simplified in MiCollab Client 6.0 to only display the following Features .



Basic MiCollab Client: MiCollab Client 6.0 offers Desktop and Web clients the option to be configured as Basic MiCollab Client. The Basic UC Client is assigned the **default** feature profile which only provides access to the non-licensable features . Also see Licensed Features and Synchronization

Allowed Features	Desktop Client	Web Client
Blind Transfer	X	X
Call Forwarding	X	
Compact Mode	X	
Contact Groups	X	X
Corporate Contact	X	X
External Dial	X	
Missed Call Logs	X	X
Make and Receive Call	X	X
Office Communicator Integration	X	
Phone Button Programming	X	
RSS Window	X	
Visual Voice Mail	X	X
WLM Integration	X	

Teamwork mode: For accounts in Teamwork Mode, you can select any feature, however any phone or call control related features (such as Desk phone or Softphone) will be ignored. Licenses for individual features such as Chat, Visual Voicemail, etc… are still required.

26.204.1 Adding and Editing Feature Profiles

On the Feature Profile Details page, you can add new feature profiles and edit the features for existing feature profiles. See the About Licensed Features topic for feature descriptions.

Note:
Refer to the Licensed Features and Synchronization topic if you intend to create MiCollab Client accounts using a PBX Node or AD/LDAP synchronizer.

To add or edit a feature profile:

1. Configure the settings for the feature profile.
   - **Name:** (*Required*) Type a name for the feature profile. Maximum length is 64 characters, and the vertical bar character is not supported.
   - **Description**: (*Optional*)Type a description for the feature profile. Maximum length is 128 characters, and the vertical bar character is not supported.
   - **Member count**: This read-only field displays the number of members assigned to the feature profile.
2. *If you are creating a new feature profile,* click **Create**. The page expands to show the Features section.

3. Configure the features for the feature profile.

   The **Features** section shows a list of all the features that you can include in the feature profile. In addition, this section provides the following licensing information:

   - **Seats Available**: Displays how many licensed seats are available for each feature.
   - **Seats in Use**: Displays how many licensed seats are currently in use for each feature for the feature profile. The value displayed here corresponds with the number of members you have assigned to the feature profile. If you have not yet assigned members to the feature profile, the value will be 0.

   To add features to the feature profile, do one of the following:

   - Select the individual features you want to include in the feature profile.
   - Click **Select All** to include all features in the feature profile.

   Note:
   Both Web Portal features are set automatically when you select either one of them.

   To remove features from the feature profile, do one of the following:

   - Clear the feature check box for those individual features you want to remove.
   - Click **Remove All** to remove all features from the feature profile.

   Note the following if you are editing a feature profile with assigned members:

   - When you select and deselect features, the **Seats Available** and **Seats In Use** columns are updated to show the effect of including or excluding the feature in the feature profile.
   - If the number of available seats is less than the total number of profile members, the feature is disabled and displayed in *italic font*.

4. Click **Save** to save the feature profile. You are returned to the Features tab.

You can add members to the feature profile from the Features tab.

26.204.2 Adding and Editing Feature Profile Members

The Feature Profile Members page provides a table that lists all of the members for the feature profile. From this page you can add and remove members from a feature profile.

To add feature profile members:

1. Click the **Add Members** link. The Add Feature Profile Members page appears. Account names are presented alphabetically. Note the following:

   - Click the arrow buttons at the bottom of the page to scroll to a different page.
   - Use the Search function to quickly search for a name.

2. Select the accounts you want to add to the feature profile.
3. Click **Add to Profile**. The list of accounts you selected are added to the feature profile.
4. Click **Save**. The progress bar on the Feature Profile Member Update Status page indicates the progress of the operation.
5. Click **Done**. You are returned to the Features tab.

To remove feature profile members:

1. Select the members you want to remove from the feature profile.
2. Click the **Remove Members** link. The members are removed from the feature profile.
3. Click **Save**. The progress bar on the Feature Profile Member Update Status page indicates the progress of the operation.
4. Click **Done**. You are returned to the Features tab.

26.205 Peering Tab

Note:
Peering is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

Note:
The presence of the peered users with the login ID as UPN will be seen only when both the peered servers are on MiCollab version 9.4 and above.

The Peering tab allows you to configure peering for the Enterprise by adding MiCollab Client Services or external servers as peers. Peering between different enterprises on the same MiCollab Client server is supported.

Select the Enterprise from the list box and the following information is displayed in the Peer Server table for each peer server you have added:

- **Description**: The name that you have provided for the peer server.
- **Server**: The Fully Qualified Domain Name (FQDN) that you added for the peer MiCollab Client Service. N/A is displayed for external peer servers.
- **Peer Type**: The type of peer server (**MiCollab Client Service** or **External**).
- Peer Server Version: The MiCollab Client Service version which is installed on the peer server.
- **Status**: The status of the connection to the peer MiCollab Client Service. N/A is displayed for external peer servers.

You can complete the following tasks from the Peering tab:

- Click the Add Server link to add a peer server.
- Click the server link in the description, column to edit the peer server details.
- Delete a peer server. When you delete a peer server, all the information associated with the synchronizer is also deleted.
- Sort the information in the Peer Server table.
- Click  to open the peered MiCollab Client Service Administrator interface.

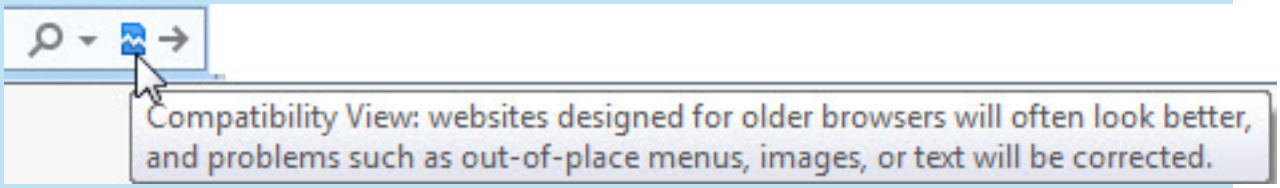
Note:

The following procedure must be done on MiCollab Client 5.1 to resolve peering on a server that had a changed IP address:

Go to the Enterprise Tab, expand Trusted Servers, select the peered server whose IP address changed, and in the Trusted Server Details page edit the field "IP address/hostname" with the correct IP address.

Note:

Peering contacts not displayed for a corporate directory on IE9 or IE10, then enable compatibility view by clicking here (icon is displayed to the right of the URL address in the browser window):



Note:

Whenever the peered server address is changed, the server address must also be updated in the peer trusted servers list.

26.205.1 Adding and Editing Peer Servers

The Peer Server Details page allows you to add and edit MiCollab Client Service and external peer servers.

If you are adding an external server to enable federation, the customer must install the IM server and deploy the XMPP gateway provided with the server to federate with MiCollab Client Service. Refer to the IM server documentation for instructions about configuring federation.

To add or edit a peer server:

1. Configure the server **Settings**.

   - Select the **Peer Type**. Options include **MiCollab Client Service** and **External**.
   - Type a **Description** for the peer server. The Description is limited to 64 characters in length and must contain alpha-numeric characters, dashes, and/or spaces.
   - (*MiCollab Client Services only*) Type the **hostname** for the MiCollab Client Service. The value entered in the hostname field must match the value used for generating the web server certificate on the MiCollab Client Service to which the MiCollab Client Service is being peered.
   - (*MiCollab Client Services only*) The **Peer enterprise ID** field defines which enterprise from the peered MiCollab Client Service will be synchronized with the selected Enterprise on the local MiCollab Client Service. The Enterprise ID is configured on the Enterprise tab. Do one of the following to add the Enterprise ID:
   - Click the **Select Enterprise** link, and then select the correct Enterprise from the list.
   - Type the Enterprise ID in the box. The Enterprise ID:
   - is limited to 4-32 characters in length.
   - must contain alpha-numeric characters (dashes included).
   - cannot contain spaces, vertical bars, commas, semicolons, or colons (| , ; :).

   Note:
   The Enterprise domain should be unique for each MiCollab Client Service peer. Mitel suggests using the site location or Enterprise ID (configured on the Enterprise Details page) as part of the Enterprise domain (for example, **Phoenix.xyzcompany.com**, where **Phoenix** is the Enterprise ID).

   - (*MiCollab Client Service s only*) *If required*, type the **Peer Dialing Prefix** for the server. The Peer Dialing Prefix is only required for PBX-to-PBX calls where the networked PBXs are not configured for transparent extension dialing. The value you enter here corresponds with the dialing prefix (not including the outgoing call digit) that PBX users must press to dial an extension on the networked PBX. The Peer Dialing Prefix is limited to 20 characters in length.

     Note: No validation is performed on the characters entered for the Peer Dialing prefix. The administrator should enter what is set up in the PBXs for calling from one PBX to another. The Peer Dialing prefix can start with a hyphen (-) character. Doing so informs the MiCollab Client Service to **not** append the outgoing prefix digit defined under the PBX node settings when making calls to extensions on the PBXs associated with the peered MiCollab Client Service .

2. *If you are adding a new peer server*, click **Create**.

3. (*External Servers only*) Configure the **Synchronization Settings** for the server

   a. (*Optional*) Schedule automatic synchronizations between MiCollab Client and the AD/LDAP databases by specifying the following:

      - The frequency (in days) the synchronization should occur.
      - The hour the synchronization should start.
      - The minute the synchronization should start.
      - Whether the synchronization should occur in the AM or PM.

   b. Click Add to add an AD/LDAP synchronizer and configure the settings.

   c. Click **Sync Now** to synchronize the AD/LDAP directory with the Unified Communications server. After you click **Sync Now**, the peer server contacts are imported to the MiCollab Client Service database (visible from the Corporate Directory Tab) and federation with these contacts is automatically enabled.

4. Click **Save**.

After you create peer servers, you can edit the associated fields at any time.

Peering between different enterprises on the same MiCollab Client Service is supported.

26.20.6 Federation Tab

Note:
Federation is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

The Federation tab allows you to configure IM and presence federation. IM and Presence Federation provides a communication path between a single MiCollab Client Service and one or more IM servers for the purpose of providing extended IM capabilities to MiCollab Client users. The communication path between the servers uses the Extensible Messaging and Presence Protocol (XMPP).

The customer must install the IM server and deploy the XMPP gateway provided with the server to federate with MiCollab Client Service. Refer to the IM server documentation for instructions about configuring federation.

Note:
You can also configure federation for an external IM server from the Peer Server Details page. After adding the server and performing a synchronization with the server's AD/LDAP database, the IM server contacts are imported to the MiCollab Client Service database (visible from the Corporate Directory tab) and federation is automatically enabled.

When a MiCollab Client Service and IM server are configured for federation, MiCollab Client users are provided with IM presence information and the ability to chat with IM contacts using the Desktop Client's Chat window.

When you configure federation from the Federation tab, instruct users to manually add federated contacts to the Desktop Client. Users should create a new personal contact, and then add the IM login information (for example, john_smith@ocs.com) for the contact using the MiCollab Client Login option.

Note:
For MiCollab Client v4.0, IM server support is limited to Microsoft Office Communicator Server (OCS) and IBM Lotus Sametime Server. For MiCollab Client v6.0, NextPlane Federation is supported.

In addition, for MiCollab Client v6.0, federation with MBG in the network path between MiCollab Client Service and the federated server (Skype for Business, IBM Sametime) is supported. This is accomplished by adding MBG connector for TCP port 5269 in MBG v8.0.

To configure federation with an external IM server:

1. Configure the external IM server for federation. Refer to the IM server documentation for instructions.
2. On the Federation tab, click **Enable Federation**. This configures the embedded XMPP MiCollab Client Service for federation.
3. Add the external IM server to the Federated Servers table.

    a. Click **Add Server**. A server entry is added to the Federated Servers table.
    b. Double-click **Enter domain**. An editable text box appears.
    c. Type the domain for the IM server (for example, ocs.com).

    Perform these additional steps if adding a NextPlane server:

    a. Select checkbox NextPlane.
    b. Double-click **Enter server**. An editable text box appears.
    c. Double-click **Port**. An editable text box appears.
4. Click **Apply** to save the information, or click **Reset** to clear your changes.

You can also complete the following tasks from the Federation tab:

- Click the **Disable Federation** button to disable federation on the MiCollab Client Service .
- Click the Delete Server link to delete an IM server from the Federated Servers table.

26.206.1 Federation Tab

Note:
Federation is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

The Federation tab allows you to configure IM and presence federation. IM and Presence Federation provides a communication path between a single MiCollab Client Service and one or more IM servers for the purpose of providing extended IM capabilities to MiCollab Client users. The communication path between the servers uses the Extensible Messaging and Presence Protocol (XMPP).

The customer must install the IM server and deploy the XMPP gateway provided with the server to federate with MiCollab Client Service. Refer to the IM server documentation for instructions about configuring federation.

Note:
You can also configure federation for an external IM server from the Peer Server Details page. After adding the server and performing a synchronization with the server's AD/LDAP database, the IM server contacts are imported to the MiCollab Client Service database (visible from the Corporate Directory tab) and federation is automatically enabled.

When a MiCollab Client Service and IM server are configured for federation, MiCollab Client users are provided with IM presence information and the ability to chat with IM contacts using the Desktop Client's Chat window.

When you configure federation from the Federation tab, instruct users to manually add federated contacts to the Desktop Client. Users should create a new personal contact, and then add the IM login information (for example, john_smith@ocs.com) for the contact using the MiCollab Client Login option.

Note:
For MiCollab Client v4.0, IM server support is limited to Microsoft Office Communicator Server (OCS) and IBM Lotus Sametime Server. For MiCollab Client v6.0, NextPlane Federation is supported.

In addition, for MiCollab Client v6.0, federation with MBG in the network path between MiCollab Client Service and the federated server (Skype for Business, IBM Sametime) is supported. This is accomplished by adding MBG connector for TCP port 5269 in MBG v8.0.

To configure federation with an external IM server:

1. Configure the external IM server for federation. Refer to the IM server documentation for instructions.
2. On the Federation tab, click **Enable Federation**. This configures the embedded XMPP MiCollab Client Service for federation.

3. Add the external IM server to the Federated Servers table.

    a. Click **Add Server**. A server entry is added to the Federated Servers table.
    b. Double-click **Enter domain**. An editable text box appears.
    c. Type the domain for the IM server (for example, ocs.com).

    Perform these additional steps if adding a NextPlane server:

    a. Select checkbox NextPlane.
    b. Double-click **Enter server**. An editable text box appears.
    c. Double-click **Port**. An editable text box appears.
4. Click **Apply** to save the information, or click **Reset** to clear your changes.

You can also complete the following tasks from the Federation tab:

- Click the **Disable Federation** button to disable federation on the MiCollab Client Service .
- Click the Delete Server link to delete an IM server from the Federated Servers table.

26.207 View Licensing Information

The MiCollab administrator portal opens at the **Licensing Information** page, which details user licensing for your applications.

Install and Upgrade Applications 27

This chapter contains the following sections:

- View ServiceLink Status

Note:
ServiceLink is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

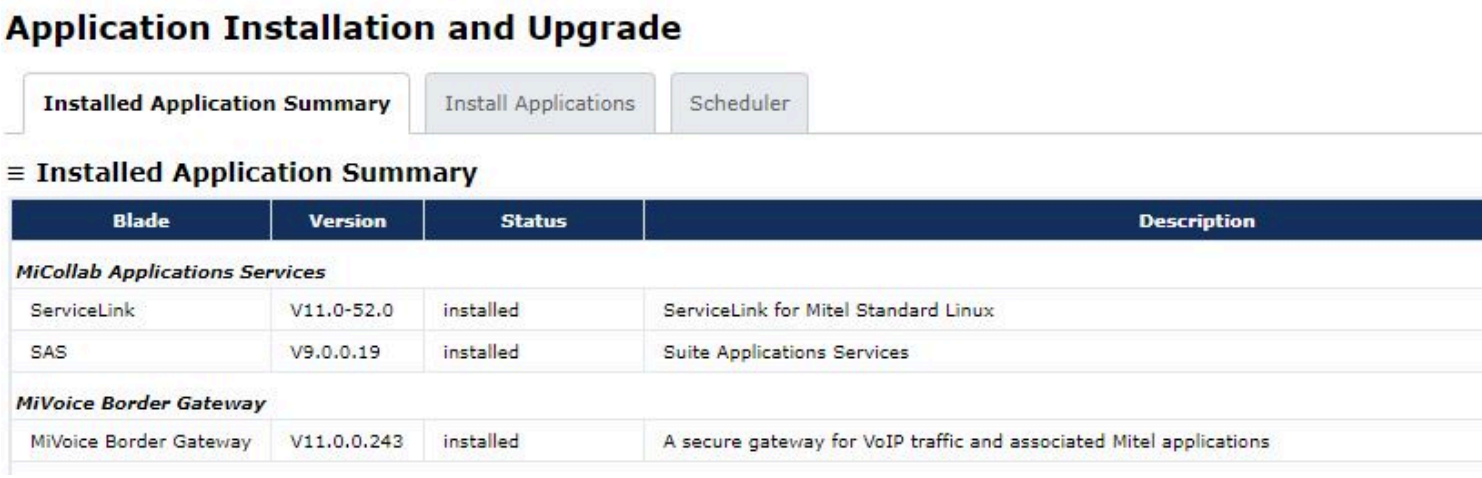
Description

Use this panel to upgrade and install MiCollab software for applications, services and security update blades.

Note:

- Ensure that the MiCollab server is NOT processing calls during an upgrade. Upgrading should be done outside of business hours.
- For Virtual MiCollab and MiVoice Business Express systems that are installed in a VMware environment, you can only use this panel to perform upgrades within the same release (for example, from Release 7.1 to 7.1 SP1). For major upgrades (for example from Release 7.0 to 7.x or from Release 7.x/8.x to 9.0) you **must** deploy a new OVA file. Refer to the *MiCollab Installation and Maintenance Guide* or *MiVoice Business Express Deployment Guide* for instructions.
- Downgrading MiCollab software to a previous (lower) release (for example, from Release 7.1 to 7.0) is not supported.
- All new MiCollab installations from R9.2 onwards will have MiCollab Client in an integrated mode by default.
- In case of an upgrade to R9.2 and above, the MiCollab servers in co-located mode will remain in co-located mode only.

Installed Application Summary Tab

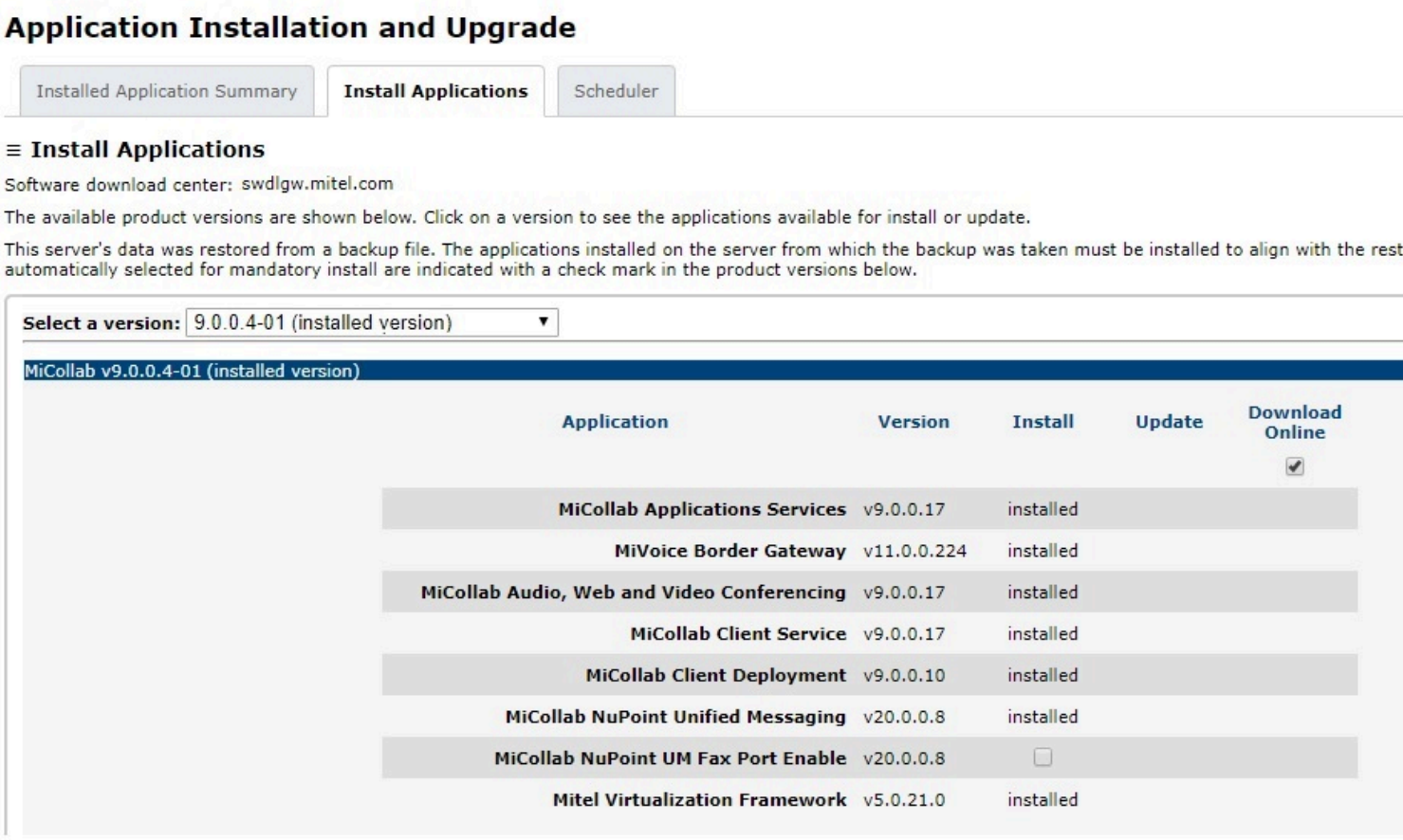


The Installed Application Summary tab lists the MiCollab applications, services and security update blades that are currently installed on the server.

Note:
In case of a download error due to network time-out or network error, the Admin again needs to start the downloading process manually. Downloads will not continue for that single file which ran into an error, but if some downloads were successful before the error, the download will not be repeated once the download resumes.

Field	Description
Blade	Abbreviated name of blade
Version	Version number of currently installed application blade
Status	Installation status (installed)
Description	Full name of application. In some cases a brief description of the application is also provided
Documentation	Link to documentation (if provided)

Install Applications Tab



Use the Install Applications tab to perform the following functions:

- Select the PBX type with which this server will interact (the first time you access the tab)
- View application information for unique MiCollab software releases.
- Determine the current status of your applications, services and security patches
- Install new applications, services and security update blades
- Upgrade existing applications (service pack updates), services and security patches

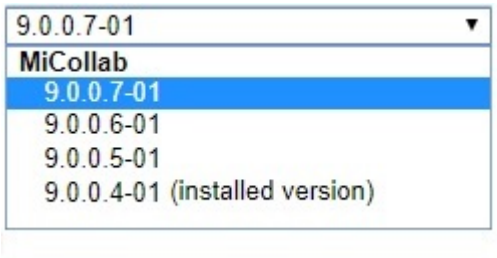
Selecting a MiCollab Version and Determining its Software Status

Use this procedure to select a MiCollab software version and determine the current status of its applications, services and security patches. By default, the system displays information pertaining to the currently installed MiCollab software version.

To select a MiCollab software version and determine the status of its applications, services and security patches:

1. Under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab.

3. To view licensed applications, services and security patches for a particular MiCollab software release, make a selection from the **Select a version** drop down menu:



The system downloads application information from online Software Download Center (SWDLC) and displays it in a table. Note that application information for the currently installed MiCollab version is displayed by default.

Field	Description
Application	The name of the application, service or security patch.
Version	This field lists the latest version of application software that is available for this version of MiCollab .
Install	If this field contains the word **installed**, the latest version of application software is currently installed on the system. If this field contains a blank check box, new application software is available for installation. To install it, select the check box and click the **Install** button. If this field contains a preselected check mark, new application software will be installed when you click the **Install** button.
Update	If this field contains a preselected check mark, updated application software will be installed when you click the I nstall button.
Download Online	Use this field to specify whether the software is to be downloaded from Software Download Center (the defaul t) or locally from CD/DVD or USB. To download from S WDLC, select the check box. To download locally, clear t he check box.

4. To view application information for a different version of MiCollab software (if available), make a selection from the **Select a version** drop down menu.

To download software from SWDLC, the firewall should allow the following connections and URLs:

- Licence entitlement:

  - register.mitel-amc.com port 22

  - sync.mitel-amc.com port 22

- Access token for contact delivery network

  - swdlgw.mitel.com port 443 (occurs during available blade software list update)
- Content delivery/blades Akamai

  - swdl.mitel.com port 443 (download of software)

Upgrading and Installing Software

Download Optional Software from MiAccess

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From the left menu, select **Software Download Center**.
3. Under **Navigate by categories**, select **MiCollab** or enter MiCollab in the search box and press Enter.
4. Click **MiCollab**.
5. Click the download icon for the appropriate MiCollab Software Download version.
6. Download the required application .iso files (for example MiCollab NuPoint Unified Messaging) to a network drive or to a folder on your PC. Do not change the names of the files. When you click a link, you are presented with a software Disclaimer.
7. Save the application .iso files to a network drive.
8. Copy the files to CD/DVD or USB (physical or virtual).

Connect CD/DVD/USB

To Physical Systems

- CD/DVD: To connect a CD/DVD to a physical platform, insert the CD/DVD in the drive
- USB: To connect a CD/DVD to a physical platform, connect the USB drive.

To Virtual Systems

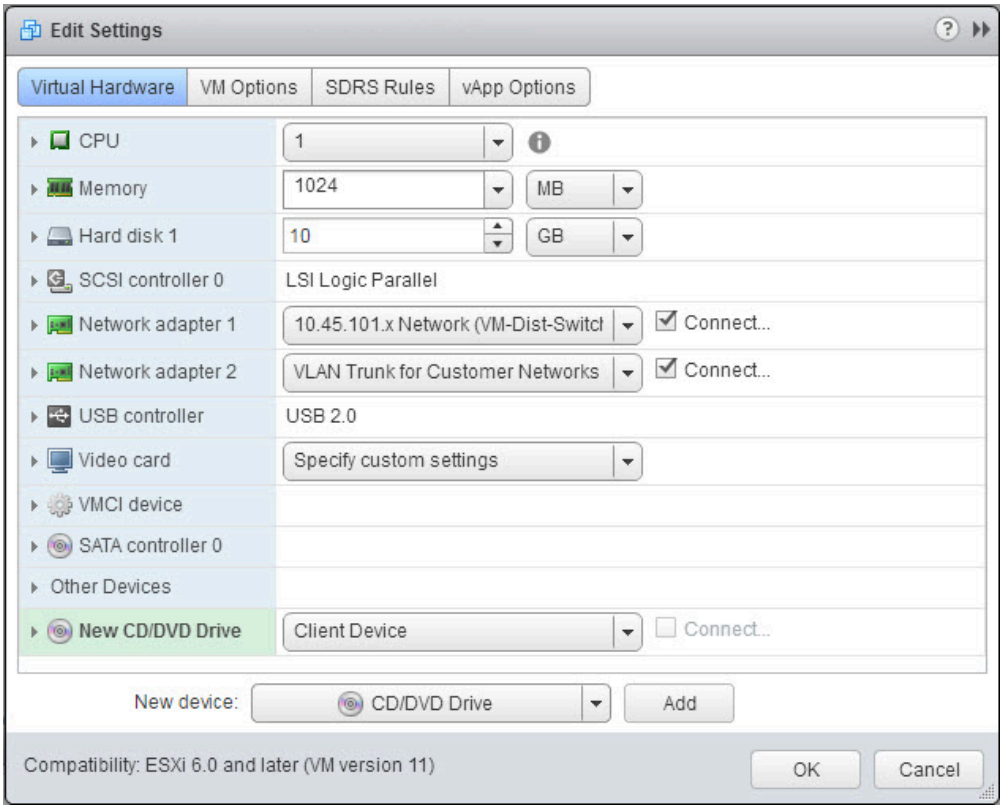
- CD/DVD

  Prerequisites:

  - Before adding the CD/DVD drive, turn off the virtual machine.
  - If the ISO image files are not available on a local or shared datastore, upload them to a datastore from your local system by using the datastore file browser.

  To connect a CD/DVD to a virtual platform:

  1. In the vSphere Client Application, right-click on the virtual instance (for example: vMiCollab 6.2.3.0 build) and then click **Edit Settings**. The Virtual Machine Properties window opens.
  2. Click the **Virtual Hardware** tab.
  3. From the New device drop-down menu, select **CD/DVD Drive** and click **Add**. The new drive appears at the bottom of the Virtual Hardware list.



  4. Expand **New CD/DVD Drive** and select the device type.

Option	Action
Client Device	a. Select to connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Web Client. b. From the **Device Mode** drop-down menu, select **Passthrough CD-ROM**. When you turn on the virtual machine, select the media to connect to from the **VM Hardware** panel on the virtual machine **Summary** tab.
Host Device	a. Select to connect the CD/DVD device to a physical DVD or CD device on the host. b. From the **CD/DVD Media** drop-down menu, select the media to connect to. c. From the **Device Mode** drop-down menu, select **Emulate CD-ROM**.
Datastore ISO File	a. Select to connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host. b. **Browse** to the file containing the ISO image to connect to and click **OK**.

5. (Optional) Select **Connect At Power On** to connect the device when the virtual machine turns on.
6. (Optional) To change the device node from the default, select a new mode from the **Virtual Device Node** drop-down menu.
7. Click **OK**.

- USB: You can add one or more USB passthrough devices from a client computer to a virtual machine on the virtual machine Summary page in the vSphere Web Client. The devices must be connected to a client computer that connects to the ESXi host on which the virtual machine resides.

  Prerequisites:

  - Ensure that a USB Controller is present.
  - Ensure that the vSphere Client application has access to the ESXi host on which the virtual machines are running.
  - Upload the ISO image files to the USB device.

  To connect a USB to a virtual platform:

  1. In the vSphere Client Application, right-click on the virtual instance (for example: vMiCollab 6.2.3.0 build) and then click **Edit Settings**. The Virtual Machine Properties window opens.
  2. Click the **Virtual Hardware** tab.
  3. Click the USB icon to the right of **USB Devices** under **VM Hardware** and select an available device from the drop-down menu.

  A Connecting label and a spinner appear, which indicates that a connection is in progress. When the device has successfully connected and the Summary tab refreshes, the device is connected and the device name appears next to USB Devices.

Select a Software Download Method

By default, all software is set to download from the Software Download Center (SWDLC). You may, however, download the software from local storage media (CD/DVD or USB). Use this procedure to specify which download method you wish to use for each application, either the SWDLC or local.

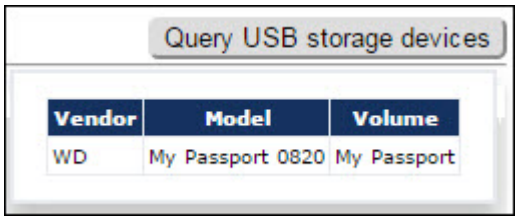
To select the download method for an application:

1. Clear the **Download Online** check box.



Each application now has its own **Download Online** check box. The boxes are cleared, indicating that MSL will attempt to download the application software from local media rather than the SWDLC.

2. Select a download method for each application:
   - To download from local media (CD/DVD or USB), clear the **Download Online** check box for the application.
   - To download from the SWDLC, select the **Download Online** check box for the application.
3. If installing from USB, click **Query USB Storage Devices**.



The system attempts to detect USB devices connected to the local computer. For each device that is found, the following information is displayed: **Vendor** name, **Model** name, and **Volume** label. When you install or upgrade an application, the system will search these devices for software (ISO files). If a device is not detected, it will not be searched.

Install New Software

The first time you access the Install Applications tab, you will be prompted to select the type of PBX with which the server will interact: MiVoice 5000 , MiVoice Business , MiVoice MX-ONE , MiVoice Office 400, or MiVoice Office 250 .

To install new applications, services and patches:

1. Under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab. If prompted, select the **PBX Type** with which this server will interact and then click **Next**.

   The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.

Note:
The MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400, are only supported in MiCollab Client Integrated Mode. If you are deploying MiCollab with one of these platforms, run the MiCollab Client Integration Wizard.

3. To display information for a different version of MiCollab software (if available), use the **Select a version** drop down menu.
4. Under the Install column:

Field Contents	Description
	The word installed indicates that the latest version of the application software is currently installed on the system.

Field Contents	Description
	A blank check box indicates that new application software is available. To install it, select the check box and click the Install button. A preselected check box indicates that new application s oftware will be installed when you click the Install button.

5. Select the software download method, either from the Online (SWDLC) or local media (CD/DVD or USB).
6. Click **Install** to install the applications/services you have selected.

   Software downloads are queued and installed sequentially from the SWDLC or local media.
7. If required, you will be prompted to insert any optional software CD/DVDs. Click **Continue**. Progress is displayed.
8. When installation is complete, click **Clear this report**. The MSL server manager displays the installed applications.
9. Remove the CD/DVD, disconnect the USB, dismount the network share, or dismount the vSphere Datastore.

Upgrade Existing Software

To upgrade existing applications, services and patches:

1. Under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab.

   The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.
3. To display information for a different version of MiCollab software (if available), use the **Select a version** drop down menu.
4. Under the Update column, a preselected check box displays for each currently installed application/ service that will be upgraded with new software when you complete this procedure.
5. Select the software download method, either from the SWDLC preselected check boxes.

   Software downloads are queued and installed sequentially from the SWDLC or local media.
6. If required, you will be prompted to insert any optional software CD/DVDs. Click **Continue**. Progress is displayed.
7. When installation is complete, click **Clear this report**. The MSL server manager displays the installed applications.
8. Remove the CD/DVD, disconnect the USB, or dismount the vSphere Datastore.

Note:
You can install and upgrade software simultaneously.

Scheduler tab

Use the **Scheduler** tab to configure the server to download the latest available application updates at a specific date and time. Only applications available online on the SWDLC are downloaded. You can schedule the update downloading to be a one-time event, or one that recurs weekly or monthly. Optionally you can choose to receive notifications that will alert you about the available updates.

Note:
The scheduler option is available only on a MiCollab or an MiVBX server.

Schedule Summary

Displays the result of the last scheduled event execution.

Scheduling Options

Complete the following steps to create a new scheduled event:

1. Under **ServiceLink**, click **Install Applications**. The **Application Installation and Upgrade** page opens.
2. Click the **Scheduler** tab.
3. In the **Scheduling Options**, select **Enabled** from the **Scheduler service status** drop-down.
4. Select the **Send update notification** check box if you want to be notified about an available update.
5. Configure the date, time, and frequency of downloading updates.
6. Click **Save**. The scheduler displays a confirmation that updates will be downloaded as scheduled by you.

Note:
The installation needs to be done manually after the blades are downloaded as per the time scheduled in the scheduler.

27.1 View ServiceLink Status

This panel provides updated ServiceLink status information for this server. License information is downloaded from the license server as part of the synchronization protocol.

You must activate ServiceLink before you can view status information. The status is a result of a successful or non-successful online or offline synchronization with the server from which the license information is downloaded.

MiCollab solutions with MiVoice MX-ONE, MiVoice 5000 and MiVoice Office 400 will use the SLS License Server, whereas the MiCollab solution with MiVoice Business and MiVoice 250 will be licensed through AMC (Application Management Center) License Server.

Online Activation

To activate ServiceLink online:

1. Obtain an Application Record ID (service account ID) or or ServiceLink ID (Serial ID) from your authorized reseller.

Note:
ARID is for AMC License Server and ServiceLink ID is for SLS.

2. Under **ServiceLink**, click **Status**.
3. In the Service Link Activation Page, enter your **Application Record ID** (also called Service account ID).) in case of AMC and **ServiceLink ID** in case of SLS.
4. Enter:

- Address of proxy
  - Address of proxy
  - when using SLS or AMC
- TCP port
  - when using a proxy with different port (valid for both AMC and SLS)

Note:
The proxy server must be configured to forward TCP packets on the incoming port to the AMC address which is sync.mitel-amc.com on port 22. In case there is no proxy, the AMC address field can be left blank.

Note:
If SLS is being used, then enter the proxy address as **sync.sls.mitel.com.** This is not an optional field in case of SLS.

5. Click **Activate** to synchronize with the license server and activate ServiceLink.

Following successful activation, MSL periodically reconnects to the AMC (every 24 hours by default) via a secure, encrypted connection to synchronize ServiceLink status information. New configuration instructions, such as services you have added or deleted to your AMC account, are updated at this time.

Manual Synchronization

Although the system automatically synchronizes with the license server on a periodic basis (every 24 hours by default), you can force an immediate synchronization at any time. This is useful to check the network connection between MSL and the license server, attempt to clear major alarms that are generated if the automatic sync process fails, or to obtain up-to-date ServiceLink configuration information from the license server. This procedure can be performed on systems that have been activated either online or offline.

To manually synchronize with the license server:

1. Under **ServiceLink**, click **Status**.
2. Click the **Sync** button.

Deactivation

If the system hardware has been changed or replaced, you will need to deactivate your ServiceLink account, reset your Hardware ID, re-enter your Application Record ID and then reactivate your ServiceLink account. Use the MSL server manager to complete all steps with the exception of resetting your Hardware ID, which must be done on the licence server.

To deactivate ServiceLink:

1. Under ServiceLink, click **Status**.
2. Click the here link to access the deactivation screen.
3. Click **Deactivate**.

Note:
Following deactivation, you must reset your hardware ID on the license server and then reactivate your ServiceLink account using either the online or offline method.

Administration 28

This chapter contains the following sections:

- MSL Web Services
- Backup Server Data
- View Log Files
- View Event Logs
- About SDS Distribution Errors
- View System Information
- Access System Monitoring Tools
- System Users
- Shutdown or Reboot
- Mitel Virtualization Diagnostics Tool
- Applications

28.1 MSL Web Services

Mitel Standard Linux includes a Representational state transfer (REST) API that provides a secure web services framework using the OAuth 1.0 protocol. This "Web Services" interface is intended to support the features and functions currently available in the traditional Mitel administrative interfaces.

In its initial release, the Web Services interface supports MiCloud Management Portal (MMP) management integration. MiCloud Management Portal (MMP) is a web-based customer provisioning application that employs the Multi-instance MiVoice Business to deliver multi-customer communications services for service providers. Hosted from the data center, MiCloud Management Portal (MMP) is intended as the primary management tool for customers and end-users to access and modify services.

By default, the Web Services panel includes a single registered web services client for MiCloud Management Portal (MMP). Do not change this configuration in any way. Do not modify the existing consumer information or tokens, and do not attempt to add a new consumer.

The administrator can create a new web services consumer. A consumer is a vendor of a particular web services client. The credentials entered are used in the client to begin the OAuth authentication process.

You can use the Web Services panel to enable/disable the interface. To enable/disable the MSL Web Services interface:

1. Under **Administration**, click **Web services**.
2. Under Manage web service availability, click **Start** to enable or **Stop** to disable the web services interface.

Note:
The expired consumer tokens must be manually renewed from the Web Services interface. Periodically check the **Approved tokens** table to **Modify**, **Renew**, or **Revoke** the tokens that are representing an approved client for the web service.

28.2 Backup Server Data

There are two main methods for backing up system data (including all server configuration data, application configuration data, user settings, messages, and greetings):

- Server Manager **Backup** (to backup data to a local workstation or a network file server that supports SFTP or SMB/CIF), and
- Server Console **Perform Backup** (to backup to a USB device or to a network file server)

If you are planning to restore a pre-existing MiCollab 1.1 backup, we recommend that you verify the file beforehand.

Note:

- If your MiCollab system is integrated with a directory service, ideally you should back up both the MiCollab database and the directory server database at the same time.
- You can use different filenames for backup files, but the filename must not contain spaces and the file extension must be **.tgz**. (Note that all backup files of systems prior to Release 9.0 will be titled "smeserver.tgz".)
- The content of the system's /root directory will be included in the backup. To minimize the backup size, delete any temporary unwanted files that administrators might have created during system support activities. Do not delete the content of hidden files and directories such as /root/.ssh and /root/.bash* which are required for proper server functionality.
- The backup file does not include OAuth 1.0 data. Accordingly, if you have implemented Google Apps integration with OAuth 1.0, you must re-enter the data after performing a restore procedure. (Note that OAuth 2.0 data *is* included in the backup file.)
- To ensure that MiCollab has consistent Network Element (ICP) information, you must use one of these backup procedures. Restoring backups made from inside the individual applications may cause incorrect Network Element data to be presented to the MiCollab server.
- To restore the data, you must transfer the backup file to a storage medium (CD/DVD or USB storage device).
- If MiCollab is deployed in LAN only mode with Teleworker running remotely on an MBG server in the DMZ, you should back up both the MiCollab server database and the MBG server database at the same time.
- You cannot restore a MiCollab database backup to a Virtual MiCollab Release 2.1 deployment. For Virtual MiCollab Release 2.1 deployments you must use VMware tools to perform backups and restores. See the *MiCollab Installation and Maintenance Guide* for instructions. However, it is recommended that you continue to take scheduled MiCollab database backups from a Virtual

MiCollab Release 2.1 deployment, because MiCollab database restores are supported in MiCollab Release 2.2 and later.

Server Manager "Backup"

Backup to Desktop

Use this procedure to save your system backup to a file or device on your desktop computer or maintenance PC if your MiCollab system has only one application installed .

A "Backup to desktop" saves all of the data to a single, large compressed file and is therefore limited by the file system and browser of the client operating system. For example, if you are backing up data to a Windows client that uses the FAT32 file system (the default for many older versions of Windows), you are limited to a maximum file size of 4 GB; newer Windows operating systems that use the NTFS file system have a much larger capacity. If the backup file exceeds the maximum file size of the client operating system, it cannot be properly restored. For this reason, we recommend that you use the Verify Backup File option in the MSL server console to ensure the backup was successful.

1. Under **Administration**, click **Backup**.
2. Select the **Backup to desktop** option.
3. Click **Perform**. MSL prepares the system for backup.

   The "Operation status report" is displayed with the estimated backup size, along with the "Backup Encryption" option.
4. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. The encrypted backup file is identifiable with an .aes256 extension.

Note:
You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

5. Click **Download Backup File**.
6. When prompted to Open or Save, click **Save**.
7. In the file download window that appears:

   - Name the file and then select the location where the file will be saved. Note the backup filename must not contain spaces; otherwise, you will get an error when you attempt to restore it.
   - Click **Save**. After saving, you can copy the backup file to a CD/DVD or USB storage device, if required. The backup file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

Schedule Backups to Network File Server

Use this option to:

- perform immediate system backups to a Network File Server
- schedule daily, weekly, or monthly system backups to a Network File Server

Use this option if your system has more than one application installed.

Note:

- You can only have one backup scheduled on the server. To cancel an existing backup schedule, select **Disabled** and then click **Save**.
- If you are backing up to an MSL server, configure it to accept access from the backup server. See Configure Network Privileges for details.
- Two file-sharing protocols are supported:
  - SMB/CIFS
  - Secure File Transfer Protocol (SFTP)

To perform a backup to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Perform**.
4. Specify the following details.

Field	Description
IP Address	IP address of the network file server where you have stored the database backup file.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.

Field	Description
Domain or Workgroup Name	Domain or workgroup name. Applies only to SMB/CIFS. Leave the field blank for SFTP. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then the server's local Security Account Manager (SAM) is used for authentication, instead of the domain SAM. This field is required only for the SMB/CIFS protocol.
Sharename	The file-share name. Applies only to SMB/CIFS. Leave the field blank for SFTP. The restore utility will try to connect to the server/shared folder as an SMB/CIFS resource. The shared folder must have permissions set to "Full Control."
(Optional) Sub Directory	Name of the sub-folder where you have stored the database backup file. For SMB/CIFS, the sub-directory is relative to the share. For SFTP, the sub-directory is relative to the root of the file system accessed through the SFTP protocol.

Note:
If you are backing up to an MSL server, enter its IP Address and the Username/Password of the "root" user. Leave the remaining fields blank..

5. (Optional) Select the **Maximum number of backup files to keep** (1-999) on the server. When the number of stored files reaches this maximum count, the oldest version is deleted.
6. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters.

Note:
You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

7. Click **Backup Now** to test your server configuration by performing an immediate backup.

   The backup file is saved to the network file server. The file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

To perform an immediate backup, Click **Backup Now**.

To schedule backups to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Save**.
4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example:

   mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz).

   - For Daily backups, select a time of day (hour, minute, AM/PM)
   - For Weekly backups, select a time of day, and day of the week
   - For Monthly backups, select a time of day, and day of month
   - To disable regularly scheduled backups, click **Never.**
5. Click **Save**.

Server Console "Perform Backup"

You can save your system backup to a USB storage device (such as a memory stick or hard drive) or to a network file server that supports SFTP (typically a Linux server, including MSL) or SMB/CIF (typically a Windows server). Any USB storage device that is formatted as FAT32 (DOS), EXT3 (Linux), or NTFS (Windows and Linux) is compatible.

The backup file size limit via USB or network backup is set by the destination file system: 4 GB for a FAT32, 2 TB (terabyte or trillion bytes) for NTFS, and 16 GB to 16 TB for ext3 (depending on file system block size). The current MSL ext3 block size is 4096 bytes which allows file sizes of 2TB.

Optionally, you can encrypt the backup file if you are saving it to a USB device from the server console. This option is not available if you are saving the backup file to a network file server from the server console.

1. Access the server console.
2. Log in as " admin".
3. From the console, select the option to **Perform backup**.

4. Select a destination for the backup file:

   - Backup to a USB device.
   - Backup to a network file server.

Backing up to a USB Device

1. Select **Backup to a USB device**.
2. At the prompt, insert the USB device (if not already in place) and click **Next**.
3. When prompted, enter a filename for the backup file (default is ' mslserver') and click **Next**. Note the backup filename must not contain spaces; otherwise, you will get an error when you attempt to restore it. The file extension, either .tgz (unencrypted) or .aes256 (encrypted), is automatically added.
4. (Optional) To encrypt the backup file, enter an encryption password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. Click **Next**.

> **Note**:
> You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

5. MSL displays an estimate of the size of your backup. Click **Proceed**.
6. When the backup is complete, remove the USB device at the prompt. Click **Continue**.
7. Re-mount the USB and verify that the backup was performed successfully using the Verify Backup Data procedure.

Backing up to a Network File Server

> **Note**:
> If you are backing up to an MSL server, enter its IP address and the username/password of the "root" user. Leave the remaining fields blank.

1. Select **Backup to a network file server**.
2. Enter the **IP address** of the file server where the backup will be stored.
3. Enter the **domain** or workgroup name of the server. (For example, mitel.com.)
4. Enter the name of the **shared folder** where the backup file will be stored. (For example, "Backups".) The shared folder must have permissions set to "Full Control".
5. Enter an **Optional Sub Directory** for the backup file. The specified directory must exist in the share folder. The field accepts multi-level directories; for example"MAS/Sept/backups". If you leave this field blank, the system stores the file in the root directory of the specified network share.

6. Enter the **username** to use when connecting to the backup server.
7. Enter the **password** to use when connecting to the backup server.
8. Click **Next**. A progress bar indicates backup status. When the backup is complete, file verification is performed automatically.

Verify Backup Data

When backing up to a USB device or when using a pre-existing backup file, it is important to verify the file before starting a restore procedure. If your backup file cannot be verified, then it cannot be used to restore system information.

To verify a backup file:

1. Access the server console at the MiCollab server or from a maintenance PC.
2. Log in as " admin".
3. From the console, select the option to **Verify backup file**.
4. At the prompt, insert your storage medium. (Note: if your USB device was left mounted after your last backup, you must remove it and re-mount it first.) A list of all storage devices found on your system is displayed.
5. If more than one storage device is connected to your system, select the device containing the backup file.
6. If more than one backup file is contained on the storage device, select the file you want to verify.
7. Click **OK**. Verification of the file is confirmed. If you receive an error message, you cannot use this backup file for the restore. Check your storage media and try the backup procedure again. See the *MiCollab Engineering Guidelines* for a list of supported USB devices.

Restore (Disaster Recovery Situations)

When recovering from a disaster situation, it is necessary to reinstall MSL operating system software. Follow the instructions for Disaster Recovery in the *MiCollab Installation and Maintenance Guide MSL Installation and Administration Guide*.

28.3 View Log Files

Use this panel to view/download log files and to collect log files and diagnostic data.

View/Download Log Files

To assist in troubleshooting, you can either view or download the log files generated by the services running on your server.

To view/download the log files:

1. Under **Administration**, click **View log files**.
2. Under View Log Files, choose a log view. Most system services write their logs to the "messages" file.

3. Enter a **Filter Pattern** to view online the lines of the log that contain that text. This option applies only to viewed files. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.

   A regular expression (abbreviated as regexp, regex, or regxp) is a string that describes or matches a set of strings, such as particular characters, words, or patterns of characters, according to certain syntax rules. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification.
4. Specify a **Highlight Pattern** to mark in bold the specified text in any logs that the text appears. This option applies only to viewed files. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.
5. From **Operation**, select **View log file** or **Download**.
6. Click **Next**. If you selected **View log file**, the log files are displayed.

Note:
The system automatically updates the list every 5 seconds with any new logs.

Collect Log Files and Diagnostic Data

This utility allows system-level logs to be collected for the server platform and then saved to another location such as your local PC. Logs can be selected for collection from specific applications.

To collect and save log files:

1. Under **Administration**, click **View log files**.
2. Under Collect log files & diagnostic data, select which categories you wish to collect. To minimize the size of the log file, uncheck categories you do not require.

Note:
Coredump log files can be very large and take a long time to collect. It is recommended that you uncheck the "Coredump files" category.

3. Click **Start**. A progress indicator appears while the logs are being collected.

Note:
You can navigate to other screens without interrupting the process.

4. When the log collection process finishes, the indicator changes to "Complete / 100%" and the archived log file is listed on the screen. Depending on which type of web browser you are using, a copy of the file will be downloaded automatically or you will be prompted to save it.
5. You can manage the list of archived log files as follows:

   - To save and encrypt a file, click **Encrypt Download**, enter a **Password**, and then re-enter it. Create a strong password by using a mix of characters, numbers and symbols, plus both upper and lower case characters. Click **Continue**. An encrypted tar file with the filename "sosreport-<file>.tar.gz.aes256" is saved to the **Downloads** folder.
   - To save a file without encrypting it, click **Download**. A tar file with the filename " sosreport-<file>.tar.gz" is saved to the **Downloads** folder.
   - To delete a file, click **Delete**, and then click **OK**. The archived log file is deleted from the server.

After saving an archived log file, send it to Mitel Product Support for analysis. If the file is encrypted, also send the password. Without it, the file cannot be decrypted.

Note:

- To decrypt an encrypted log file, transfer the file to a Linux system, access a console on the system, and then enter the following command: **openssl enc -aes-256-cbc -d -in filename -out newfilename**. **openssl** - This is the openssl command. **enc** - This indicates the symmetric cipher routine being used.
- When prompted, enter the password used to encrypt the file. If you only have access to a Windows system, use a Unix emulator such as CygWin to perform these steps.
- Archived log files are automatically deleted from the server after 72 hours.
- You can also manage the archived log files from the MSL shell. The files are located on the server in / var/cache/e-smith/ logcollector.
- For MSL-based versions of MiVoice Business , collecting logs is a multi-step process:

  1. In the MSL Server Manager, access the View logs files screen and select the **Collect MCD logs** check box.
  2. In the MiVoice Business System Administration Tool, access the System Diagnostics form, run the System Diagnostics and package the log files.
  3. In the MSL Server Manager, access the View logs files screen and click **Start** to collect the logs.
- For an EX controller, the SOS report contains the Notification file that consists of EX events along with the EX configuration data.

28.4 View Event Logs

You can display the current alarm state of the system and view the application event logs for some applications (such as MBG).

Note:
Some deployments may display a Critical alarm after initial installation. Follow the instructions below to clear the alarm.

Alarm Notification

The header bar of the MSL server manager contains an "Alarm Status" label which indicates the system alarm severity level. For example, if the system has a service-affecting fault, the label will display "Minor" with a yellow background. Clicking the label opens the Event Viewer.

View Application Event Logs

To view application event logs:

1. To access the Event Viewer, do one of the following:
   - Click the **Alarm Status** severity indicator.
   - Under **Administration**, click **Event viewer**.
2. Select the number of events that you want to display per page from the **Events per Page** drop-down menu.
3. The **Boundary dates and times** are populated automatically by the system. To enter non-default values:
   - Under **Start** and/or **End**, click the **Manual** box.
   - Enter a new **Date** (YYY-MM-DD) and/or **Time** (HH:MM:SS).
4. Select the **Severity filter**. All logs with the selected alarm severity or higher will be displayed.
5. In the **Text filter** field, enter any text that you want the logs to be filtered against. Only logs that contain the specified text will be displayed. The filter is applied against the log data in the "Application", "Event type", "Value" and "Description" fields.
6. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.

   A regular expression (abbreviated as regexp, regex, or regxp) is a string that describes or matches a set of strings, such as particular characters, words, or patterns of characters, according to certain syntax rules. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification.
7. Select the **Show Cleared Events** box if you want to view both cleared and new events. Clear the box if you only want to view new events.

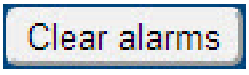
Note:
Events may also be cleared automatically by the applications.

8. Select the **Auto Reload** box if you want the system to automatically reload the events each time you open the page.
9. Click **Reload**. The event logs are displayed.

Field	Description	Possible Values
Clear	Click to clear this ietm.	
Application	Application name	
Event Type	Event that was occurring or attempting to occur when the alarm was set.	• set connection • set registration • one-way audio
Value	Value associated with the event	• established • rejected • lost • MAC address (for one-way audio)

Field	Description	Possible Values
Severity	Level of severity associated with this alarm	• **Cleared** (green): No alarms have been raised since the alarms were last cleared. • **Indeterminate** (turquoise): The cause of the alarm cannot be determined at this time. • **Warning** (blue): Indicates an "information only" alarm. • **Minor** (yellow): Indicates a fault which affects service. This may result in a major degradation in service and requires attention to minimize customer complaints. • **Major** (orange): Indicates a fault which will cause a major degradation in service and requires attention as soon as possible. • **Critical** (red): Indicates a total loss of service which demands immediate attention. The "Indeterminate", "Warning" and "Cleared" states are informational only
Date and Time	Timestamp of the alarm	
Description	A comma-separated list of identifiers that pertain to the alarm; may contain MAC and IP addresses as well as Reason for alarm.	(various) Click the **Refer to...** link to open the application that is affected by this alarm.

Clear Alarms

- To clear all alarms, click **Clear alarms**. 

- To clear an individual alarm, click **Clear** for the item. 

28.5 About SDS Distribution Errors

Flow Through Provisioning synchronizes user and services data updates between the MiCollab database and MiVoice Business system databases in a sharing network. If you make an update in the MiCollab USP database and the update is not successfully shared to all the other elements in the sharing network, a distribution error is sent to the MiCollab SDS Distribution Errors application. If the number of distribution errors exceeds an SDS alarm threshold, a data distribution alarm is generated in the Event Viewer application.

The SDS Distribution Error application allows you to view and manage distribution errors and pending updates:

- **Distribution Errors** are updates that could not be applied to the destination elements.
- **Pending Updates** are updates that have not yet been applied to the destination elements.

From this application, you can:

- reload the list of distribution errors
- export the errors to a file
- delete updates
- retry failed updates
- filter errors in the list.

Launching the SDS Distribution Error Application

Note:
The SDS Distribution Error application is only available if Flow Through Provisioning has been enabled between MiCollab and MiVoice Business platforms.

1. Under **Administration**, click **SDS Distribution Errors**.
2. Resolve any distribution errors.

Field Descriptions

Parameter	Description
	Click to select a record
	Click to display the details for the record.

Parameter	Description
Action ID	A unique number sequence that identifies the transaction of a specific shared form distribution attempt.
To	Indicates the destination network element for the membership data. **Note**: This field displays the name of the destination network element as it appears in the Network Elements form of the MiVoice Business system.
Date/Time	Displays the date and time that a distribution transaction was attempted.
Last Retried	Displays the date and time of the most recent failed update retry.
Action	Specifies the configuration action type (for example: add, modify, or delete).
MiVB Form Name	Identifies the name of the MiVoice Business form from which the data distribution originated.
Error Type	The types of distribution error messages include: • Transport errors - failures of data update event delivery • Application errors - failures of data update transaction at destination • Concurrency error - conflicting data update information at the destination because • a change was made to a record but the original record on the remote system(s) was not in sync with the original record on the local (master) system, or • a change was made at the same time by two or more administrators on the same record. • Transport and Concurrency Error • Application and Concurrency Error
Reason	Displays an error message.

Parameter	Description
Status	Displays the status of the update: • Idle - awaiting Retry operation • Retry Pending - administrator has retried the update and a system response is pending. • Pending - automatic update has been sent and a response is pending. **Note**: The status field is updated approximately every 30 seconds.
Count	The Count in the lower left corner of the Distribution Error screen displays the total number of error listed.

28.6 View System Information

System Information for your server can be viewed under **Administration** > **System Information** panel.

The System Information panel provides hardware manufacturer and product name/model information. This panel also provides a summary of networking parameters, server details, and domain information.

The following system parameters are displayed in this panel:

- **System Vital** - hostname, IP address, kernel version, and so on. For example, this panel indicates whether the MSL Kernel Version is 32-bit or 64-bit.
- **Memory Usage** - Server-wide memory utilization statistics, size and the usage of random-access memory.
- **Mounted Filesystem** - list of the mounted partitions, root, directory (mount point), size, and available storage
- **Network Usage Information** - the amount of data sent and received by your system network interfaces, network interface throughput.
- **Hardware Information** - server manufacturer/model, number of processors/model, CPU speed, cache size, and so on.

28.7 Access System Monitoring Tools

To enable access to system monitoring tools:

1. Under **Administration**, click **System Monitoring**.
2. In the **Access to system monitor display** field, select one of the following:

   - **Private**: to allow access only for private networks (local networks only)
   - **Public**: to allow public access to entire Internet (visible to anyone on the Internet)
   - **Disabled**: to disable access
3. Click **Save**.

To view the system monitor display, click **System monitor display**.

28.8 System Users

28.8.1 Manage User Accounts for Remote VPN Access

You can add, modify, lock, or remove user accounts for Virtual Private Network (VPN) client access. When you create a new system user account, the account is locked. You must reset the password to enable access to the account.

To add a system user account for VPN client access:

1. Under **Administration**, click **System users**.
2. Click **Add user account**.
3. Enter the **Account name**, **First name**, and **Last name**. The account name should contain only lower-case letters, numbers, hyphens, periods, underscores and should start with a lower-case letter. For example "betty", "hjohnson", and "mary-jane" are all valid account names, but "3friends", "John Smith", and "henry:miller" are not.
4. Set **VPN Client Access** to **Yes**.
5. Click **Add**.
6. Click **Reset Password** and reset the password for the account. By default, passwords must be at least 8 characters. See Password quality requirements.
7. From the list of users, you can modify or remove a user account (by clicking **Modify** or **Remove** next to the user name), or set the user's password. User accounts are locked out and cannot be used until you set the initial password for each account.

28.8.2 Manage Multiple Admin Accounts

You can create additional administrative accounts which have complete Server Manager access. This setting allows multiple users to have administrative access to the server without having to share the primary **admin** user account password.

The primary system **admin** account has privileges to create and modify any system account, including password resets of the sub-admin accounts. Additional sub-admins can only modify their own account information and do not have privileges to create additional administrative accounts.

Note:

- It is strongly recommended that only a single admin user perform any system modification at one time to prevent concurrency issues.
- Any logs produced, by operations performed by the logged in user, are recorded with the user login name for audit trail purposes.

To provide a system user account with Admin access:

1. Under **Administration**, click **System users**.
2. Click **Add user account**.
3. Enter the **Account name**, **First name**, and **Last name**. The account name should contain only lower-case letters, numbers, hyphens, periods, underscores and should start with a lower-case letter. For example "betty", "hjohnson", and "mary-jane" are all valid account names, but "3friends", "John Smith", and "henry:miller" are not.
4. Set **Admin User Access** to **Yes**.
5. Click **Add**.
6. Click **Reset Password** and reset the password for the account. By default, passwords must be at least 8 characters. See Password quality requirements.

Note:
Only ASCII characters are supported for sub-admin passwords.

7. From the list of users, you can modify or remove a user account (by clicking **Modify** or **Remove** next to the user name), or set the user's password. User accounts are locked out and cannot be used until you set the initial password for each account.

Locking (Disabling) User Accounts

When an account is locked, the user will no longer be able to access server resources such as the VPN. To unlock the user account, reset the password using the Reset password link.

Changing User Passwords

Administrators can change user and/or administrator passwords by using the Reset password link for that user's account on the Users panel. This entry overrides any previous password entered. Passwords can contain any combination of printable characters, including upper- and lowercase letters, numbers, and punctuation marks. By default, passwords must be at least 8 characters. See Password quality requirements.

Note:
There is no way to recover a forgotten password for a user. If this occurs, a new password must be set.

28.8.3 Digital Certificates for VPN Connections

For increased security, you can use SSL client certificates to authenticate VPN connections.

To implement this feature for a user, you must download a certificate from MSL, import the certificate to the user's computer, and then set up the user's VPN connection.

Downloading the Certificate from MSL

Use this procedure to download the user's digital certificate from MSL, the certificate authority (CA).

To download a certificate from MSL:

1. Log in to the server manager remotely from a Windows PC.
2. In the server manager under Administration, click **System Users**.
3. Find an existing user (or set up a new user and reset the password).
4. Click **Download VPN certificate**.
5. Click **Save** or **Save as** and save the file to a location on your computer.

Importing the Certificate

Use this procedure to import the user's digital certificate to the user's computer.

Note:
The following procedure outline how to import a certificate to Internet Explorer 9 in a Microsoft Windows environment. For instructions to perform these procedures on a different browser, refer to your product documentation.

To import a certificate to the user's computer:

1. In Internet Explorer, click **Tools > Internet Options**.
2. On the Content tab, click **Certificates**.
3. Click **Import**.

4. The Certificate Wizard opens. Click **Next**.
5. Browse to the location of the stored certificate file.

> **Note**:
> The file may not be visible until you specify files with extension .pfx or .p12.

6. Click **Open** and then click **Next**.
7. In the Password dialog, click **Next** to continue. Do not enter a password for the private key.
8. In the Certificate Store dialog, select **Automatically select the certificate store based on the certificate type**.
9. Click **Next**. If Windows prompts you for confirmation to install the certificate, click **Yes**.
10. Click **Finish** to complete the certificate import.

Setting Up the VPN Connection

Use the following procedures to set up a VPN connection on the user's computer:

- Windows 7 VPN Setup
- Windows 10 VPN Setup

Windows 7 VPN Setup

Creating the Connection

To create a VPN connection on a Windows 7 computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the Connection Option list, select **Connect to a Workplace**.
4. Select **No, create a new connection** if prompted, and then click **Next**.
5. Select **Use my Internet connection**.
6. Enter the server **IP address** or **host name**.
7. Enter a **Destination name** for your VPN connection.
8. Select **Don’t connect now; just set it up** and then click **Next**.
9. Enter your **User name**. Password is not required if you are using certificate for authentication.
10. Click **Create** and then click **Close**.

Configuring the Connection

To configure a VPN connection on a Windows 7 computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. In the left-hand menu, click **Change adapter settings**.

3. Right-click your VPN name and then click **Properties**.
4. On the Networking tab, select **Internet Protocol Version 4** and then click **Properties**.
5. Click **Advanced**.
6. Clear the **Use default gateway on remote network** check box.
7. Click **OK** twice to return VPN Connection Properties dialog.
8. On the Security tab, in the Type of VPN list, select **Point to Point Tunneling Protocol (PPTP)**.
9. Under Authentication, select **Use Extensible Authentication Protocol (EAP)**.
10. In the EAP list, select **Microsoft: Smart Card or other certificate**.
11. Click **Properties**.
12. Under “When connecting” select **Use a certificate on this computer** and then select **OK**.
13. Choose whether to validate the server certificate. When selected, Windows prompts users to confirm that they're connecting to the correct server and that the certificate is valid. If you choose to enable validation, clear the **Connect to these servers** check box.
14. Click **OK** until you return to the Control Panel > Network Connections dialog.
15. Right-click on your VPN name and then click **Connect** to test the connection.

Windows 10 VPN Setup

To create and configure a VPN connection on a Windows 10 computer:

1. Click **Start > Settings**.
2. Click **VPN**, and then click **Add a VPN connection**.
3. Configure the following:

   - For the **VPN Provider**, select **Windows (built-in)**.
   - For the **Connection name**, enter a name of your choice.
   - For the **Server name or address**, enter the server address.
   - For the **VPN type**, select **Automatic**.
   - For the **Type of sign-in info**, select **Certificate**.

   Do not enter a Password. Since you are using a certificate for authentication, It is not required.
4. Select **Remember my sign-in info**, and then click **Save**.
5. Click **Connect** to test the connection

28.8.4 Password Quality Requirements

As an administrator, you can enforce password complexity by setting password complexity rules. The following rules and configuration instructions apply to all system accounts.

Note:
The credit value of each field indicates the requirement of the corresponding item in the password. For example,

- Uppercase credit 0 : Uppercase characters may or may not be included in the password.
- Uppercase credit -2: The password must contain a minimum of 2 uppercase characters.
- Uppercase credit 2: If uppercase characters are included in the password, 2 of these characters will have a length credit assigned, which means, each of these 2 uppercase characters will be counted as 2 characters towards the minimum password length. Additional uppercase characters included in the password will not get this credit and will be counted only as 1 towards the minimum password length. Positive credit for a character does not imply that that character must be included in the password.

The following rules and configuration instructions apply to all system accounts by default:

- **Minimum length**: The password must contain at least 8 characters.
- **Uppercase credit**: Specifies the maximum length credit for having uppercase characters in the password. If less than 0, it is the minimum number of uppercase characters required.
- **Lowercase credit**: Specifies the maximum length credit for having lowercase characters in the password. If less than 0, it is the minimum number of lowercase characters required.
- Digit credit: Specifies the maximum length credit for having digits in the password. If less than 0, it is the minimum number of digits required.
- **Non-alphanumeric credit**: Specifies the maximum length credit for having non-alphanumeric characters in the password. If less than 0, it is the minimum number of non-alphanumeric characters required.
- **Minimum character classes**: Specifies the minimum number of character classes required. The four classes are digits, uppercase, lowercase and non-alphanumeric characters.

Note:
To require 1 character from each class set this value to 4.

- **Maximum class repeat**: Specifies the maximum number of allowed consecutive characters of the same class. The option is disabled if the value is 0.
- **Maximum repeat**: Specifies the maximum number of same consecutive characters allowed. The option is disabled if the value is 0.
- **Character difference**: Specifies the number of characters in the new password that must not be present in the old password during a password change.
- **User real name check**: Checks whether any words, more than 3 characters long, from the account owner's real name (the "User name" field of the account) are contained in the password, in which case the password is not acceptable.
- **Reset non-compliant password**: Forces password change at logon if the password does not comply with the password quality requirements.
- **Forbidden words**: Specifies space separated list of forbidden words (containing more than 3 characters). These are in addition to the words included in the normal cracklib dictionary check.

28.9 Shutdown or Reboot

To shut down, reboot or reconfigure the server:

1. Under **Administration**, click **Shutdown or reboot** in the main menu.
2. Select one of the following actions:
   - **Reboot** - reboots the server after graceful shutdown.
   - **Shutdown** - shuts down the server for service outage or scheduled down time.
3. Click **Perform** and then confirm your selection. Click **Yes** to initiate the action or click **No** to return to cancel the action.

Note:
Each of these functions take several minutes to complete.

28.10 Mitel Virtualization Diagnostics Tool

The intended use of the Virtualization Diagnostic tool is to pinpoint performance and voice quality issues found when running Mitel applications in a virtual environment. The tool is especially helpful for customers who do not have control of the underlying infrastructure but are interested in determining the cause of problems.

The Diagnostic tool is a component of the Mitel Virtualization Framework (MVF) and includes a "Mitel Virtualization" screen that appears within the MSL Server Manager. The screen enables you to obtain an overview of the virtual machine and MVF properties, manage storage monitoring, receive a diagnostic overview, configure a connection to the vCenter server or ESXi hypervisor, and run the diagnostic tool to generate a variety of log files containing statistical, performance and configuration data.

Supported Applications

To employ the Diagnostics tool, you require the following:

- Operating System: MSL 10.0 or higher
- VMware environment: vSphere 4.1 or higher
- Mitel Virtual Framework: MVF 2.0 or higher

Reviewing the Virtual Machine Properties

The "Virtual Machine Properties" table displays information concerning the Virtual Machine and Mitel Virtual Framework. The information is presented in two columns:

- **Current Dimensions**: Lists the configuration at the time that the current Mitel Virtualization page was loaded. Refreshing the page resets the settings.

- **First Boot Dimensions**: Lists the configuration after the Mitel Open Virtual Appliance (OVA) package has been installed and the settings configured, but before the virtual machine has been powered on for the first time.

To review the virtual machine properties:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtual Machine Properties**, review the following settings:

Setting	Description
MVF Version	The version number of the Mitel Virtualization Framework (MVF), a software package that enable Mitel applications to run in a virtual infrastructure. MVF has the capacity to support multiple operating systems and hypervisor products.
Virtualization Agent Version (VMware Tools)	The version number of VMware Tools, a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.
Hypervisor Version	The version number of the VMware ESXi hypervisor that hosts one or more virtual machines and their "guest" operating systems.
vCPU count	The number of virtual Central Processing Units (vCPUs) configured on this virtual machine.
Memory (MB)	The amount of virtual physical memory available for use by the operating system on this virtual machine.
Disk size (GB)	The virtual disk size available for use by the operating system on this virtual machine.
NIC count	The number of virtual network interface cards configured on this virtual machine.
CPU Reservation (MHz)	The guaranteed minimum allocation of CPU resources for this virtual machine.
Memory Reservation (MB)	The guaranteed minimum allocation of memory resources for this virtual machine.
CPU Limit (MHz)	The upper limit of CPU resources that can be allocated to this virtual machine. This limit is expressed in concrete units (Megahertz) and cannot be exceeded.
Memory Limit (MB)	The upper limit of for memory resources that can be allocated to this virtual machine. This limit is expressed in concrete units (Megabytes) and cannot be exceeded.

Setting	Description
vCPU Speed (MHz)	The speed of the virtual CPU, which is dependant on the speed of your underlying processor. So if you have a 12 cores and a processor speed of 3.36GHz, that means a virtual machine with a single vCPU running a single threaded application can consume 3.36GHz. The setting defines what a single vCPU will consume, not the aggregated amount among multiple vCPUs on a single virtual machine. Accordingly, if you have two vCPUs this figure should be doubled.

Managing Storage Monitoring

Use this tool to detect to degrading storage conditions and take corrective actions.

To manage the storage monitoring settings:

1. Under **Administration**, click **Storage Monitoring**.
2. Under **Storage Monitoring**, enter the following settings:

Setting	Description
File System Monitoring	Use this setting to specify whether file system monitoring is enabled or disabled. If the feature is enabled (the default), the system will check for disk I/O errors every five seconds. If any errors are detected, a warning notification is sent to the "admin" email address configured on the Email Settings screen. The following errors are monitored: • File system errors: Errors related to storage degradation • CPU Starvation: When the monitoring process is not dispatched within a specified time (default is 5 seconds), • High I/O Latency: When I/O operations exceed the configured duration time.

Setting	Description
Reboot on Read-Only State	If this setting is enabled (the default), the system will automatically reboot whenever it enters read-only state. After the system reboots, all disk I/O errors will be cleared and the system will be in read-write state. **Note**: • File System Monitoring must be enabled before this feature can be employed.

Setting	Description
	• Read-only state occurs when there are I/O errors on the virtual machine disk drives, and is intended to protect the file system from damage.

3. Click **Save**.

Reviewing the Diagnostic Overview

The Virtualization Diagnostic tool constantly monitors the system in order to report on three alarm conditions and the state of the last nightly analysis.

To review the virtualization diagnostics overview:

1. Under **Administration**, click **Virtualization**.
2. Under **Diagnostic Overview**, review the following settings:

Condition	Description	States
Hypervisor Version	Indicates whether or not the version of VMware ESXi Hypervisor is supported. The Hypervisor is also known as the Virtual Machine Monitor (VMM).	• **Supported** - Your ESXi version is supported and no changes are required. • **Unsupported** - Your ESXi version is not supported and you must switch to a supported version in order to restore monitoring functionality. For example, if you are running ESXi 4.0 or earlier, you must upgrade to version 4.1 or later.

Condition	Description	States
Current Dimensions	Indicates whether the currently configured application resource dimensions are supported.	• **Supported** - Your configuration is supported and no changes are required. • **Unsupported** - Your configuration is not supported due to a setting (vCPU count, Memory, Disk size, or NIC count) being out of boundaries. To resolve any performance issues, do the following: **a.** Revert to the default configuration for your deployment. For details, see Default Configurations. **b.** Contact Mitel Product Support for assistance.
AMC Connectivity	Indicates whether the Virtual Machine can connect to the Mitel Application Management Center (AMC) for licensing purposes.	• **Connected** - Your Virtual Machine can connect to the AMC. • **Error** - Your Virtual Machine cannot connect to the AMC. Check the networking configuration and Application Resource ID (ARID). See the *Mitel Standard Linux Installation and Maintenance Guide* for more information.
Last Nightly Analysis	Indicates the date and time that the last nightly analysis was completed, and whether any problems occurred while it was being run. Upon successful completion, the nightly analysis generates the following log file: NIGHTLY-REPORT-YYYY-MM-DD.txt	YYYY/MM/DD & Problems (if any)

Configuring the Virtualization Diagnostics Credentials

To enable the Virtualization Diagnostics tool to collect statistics for the virtual machine and the host, and then use the statistics to generate log files, you must enter credentials for the vCenter server or ESXi hypervisor.

The information collected depends on the credentials entered:

- Admin login to vCenter - full range of features and statistics.

- Read-only login to vCenter - subset of features and statistics.
- Read-only login to ESXi - subset of features and statistics.
- No credentials - Allocation and Reservation & Limits information only.

Note:
For optimum results, enter credentials for the vCenter. Entering credentials for the ESXi may result in connectivity problems if settings are changed on the hypervisor.

Enter New Credentials

To enter the virtualization diagnostics credentials:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtualization Diagnostics**, enter the following settings:

Setting	Description
FQDN or IP address	Enter the Fully Qualified Domain Name or IP address of the vCenter or ESXi hypervisor.
Username	Enter the username required to access the vCenter or ESXi hypervisor.
Password	Enter the password required to access vCenter or ESX i hypervisor.
Nightly Analysis Time	Specify the one-hour period during which the nightly analysis will be run each day. Select hours between 0-1 and 23-24. Upon successful completion, the nightly analysis generates the following log file: NIGHTLY-REPORT-YYYY-MM-DD.txt.

3. Click **Save**.

Once a connection is established, the system will obtain performance statistics for the virtual machine and the host, and you may click the **Run Diagnostics** button in order to manually generate log files and an online report. For more information, see Manually Generated Log Files.

Note:
For a newly installed system, wait for it to collect statistics for at least 15 minutes before clicking the **Run Diagnostics** button.

Remove Current Credentials

To remove the virtualization diagnostics credentials:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtualization Diagnostics**, click **Remove**.

You may now enter new credentials.

Note:
Without credentials, the system will not collect statistics or generate log files for virtualization diagnostics.

Reviewing the Log Files

The system generates log files containing performance and configuration data plus statistical events.

To view and/or download the log files:

- See View Log Files.

Automatically Generated Log Files

The following log files are generated automatically by the system on a periodic basis.

Report Name	Description
NIGHTLY-REPORT-YYYY-MM-DD.txt	This report contains the previous day's detailed perform ance and configuration information, and is generated dai ly in the Nightly Analysis Time you have specified. The system retains seven reports, deleting the oldest file a fter seven days.
VM-STATS-YYYY-MM-DD.csv	This report contains virtual machine statistics for the previous week. The system polls for new data every 15 minutes and deletes existing data after seven days.

HOST-STATS-YYYY-MM-DD.csv	This report contains host system statistics for the previous week. The system polls for new data every 15 minutes and deletes existing data after seven days.
ALL-CONFIG-YYYY-MM-DD.csv	This report contains all CPU, performance and network configuration statistics concerning the host and virtual machine for the previous week. The system polls for new data every 15 minutes and deletes existing data after seven days.

Manually Generated Log Files

A number of log files are created when you request them.

To manually generate the log files and an online report:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtualization Diagnostics**, click **Run Diagnostics**.

Note:

- For a newly installed system, allow it to collect statistics for at least 15 minutes before you click the **Run Diagnostics** button.
- If you repeatedly click the **Run Diagnostics** button, you may exceed the storage capacity of the host server's hard drive.

Report Name	Description
USER-REPORT-YYYY-MM-DD-HH-MM-SS.txt	This report is similar to the NIGHTLY-REPORT-YYYY-MM-DD.txt report, but contains detailed performance and configuration information for the previous week (rather than a single day), collected from the moment you click the **Run Diagnostics** button. The report file is retained for seven days and then deleted. In the event you cannot resolve a problem by yourself, Mitel Product Support will request that you obtain this log file and send it to them. For details, see View/Download Log Files

Report Name	Description
USER-SUMMARY.tmp	This report is an abbreviated version of USER-REPORT-YYYY-MM-DD-HH-MM-SS.txt report. It contains performance and configuration overviews for each day of the previous week. This report is presented in two formats: • Displayed on the Mitel Virtualization screen. This report is retained until you navigate away from the screen. • Recorded in the log files. This file is retained until the **Run Diagnostics** button is clicked again.
VM-EVENTS-YYYY-MM-DD.csv	The report contains 15 days' activity regarding the operation of the Virtual Machine. This file is retained until the Run Diagnostics button is clicked again.

Log File Contents

Although the log files are primarily intended for use by Mitel Product support, you may use them to troubleshoot basic issues with the following issues:

- **Performance Problems**: The system analyzes performance data and if it detects five consecutive "out of bounds" events, an problem will be reported. For example, if the virtual machine waits longer than two seconds to be serviced by the host, five times in a row, the system will report a "CPU Ready" error. Note that system events are registered every twenty seconds.
- **Configuration Problems**: The system checks configuration data and statistical events on an ongoing basis. If a problem is found, and error is logged immediately.

See Analysis Tuning Parameters for detailed information concerning the system settings which control the generation of log file problems.

Performance Problems	Description
CPU Ready (seconds)	The virtual machine has exceeded the maximum amount of time that it can wait to be run on the physical CPU(s). The default is 2 seconds.
CPU Usage (percent)	The virtual machine has exceeded its CPU capacity limit, which is expressed as a percentage of the total amount available. For example, with a limit of 50%, if the virtual machine has four CPUs with 2 GHz processors, and you are running an application that requires 6 GHz (75% of capacity), the limit has been exceeded by 25%. The default is 50%.
Disk Latency (seconds)	The virtual machine has exceeded the maximum amount of time permitted for a SCSI command to be issued by the guest operating system to the virtual machine hard disk. The default is 0.02.
Network Usage (MB)	The virtual machine has exceeded the maximum network utilization (combined transmit and receive rates, in Megabytes per second). The default is 50.0 MB.

Performance Problems	Description
Memory Swapped (MB)	The virtual machine has exceeded the maximum amo unt of memory, in Megabytes, that can be swapped into memory from disk. The default is 0 MB.
Memory Use (MB)	The virtual machine has exceeded the maximum amo unt of memory capacity that it can use, expressed as a p ercentage of the total amount available. For example, if the virtual machine has 4 GHz of memory, and you are running an application that requires 3 GHz (75% of cap acity), an event will be registered. The default value is 50%.
Number of Packets Dropped (average)	The virtual machine has exceeded the maximum num ber of received packets that can be dropped at the n etwork interface. The default value is 0.
Disk Usage (MB)	The virtual machine has exceeded the maximum amo unt of data, in Megabytes per second, that can be read f rom the virtual machine hard disk. The default value is 30 MB.
Configuration Detections	Description (Yes/No)
High VM-to-host CPU ratio	If "Yes" is displayed, the ESXi host has exceeded the vi rtual CPU to host CPU ratio, which is 0.79 by default. F or example, if five virtual machines with 4 GHz vCPUs ar e powered on, and the host has 8 physical/16 logical cor es, then the ratio is 4 + 4 + 4 + 4 + 4 ÷ 16 = 1.25. Since 1.25 exceeds 0.79, a potential configuration issue is det ected.
High VM-to-host Memory ratio	If "Yes" is displayed, the ESXi host has exceeded the vi rtual memory to host memory ratio, which is 1.20 by defa ult. For example, if five VMs are powered on, each using 2 GHz of memory, and the host has 8 GHz of physical memory, then the ratio is 2 + 2 + 2 + 2 + 2 ÷ 8 = 1.25, which will cause an event to be registered.
Snapshots Present	If "Yes" is displayed, the system checks to determine if snapshots are supported on the virtual machine. Bec ause snapshots create considerable disk I/O load, use of this feature may degrade the voice quality of calls.
Low CPU Speed (MHz)	If "Yes" is displayed, the maximum speed of the virtual CPU, which is dependant on the speed of the underlying processor on the ESXi host, has been exceeded.
No Hyperthreading (Ignore if running on non-Intel proces sor)	If "Yes" is displayed, the system checks to determine if hyperthreading is enabled on the ESXi host. **Note**: This parameter can only report on Intel processors that support hyperthreading. It cannot report on AMD or other non-Intel processors.
vMotion occurred	If "Yes" is displayed, the system checks to determine if vMotion is enabled on the ESXi host.
Low CPU Reservation (MHz)	If "Yes" is displayed, the guaranteed minimum allocation of CPU resources for this virtual machine has been exce eded.

Performance Problems	Description
Low Memory Reservation (MB)	If "Yes" is displayed, the guaranteed minimum allocation of memory resources for this virtual machine has been exceeded.

28.11 Applications

About Remote Access 29

This chapter contains the following sections:

- PPTP Settings (Client-to-Server VPN)
- Configure Port Forwarding
- Configure Syslog
- About SSL Web Server Certificates
- Manage Third-Party Certificates from Let's Encrypt
- Manage Third-Party Certificates from an Alternate Certificate Authority
- Manage Self Signed SSL Certificates
- Manage TLS Protocol
- Certificate Authority Trust

You can access the MiCollabMitel Standard Linux network, either from a computer on the internal network, or from a computer outside the site on the Internet. You can also access the computer network securely from a remote computer.

- PPTP Settings
- Remote Management
- Secure Shell Settings
- Managing Digital Certificates

29.1 PPTP Settings (Client-to-Server VPN)

The Point-to-Point Tunneling Protocol (PPTP) is used to create client-to-server Virtual Private Networks (VPNs).

The IP addresses for PPTP clients are allocated from within the local subnet range managed by the DHCP server. The addresses are taken from the last portion of the range, and the number used depends on the “Number of PPTP clients” that you program.

For example, if you program “10” as the “Number of PPTP clients” for local subnet 192.168.1.10 to 192.168.1.100, then the last ten addresses in the range (.11 to .100) will be allocated to PPTP clients for VPNs.

If necessary, you can increase the total number of addresses available to all clients by modifying the local subnet range. For details see Configure DHCP Server.

VPN access and configuration

To enable VPN access:

1. Under **Security** click **Remote access**.
2. Under **PPTP Settings** in the Remote Access panel, enter the number of individual PPTP clients that will be allowed to connect to the server simultaneously. This can be the total number of remote PPTP

clients in the organization, or, if you have a slow connection to the Internet and do not want all of those PPTP clients to connect at the same time, enter a lower number. Enter 0 to deny PPTP connections.

3. Click **Save**. The server is now ready to accept PPTP connections.

Setting Up a VPN Connection on Clients

Use the following procedures to set up a VPN connection on each user's computer:

Note:
The following procedures outline how to create and configure a VPN connection in Microsoft Windows 7. For instructions to perform these procedures in another operating system, refer to your product documentation.

To create a VPN connection on the user's computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the Connection Option list, select **Connect to a Workplace**.
4. Select **No, create a new connection** if prompted, and then click **Next**.
5. Select **Use my Internet connection**.
6. Enter the server **IP address** or **host name**.
7. Enter a **name** for your VPN connection.
8. Select **Don't connect now; just set it up** and then click **Next**.
9. Enter your **user name**. Password is not required if you are using certificate for authentication.
10. Click **Create** and then click **Close**.

To configure a VPN connection on the user's computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. In the left-hand menu, click **Change adapter settings**.
3. Right-click your VPN name and then click **Properties**.
4. On the Networking tab, select **Internet Protocol Version 4** and then click **Properties**.
5. Click **Advanced**.
6. Clear the **Use default gateway on remote network** check box.
7. Click **OK** twice to return VPN Connection Properties dialog.
8. On the Security tab, in the Type of VPN list, select **Point to Point Tunneling Protocol (PPTP)**.
9. Under Authentication, select **Use Extensible Authentication Protocol (EAP)**.
10. In the EAP list, select **Microsoft: Smart Card or other certificate**.
11. Click **Properties**.
12. Under "When connecting" select **Use a certificate on this computer** and then select **User simple certificate selection**.

13. Choose whether to validate the server certificate. When selected, Windows prompts users to confirm that they're connecting to the correct server and that the certificate is valid. If you choose to enable validation, clear the **Connect to these servers** check box.
14. Click **OK** until you return to the Control Panel > Network Connections dialog.
15. Right-click on your VPN name and then click **Connect**.

Remote Management

Remote management allows hosts on the specified remote IPv4 and IPv6 network(s) to access the server manager of your MSL server. To limit access to the specified host, enter a subnet mask of 255.255.255.255 for IPv4 networks or a CIDR prefix of /128 for IPv6 networks. If your mask allows a range of IP addresses, any hosts within that range can access the server manager using HTTPS. See also Grant Access Privileges to Trusted Local Networks.

To add a remote management network:

1. Under **Security**, click **Remote access**.
2. Scroll to the Remote Management section.
3. In the **Network** field, enter the IP address of the remote host for which you want to allow access.
4. In the **Subnet mask** field, enter a mask to limit the range of access (255.255.255.255 limits access to the specified IP address).
5. Click **Save**.

Secure Shell Settings

About the Secure Shell

Use the Secure Shell Settings section to control access to your server. The public setting should only be enabled by experienced administrators for remote problem diagnosis and resolution. We recommend leaving this parameter set to "No Access" unless you have a specific reason to do otherwise.

Warning:
Before allowing secure shell access to the server using standard passwords, please ensure you set a secure admin/root password on the server. With a weak password, an internet- facing server can be compromised very quickly.

Configuring SSH (Secure Shell)

SSH (secure shell) provides a secure, encrypted way to log in to a remote machine across an IPv4 or IPv6 network, or to copy files from a local machine to a server. Programs such as telnet and ftp transmit passwords in plain, unencrypted text across the network or the Internet. SSH and its companion program SCP provide a secure way to log in or copy files. For more information about SSH Communications Security and its commercial products, visit http://www.ssh.com/.

OpenSSH, included with the MSL server, is a version of the SSH tools and protocol. The server provides the SSH client programs as well as an SSH server daemon and supports the SSH2 protocol.

To configure SSH:

1. Under **Security**, click **Remote access**.
2. Scroll to the Secure Shell Settings section.
3. Select a Secure shell access option:

   - **No Access** – (Default) SSH access not allowed.
   - **Allow access only from trusted and remote management networks** – This option enables you to access the server from local networks and remote management networks. To add a remote management network, see **Remote Management**.
   - **Allow public access (entire Internet)**– This option enables you to access the server from anywhere on the Internet. It is selectable only if you have configured a strong SSH (system admin) password. If you have weak password and attempt to select this option, you will receive the following warning: "The system administration password is set to a weak value. The "Allow public access" option in the form below will remain disabled until the system administration password has been reset to a strong value."
4. Program the configuration options:

   - **Allow administrative command line access over secure shell** - This option allows someone to connect to the server and log in as "root" with the administrative password. The user would then have full access to the underlying operating system. This can be useful if someone is providing remote support for the system, but in most cases we recommend setting this option to No.
   - **Allow secure shell access using standard passwords** - If you set this option to Yes, users will be able to connect to the server using a standard user name and password. This may be a concern from a security point of view, in that someone wishing to break into the system could connect to the SSH server and repeatedly enter user names and passwords in an attempt to find a valid combination. A more secure way to allow SSH access is called RSA Authentication and involves copying an SSH key from the client to the server.
5. Click **Save**.

Once SSH is enabled, connect to the server by launching the SSH client on the remote system. Ensure that it is pointed to the external domain name or IP address for the server. In the default configuration, you will be prompted for your user name. Enter "admin" and the administrative password. You will be in the server console. From here you can change the server configuration, access the Administrator Portal through a text browser or perform other server console tasks.

Note:
By default, only two user names can be used to log in remotely to the server: "admin" (to access the server console) and "root" (to use the Linux shell). Regular users are not permitted to log in to the server.

Obtaining an SSH Client

A number of different free software programs provide SSH clients for use in a Windows or Macintosh environment. Several are extensions of existing telnet programs that include SSH functionality. Two different lists of known clients can be found online at http://www.openssh.com/windows.html and http://www.freessh.org/.

A commercial SSH client is available from SSH Communications Security at: http://www.ssh.com/products/ssh/download.html. Note that the client is free for evaluation, academic, and certain non-commercial uses.

29.2 Configure Port Forwarding

Port Forwarding allows you to modify your firewall rules so that the port you need is opened, and forwarded to another port on another host. This is typically done to provide network services from a server inside of your private LAN, permitting incoming traffic to directly access one of your private hosts.

CAUTION:
Misuse of this feature can compromise the security of your network.

In the Administrator Portal, under **Security**, click **Port forwarding**. On the panel that appears, a table lists the current port forwarding rules.

To create a port-forwarding rule for TCP or UDP traffic:

1. Under **Security**, click **Port forwarding**.
2. Click **Create Port forwarding rule**.
3. Enter the following information:
   - **Protocol**: select either TCP or UDP.
   - **Source Port**: enter the number of the port that is to be forwarded.
   - **Destination Host IP Address**: enter the IP address of the machine to which the traffic on the Source Port is to be forwarded.
   - **Destination Port**: enter the port on the Destination Host to which the traffic is to be forwarded.
   - **SNAT**: select to enable Secure Network Address Translation.
4. Click **Add**.

To remove a port forwarding rule, select the rule from the table of current rules and click **Remove**.

Note:
Port Forwarding is not available in a server-only configuration.

29.3 Configure Syslog

MSL includes a syslog server for message logging. When a system event occurs, such as a failed authentication attempt or login failure, the affected service generates a message which is recorded in a log file. You can examine these messages in the Log File Viewer.

You can enhance this functionality by enabling the local system to accept syslog messages from remote hosts, and by enabling the local system to send its own syslog messages to remote hosts.

Receiving Messages from Remote Hosts

You can configure the local syslog server to accept event messages from other syslog servers, provided that they are in list of trusted networks. The event messages can be received over UDP (using port 514) and TCP (using a configured port).

To start receiving syslog event messages from remote hosts:

1. Under **Security**, click **Syslog**.
2. Under **Accept syslogs from remote hosts**, do the following:

    a. In the **Accept remote syslog on UDP** field, click **Enable**.
    b. (Optional) In the **Accept remote syslog on TCP** field, click **Enable**. In the **Listen Port** field, enter a port number (for example, 514), and then click **Save**.

The local system can now receive syslog event messages from remote hosts.

To stop receiving syslog event messages from a remote host:

1. Under **Security**, click **Syslog**.
2. Under **Accept syslogs from remote hosts**, locate the protocol you wish to disable (UDP or TCP).
3. Click **Disable**.

Sending Messages to Remote Hosts

You can configure the local syslog server to forward its own event messages to one or more other syslog servers.

To start sending local syslog event messages to a remote host:

1. Under **Security**, click **Syslog**.
2. Under **Forward local syslogs**, click **Add remote syslog destination**.
3. In the **Configure syslog** screen, do the following:

    a. In **Facility**, select type of program or subsystem that is logging the message. By default, the **auth** facility code (security/authorization messages) is selected. You may also select **authpriv** (messages generated internally by syslogd) or any other facility code. For a complete list of facility code descriptions, see RFC 3164.
    b. In **Destination Host (ip:port)**, enter the IP address and port number of the remote syslog server.

Note:

- A port number is required only if TCP is selected as the transport.
- You can enter multiple destination hosts, provided that they use the same facility and port number. Use commas to separate the individual entries.

c. In **Protocol**, select the transport, either **UDP** or **TCP**.

4. Click **Next**, and then click **Add**.

The local system will new forward syslog event messages to the designated remote host(s).

To stop sending local syslog event messages to a remote host:

1. Under **Security**, click **Syslog**.
2. Under **Forward local syslogs**, locate the host you wish to disable.
3. Click **Remove** twice.

29.4 About SSL Web Server Certificates

Overview of SSL Web Server Certificates

An SSL web server certificate authenticates the identity of a web site and encrypts information passed between the web server and the web client using Secure Sockets layer (SSL) technology.

A default self-signed SSL certificate is provided with the MSL server at no additional cost. You can instruct remote users to install this certificate in their workstations in order to prevent the “Certificate Error: Navigation Blocked” message from appearing when they attempt to log in to the MiCollabMitel Standard Linux Server Manager.

For enhanced security and ease of use, obtain a signed SSL certificate from a third-party Certificate Authority (CA). Two options are available:

- **Let's Encrypt**: Let’s Encrypt is a free, automated, and open Certificate Authority. It enables you to obtain a valid SSL certificate simply by providing your domain settings and then clicking a button. The acquired certificate is monitored and renewed automatically. This service is supported on single-server, standalone MSL systems that are accessible to the Internet.
- **Other 3rd-Party**: An alternative third-party Certificate Authority issues an SSL certificate upon request, typically for a fee. Companies such as Entrust and GoDaddy provide such services. To obtain a generic SSL certificate, you must first generate a Certificate Signing Request (CSR) on the MSL system and send it to the CA. The CA will then return a package containing your web server certificate, plus any intermediate certificates that are required to maintain the certificate key chain. Optionally, you can download the SSL certificate and private key from the local MSL server, and upload these files to other servers in your domain.

As with the self-signed SSL certificate, a third-party SSL certificate enables remote users to log in to the MiCollabMitel Standard Linux Server Manager without receiving an error message. It also allows MiCollab Mobile Client users to establish connections and receive their deployment configurations.

For more information and programming instructions, see:

- Manage Let's Encrypt Third-Party SSL Web Server Certificates
- Manage Alternate Vendor Third-Party SSL Web Server Certificates
- Manage Self-Signed SSL Web Server Certificates

29.5 Manage Third-Party Certificates from Let's Encrypt

Let’s Encrypt is a free, automated, and open Certificate Authority (CA). It enables you to obtain a valid web server certificate simply by providing your domain settings and then clicking a button. The acquired certificate is uploaded, installed, monitored and renewed automatically. You do not need to generate a certificate signing request (CSR) or go through the manual process of installing the certificate. These steps are handled by the CA and the local MSL server, and are invisible to you.

Note:

- To use this service, the MSL server must be accessible to the Internet, either directly or through a proxy.
- The service is currently not supported on servers under the following deployment configurations:
- Any server behind a MiVoice Border Gateway Web Proxy version earlier than v9.4.
- MiCollab with AWV in server-only (LAN) mode behind a MiVoice Border Gateway in server-gateway mode on the network edge with 2nd WAN IP address configured on the MBG Web Proxy for MiCollab Audio, Web and Video Conferencing if the MBG Web proxy version is earlier than v9.4.0.25.
- The service is supported on any MSL system that meets the following criteria:
- Each FQDN configured in the certificate request must be resolvable from the external Let's Encrypt server.
- An https request to each resolved FQDN above with a URL of the form https://FQDN/.well-known/acme-challenge/CHALLENGE_TOKEN must reach and be responded to by the server on which the Let's Encrypt certificate request has been made.
- When you request an SSL certificate from the Let's Encrypt service, you must provide a Common Name and, optionally, Subject Alternative Names as fully qualified domain names (FQDNs) that are resolvable to addresses on the public network. When the Let's Encrypt servers issue an HTTP request to a resolved FQDN (such as https://mbg.mitel.com/.well-known/acme-challenge/random_file_name), this request must be able to reach the MSL server on port 80 on which the certificate request is being made. Accordingly, the MSL server must be accessible to the Internet, either directly or through a proxy.

Programming Steps

To implement a Let's Encrypt SSL certificate, complete the following procedures:

- Request a Let's Encrypt SSL Certificate
- Modify a Let's Encrypt SSL Certificate (required only if you wish to update your credentials)
- Uninstall a Let's Encrypt SSL Certificate (required only if you wish to resume using the default self-signed certificate)
- Verify the Installed Let's Encrypt SSL Certificate

Request a Let's Encrypt SSL Certificate

To request a Let's Encrypt SSL certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Get Certificate**.
5. Enter the information required to request the SSL certificate from the Let's Encrypt system:

Field Name	Description
Status	Indicates the status of the certificate, either enabled (successfully installed and active) or disabled (not successfully installed and inactive)
Contact E-Mail	Enter the email address of the administrator who Let's Encrypt should contact to deal with issues of certificate recovery or registration.
Common Name	Enter the common name to which you plan to apply your certificate. A web browser checks this field. It is required. The common name must be entered as a fully-qualified domain name (FQDN) that is publicly resolvable. Do *not* enter a domain name with a wild card character (e.g. *.example.com) because Let's Encrypt does not support wild card certificate requests.
Alternate Name(s)	Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied. The FQDNs must be publicly resolvable.

6. Click **Get Certificate**. The Let's Encrypt system generates the certificate and returns it to the MSL system for automatic installation. If there are any problems with the certificate request or installation, an error message is displayed. If there are no problems, the Status field displays "enabled," indicating that the certificate has been successfully installed and is now active.

Modify a Let's Encrypt SSL Certificate

To modify a Let's Encrypt SSL certificate request:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Modify Request**.
5. Update the field values as required in order to modify your certificate signing request (CSR).
6. Click **Get Certificate**. The Let's Encrypt system generates the SSL certificate and returns it to the MSL system for automatic installation. If there are any problems with the certificate request or installation, an error message is displayed. If there are no problems, the Status field displays "enabled," indicating that the certificate has been successfully installed and is now active.

Uninstall a Let's Encrypt SSL Certificate

To uninstall a Let's Encrypt SSL certificate and resume using the self-signed certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Remove Certificate**. The MSL system uninstalls the Let's Encrypt SSL certificate and returns to using the default self-signed certificate.

Verify the Installed Let's Encrypt SSL Certificate

To view details regarding currently installed web server certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. View details at the top of the page:

Field Name	Details
Issuer	Lists the following information for the certificate auth orization company that issued the certificate:
	C: country code
	ST: state or province
	L: locality name (for example: city name)
	O: name of the certificate authorization authority
	OU: name of the organizational unit
	CN: server hostname
	Authority/ emailAddress: email address of the Certificat e Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.

Field Name	Details
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in the certificate.
Valid From	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires. **Note**: Events are raised prior to, and on the date of expiry of the certificate. Ensure to regularly check the event viewer or configure email alerts. • Certificate already expired: **MAJOR** • Expires in less than 1 week: **MINOR** • Expires in less than 3 weeks: **WARNING**

29.6 Manage Third-Party Certificates from an Alternate Certificate Authority

To enable remote client stations to log in and MiCollab Mobile Client users to establish connections, you can purchase an SSL certificate from a alternate third-party Certificate Authority and then import it onto the MSL server.

If you have an MSL application server deployed in LAN mode with an MBG / Web Proxy server in the demilitarized zone (DMZ) or network edge, your remote clients will connect to the MSL server through the MBG / Web Proxy server. For this configuration, purchase an SSL certificate for the MBG / Web Proxy server and then share the certificate and private key file with the LAN-based MSL servers.

If you have MSL application servers deployed in LAN mode behind a corporate firewall, your remote clients will connect to the MSL servers through the firewall. For this configuration, purchase a unique SSL certificate for each MSL server.

Supported Formats

You can import third-party SSL certificates in either PEM or PKCS#12 format:

- **PEM** certificates typically have extensions such as .pem, .crt, .cer, and .key. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format. Apache and similar servers use PEM format certificates. Several PEM certificates, including the private

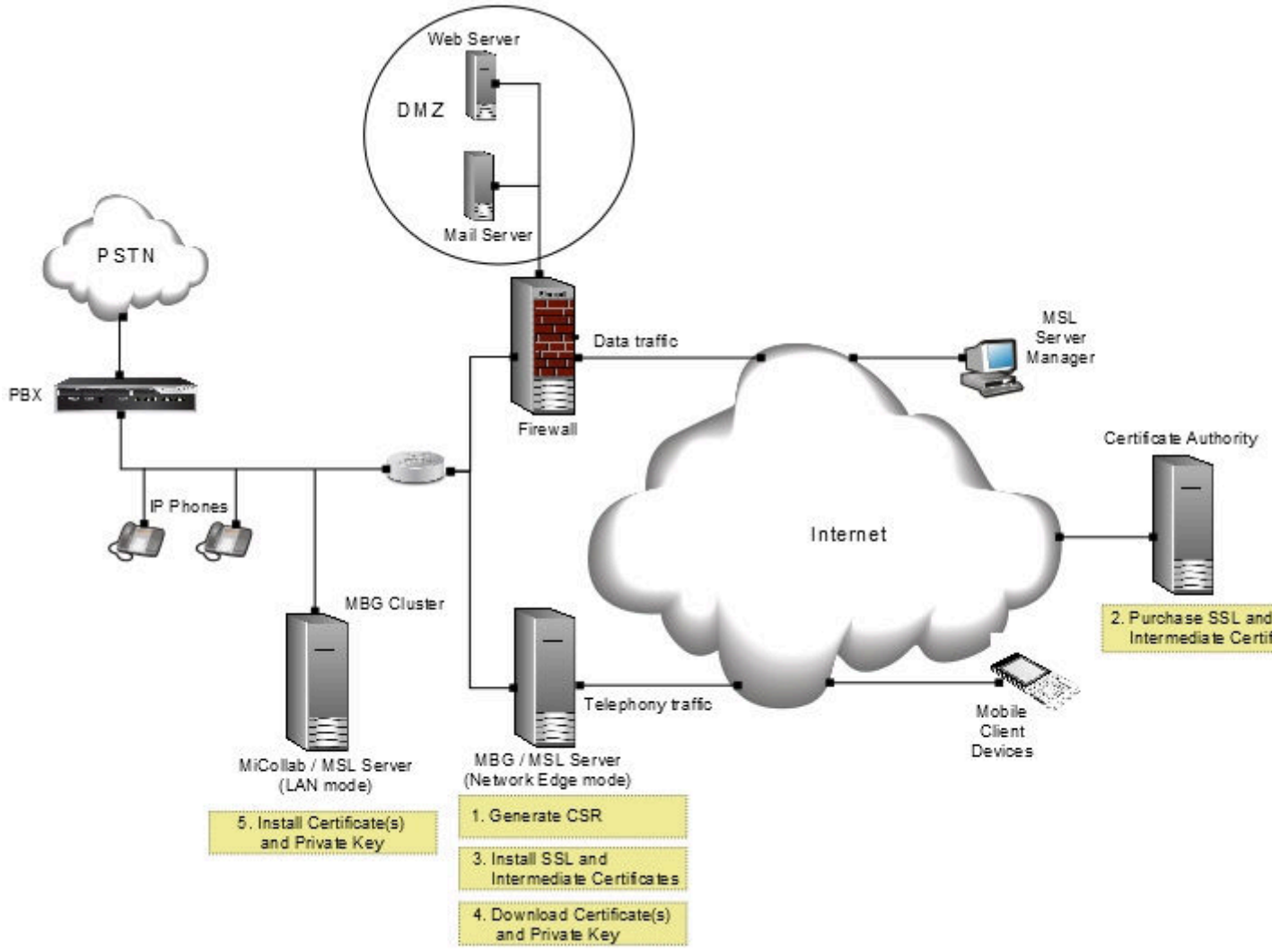
key, can be included in a single file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files.

- **PKCS#12** or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as .pfx and .p12. PFX files are typically used on Windows machines to import and export certificates and private keys.

MSL supports the SHA-2 cryptographic hash function, along with variants such as SHA-256.

Configuration Example

The illustration, below, demonstrates the five basic steps that must be completed to implement a third-party SSL certificate when you have an have an MSL application server in LAN mode with an MBG / Web Proxy on the network edge. First, generate the certificate signing request (CSR) on the MBG / Web Proxy. Second, submit the CSR to the CA, complete the online registration forms and purchase your web server certificate and intermediate certificates. Third, install the certificates on the MBG / Web Proxy (the MSL server that was used to generate the CSR). Fourth, download the certificates and private key from the MBG / Web Proxy. Fifth, install the certificates and private key on the MSL application server on the LAN. The application server can be equipped with Mitel software such as MiVoice Business, MiCollab Client, Open Integration Gateway, Oria or, as illustrated below, MiCollab.



Programming Steps

To implement a third-party SSL certificate, complete the following procedures:

- Generate a CSR and Purchase the SSL Certificate OR Enroll for a web server certificate issued by Enterprise CA using SCEP
- Install the SSL Certificate Files on the MSL Server
- Install the SSL Certificate Files on other MSL Servers (required only if your deployment has LAN-based MSL application servers accessed via an MBG / Web Proxy)
- Uninstall the SSL Certificate (required only if you wish to resume using the default self-signed certificate)
- Verify the Installed SSL Certificate

Enroll for a web server certificate issued by Enterprise CA using SCEP

To automatically enroll for a web server certificate issued by a local Enterprise CA using the Simple Certificate Enrollment Protocol (SCEP), select the Enterprise CA - SCEP Enrollment option.

To enroll for a web server certificate issued by a Enterprise CA using SCEP, do the following:

1. Log into the **MSL Server Manager**.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Enterprise CA - SCEP Enrollment** option.
5. Click **Perform**.
6. Fill out the SCEP form:
   - **CA Address**: the FQDN or IP address of the SCEP server
   - **URI Path**: the URI to use in SCEP communication (defaults to Windows SCEP URI for clients)
   - **Enrollment Password**: the enrollment challenge password if required
   - **Common Name**: the Common Name to use in the Certificate Signing Request (CSR) (defaults to the system hostname)
   - **Alternate Name(s)**: the Subject Alternate Name(s) to include in the CSR
7. Click **Get Certificate**.
8. Upon submitting the form, the data is validated and access to the SCEP server is verified. On successful verification, the SCEP enrollment is initiated to request a certificate, a progress status of the SCEP transaction is provided.
   - If the enrollment request is rejected, check the SCEP server for the details of the failure.
   - If the enrollment request is in pending state, the administrator of the SCEP server needs to approve or deny the certificate request.
9. Reload the MSL server manager for the newly acquired web server certificate to take effect.

Generate a Certificate Signing Request (CSR) and Purchase the SSL Certificate

You need a certificate signing request (CSR) in order to purchase an SSL certificate from an alternate third-party Certificate Authority (CA).

To generate a CSR and purchase the third-party SSL certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Generate a new Certificate Signing Request (CSR)**, and then click **Perform**.
5. Enter the information required to generate a certificate signing request (CSR). If you have previously generated a CSR, the previously entered values are displayed.

Note:
When completing the fields, use first capital letters only (for example Ontario, not ONTARIO).

Field Name	Description
Country Name (two letter code)	Enter the two-letter International Organization for Standardization- (ISO-) format country code for the country in which your organization is legally registered. Examples are, CA for Canada and US for United States.
State or Province Name	Enter the full name of state or province where your organization is located. Do not abbreviate. The first letter of the name entered must be a capital with remaining letters lower case. For example, you would enter "Ontario" for Mitel Corporation.
Locality Name	The Locality Name is the city, town, route used in the mail address of the organization that is submitting the CSR. Enter the full name of the city in which your organization is located. Do not abbreviate.
Organization Name	The Organization Name is the name used in the mail address of the organization / business submitting the CSR. Enter the name under which your organization / business is legally registered. The listed organization must be the legal registrant of the domain name in the trusted certificate request. If you are enrolling as an individual, please enter the certificate requestor's name in the Organization field, and the DBA (doing business as) name in the Organizational Unit field.
Organizational Unit Name	Enter the organization unit or department name. Use this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, you may enter the DBA (doing business as) name in this field.

Field Name	Description
Common Name	Enter the common name for the service to which you plan to apply your certificate. A web browser checks this field. It is required. The common name can be entered as a fully qualified domain name (FQDN) or as a domain name with a wild card character (e.g. *.example.com) in order to generate a wild card certificate request. The default value presented in this field is the FQDN of the server including the domain name (for example, mbg.example.com).

6. Check to ensure that you have entered all the required information correctly before you generate the CSR. If you need to make changes, regenerate the file. Do NOT modify the text of the generated file in a text editor such as Notepad.
7. Click **Generate Certificate Signing Request**. The system generates a CSR file.
8. Copy the text of the CSR file.
9. Access the web site of a Certificate Authority and purchase a certificate. You will be prompted to do the following:

Note:
Each Certificate Authority has unique requirements. Accordingly, you may not be prompted for all of the steps listed below, and some of the field names may vary.

a. Select the number of domains you wish to protect:

- **Single domain**: Select this option if your implementation has one MSL server on a single domain (eg. www.domain.com and domain.com).
- **Multi-domain**: Select this option if your implementation has multiple MSL servers on a specific number of domains (eg. www.domain.com and domain.com, plus three sub-domains).
- **Multi-domain and wildcard**: Select this option if your implementation has multiple MSL servers with a large number of sub-domains (eg. eg. www.domain.com and domain.com, plus an unlimited number of sub-domains).

b. Enter your account and contact details in the CA web form:

- **Login Name** and **Password**.
- **Name**, **Email Address**, and **Telephone Number**.
- **Organization Name and Address**.
- **Domain Name**.

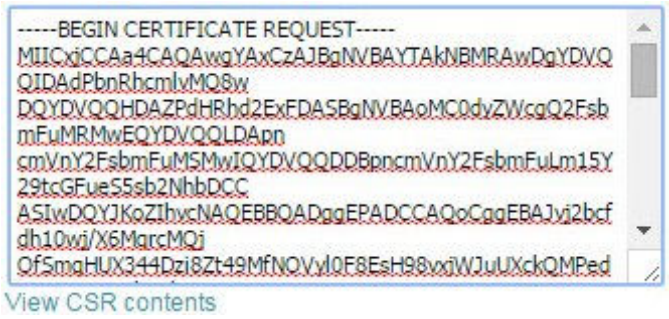
Note:
Some CAs may prompt you to enter the Subject Alternate Names (SANs) or wildcard domain in this step. For more information on these entries, see below.

- **Web Server Software**.

Note:
Select **Apache**. Other options are *not* supported on the MSL platform.

- **Hashing Algorithm**.

c. Paste the text of the CSR file into the CA web form.



d. If you have purchased a certificate for multiple domains or a wildcard domain, enter the following in the CA web form:

- **Subject Alternate Name** (SAN): Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied.

  Note: You can also enter an IP address as a SAN if your users are accessing an MSL application server from the internal network rather than through the MBG / Web Proxy. Typically, you would do this for testing purposes or to enable direct access from the LAN.
- **Wildcard**: To consolidate your domain and unlimited sub-domains into a single SSL certificate, enter a wildcard domain name. For example, if your deployment includes numerous MSL application servers on the LAN (for example, MiCollab, MiVoice Business, MiCollab Client, MiCollab Unified Messaging, generic MSL, and Oria), you can include them all by entering an FQDN such as *.mitel.com.

10. Complete the purchase transaction. The Certificate Authority will do the following:

    - Send you the certificate files.

      These include your SSL server certificate and, if required, intermediate certificates. An intermediate certificate is a subordinate certificate issued to establish a certificate chain that begins at the CA's trusted root certificate, carries through the intermediate and ends with your own SSL server certificate. Some CAs provide a single intermediate certificate while others provide multiple intermediate certificates. There should be no need to open and inspect the files, provided that they are in the correct format and that the intermediate certificates have been bundled into a single file by the CA. Consult the documentation provided by your Certificate Authority for instructions to obtain, unzip and identify exactly which files you need to use.

Note:

- If your CA requires you to open a number of intermediate certificates and assemble them into a single bundled file, perform this task with a text editor that employs Unix line formatting. Do not use an editor that employs Windows line formatting such as Notepad.
- The intermediate certificate is required for MiCollab Mobile Client deployments; without it, client connections will fail and users will be unable to download their deployment configurations.
- Contact the administrator for the domain used in a CSR.

  The administrator is identified using information supplied when your organization originally registered its internet FQDN.

11. Upload the certificate files to a location that is accessible to the MSL server.

Install the SSL Certificate Files on the MSL Server

Use the following procedure to install the certificate files that you received from the alternate third-party Certificate Authority onto the MSL server that generated the CSR. The Upload and install a web server certificate option supports only certificates and keys based on RSA algorithm for upload.

To install the SSL certificate files on the MSL server:

1. Log into the MSL Server Manager for the system that was used to generate the CSR.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Upload and install a web server certificate**, and then click **Perform**.

Note:

This option only supports certificates and keys based on RSA algorithm for upload.

5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the SSL certificate, select it and click **Open**.
6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the Intermediate SSL certificate, select it and click **Open**.

Note:

- In some cases, the CA will provide multiple intermediate certificates. Consult the CA's documentation to determine which of these certificates you should use and, if necessary, how to assemble them into a single bundled file.
- The intermediate certificate is required for MiCollab Mobile Client deployments; without it, client connections will fail and users will be unable to download their deployment configurations.

7. Click **Install Web Server Certificate**. If there is a problem with the certificate chain of trust, MSL will display an error message instructing you to take corrective action. You may need to contact your CA for assistance.
8. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence. Perform this step at a time of low system activity.

Note:
Some services, such as the MiCollab Client Service and WebRTC, are restarted automatically as soon as you install the certificate. This removes the need for you to restart the server manually.

Install the SSL Certificate on other MSL Severs

If your deployment includes LAN-based MSL application servers accessed via an MBG / Web Proxy server, use the following procedure to install the certificate files on them. This is a two-step process. First,

you must download the web server certificate, intermediate certificates (if installed), and private key file corresponding to the SSL server certificate from the MBG / Web Proxy. Second, you must upload these files to the LAN-based MSL servers.

Download certificates

To download the SSL certificate files from the MBG / Web Proxy:

1. Log into the MSL Server Manager for MBG / Web Proxy (the system that was used to generate the CSR).
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Download the current web server certificate**, and then click **Perform**.
5. Click **Save**, navigate to the location you wish to store the file, and then click **Save**. The downloaded file is in ZIP format. It includes the web server certificate, intermediate certificates (if installed), and private key file.
6. Unzip the files and upload them to a location that is accessible to the other MSL servers in your network.

Note:
Exercise caution when transferring your certificate files and private key to the other system. If your private key is stolen, it can be used to establish fraudulent connections to your applications. For optimum security, delete the files from any media they are stored on as soon as you have completed the upload process.

Upload certificates

To upload the SSL certificate files to a LAN-based MSL server:

1. Log into the MSL Server Manager for a LAN-based MSL server.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Upload and install a web server certificate**, and then click **Perform**.

Note:

This option only supports certificates and keys based on RSA algorithm for upload.

5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the SSL certificate, select it and click **Open**.
6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the Intermediate SSL certificate, select it and click **Open**.
7. Import the private key pair created on the other MSL server:
   - Beside the **SSL Private Key** field, click **Browse**.
   - Navigate to the SSL Private Key file, select it and click **Open**.
8. Click **Install Web Server Certificate**.
9. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence. Perform this step at a time of low system activity.

> **Note**:
> Some services, such as the MiCollab Client Service and WebRTC, are restarted automatically as soon as you install the certificate. This removes the need for you to restart the server manually.

10. To prevent fraudulent use of your certificates, delete the certificate and private key files from any media they are stored on.

Uninstall the SSL Certificate

To uninstall SSL certificate and resume using the self-signed certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Uninstall the third-party web server certificate**, and then click **Perform**. The MSL system uninstalls the SSL certificate and returns to using the default self-signed certificate.

Verify the Installed SSL Certificate

To view details regarding currently installed web server certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.

4. View details at the top of the page:

Field Name	Details
Issuer	Lists the following information for the certificate auth orization company that issued the certificate: C: country code ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority OU: name of the organizational unit CN: server hostname Authority/ emailAddress: email address of the Certificat e Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in the certificate.
Valid From	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires. **Note**: Events are raised prior to, and on the date of expiry of the certificate. Ensure to regularly check the event viewer or configure email alerts. • Certificate already expired: **MAJOR** • Expires in less than 1 week: **MINOR** • Expires in less than 3 weeks: **WARNING**

29.7 Manage Self Signed SSL Certificates

A default self-signed SSL certificate is provided with the MSL server at no additional cost. Remote users can add it to their local workstations. This prevents the “Certificate Error: Navigation Blocked” message from appearing when the users attempt to log in to the MiCollabMitel Standard Linux Server Manager.

The self-signed SSL certificate has the following disadvantages:

- The protection supplied by the self-signed SSL certificate is somewhat lower than that of a third-party SSL certificate.
- The self-signed SSL certificate can only be used to prevent the “Certificate Error: Navigation Blocked” message. For MiCollab Mobile Client deployments, you *must* purchase and install a third-party SSL certificate. If you fail to do this, your MiCollab Mobile Client users will not receive their deployment configurations and will be unable to establish connections.

The following procedure applies to Internet Explorer 11. For other browser versions refer to the browser help.

Note:
If you are using Windows Vista or Windows 7, you will need to run Internet Explorer as an administrator to install the security certificate. To do this, right-click the Internet Explorer icon, and select **Run as Administrator**. This task needs to be done even if you are logged in as an administrator.

Install the Default Self-Signed SSL Certificate on Local Workstation

To install the default self-signed certificate on a local workstation:

1. Open Internet Explorer.
2. When you attempt to access the MiCollabMitel Standard Linux Server Manager login page, a "Certificate Error: Navigation Blocked" page is displayed. The warning states "There is a problem with this web site's security service".
3. Click "Continue to this web site (not recommended)".
4. To the right of the domain name address in the address bar, click Certificate Error. The Untrusted Certificate warning appears.
5. Click **View Certificates**.
6. Click **Install Certificate**.
7. In the Certificate Import Wizard, click **Next** to accept the default settings.
8. Click **Place all certificates in the following store** and then click **Browse**. Select **Trusted Root Certification Authorities** and then click **OK**.
9. Click **Next** and then **Finish**. A security warning appears, asking if you want to install the certificate.
10. Click **Yes**. The certificate import is confirmed. Click **OK**.
11. Click **OK** to close the **Certificate** dialog.

Note:
After you have installed the security certificate, a second security certificate error may appear stating that the security certificate presented by the website was issued for a different website's address. This is a temporary problem and the error should be ignored. Click "Continue to this website" to access the Web View interface.

Verify the Installed Default Self-Signed SSL Certificate

To view details regarding currently installed default, self-signed web server certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. View details at the top of the page:

Field Name	Details
Issuer	Lists the following information for the certificate auth orization company that issued the certificate: C: country code ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority; "XYZ Corporation" is the name that appears for Mitel self-si gned certificates. OU: name of the organizational unit CN: server hostname Authority/ emailAddress: email address of the Certificat e Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in this certificate.
Valid From	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires. **Note**: Events are raised prior to, and on the date of expiry of the certificate. Ensure to regularly check the event viewer or configure email alerts. • Certificate already expired: **MAJOR** • Expires in less than 1 week: **MINOR** • Expires in less than 3 weeks: **WARNING**

29.8 Manage TLS Protocol

For MiCollab 8.1 or later, by default, MSL supports the use of TLS v1.1 and v1.2 for communications security. For earlier releases, MSL supports the use of TLS v1.0 by default. To migrate to the latest TLS version, you must upgrade your MiCollab for PC Client and MiCollab for Mobile Client to MiCollab 8.1 or later, and then disable support for the TLS v1.0 protocol using the following procedure. After these steps are complete, your system will be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

Note:

- With MSL 10.6 release and later, new installations have the TLSv1.0 protocol disabled by default. The protocol can still be enabled, if required, from the **Web Server** panel.
- Existing customers have the option to disable the TLSv1.0 protocol from the **Web Server** panel.
- It is not disabled by default on upgrade to MSL 10.6 release.

Disable Support for TLS v1

To disable support for the TLS v1 protocol:

1. Log into the MiCollabMitel Standard Linux Server Manager for a LAN-based MSL server.
2. Under **Security**, click **Web Server**.
3. Click the **TLS** tab.
4. To disable support for TLS version 1.0, clear **Allow TLS v1.0**.

   Your system is now in compliance with PCI DSS.

Note:

- If you disable support for TLS version 1.0, users who employ older web browser such as Internet Explorer 9 or 10 will be denied Server Manager access. To resolve this problem, users should switch to using a newer browser or enable TLS version 1.2 in their existing browsers. In Internet Explorer, the TLS settings are located under Options > Advanced > Security.
- Some services, such as the MiCollab Client Service, are restarted automatically whenever you update the **Allow TLS v1.0** setting. This ensures that the services are updated correctly.

29.9 Certificate Authority Trust

The **Certificate Authority** (CA) **Trust** tab allows the administrator to upload additional root CA certificates, in PEM format, to be added to the list of trusted CA certificates on MSL.

Some customers have their own enterprise root CA certificates, used to sign the certificate that will be installed on the MSL web server. To install a certificate signed by an untrusted CA, the root CA certificate must first be uploaded to and trusted by the server.

To upload a new root CA certificate to the CA trust bundle:

1. In the **Certificate Authority Trust** tab, click **Choose File**.
2. Browse to the location of the certificate, and click **Open**.

> **Note**:
> The certificate must be in PEM format.

3. Click **Install Root CA Certificate**.

By default, the following two Mitel root CA certificates are added to the Trust Store. These are visible in the **Certificate Authority Trust** tab.

- The legacy root CA certificate is named **Mitel Networks Root CA**. This is used to complete a full chain of trust between Mitel legacy equipment and applications such as MBG.
- The new Mitel root CA certificate is named **Mitel Products Root CA** and will be used in new products going forward.

About Integrated Directory Services 30

This chapter contains the following sections:

- Supported IDS Configurations
- Guidelines and Limitations
- Configure MiCollab or MiVoice Business Express System with IDS
- Configure MiCollab IDS for MiVoice MX-ONE
- Configure MiCollab IDS for MiVoice 5000
- Configure Active Directory Authentication
- Manage IDS Connections
- Set Default IDS Attribute Mappings
- Set Custom IDS Attribute Mappings
- Attribute Mappings for Mitel MetaDirectory
- Attribute Mappings for Mitel InAttend (BluStar)
- Disable IDS on MiCollab
- Configure Access to External (Off-board) Directory
- Partitioning the External (Off-board) Directory
- Migrate MiCollab with MiVoice Business IDS to MiCollab IDS
- Migrate MiCollab with MiCollab Audio, Web and Video Conferencing IDS to MiCollab IDS
- Migrate MiCollab with MiCollab Client IDS to MiCollab IDS
- IDS Synchronization Overview
- Scheduling IDS Synchronizations
- Add, Edit and Delete Entries using IDS
- Non-Corporate Contacts
- Teamwork Mode Users
- Partitioning the External (Off-board) Directory
- Add External Numbers
- Viewing IDS Detained Operations
- Managing LDIF Files
- LDAP Query Basics
- Filtering out Disabled AD Users from IDS
- Managing Detained and Failed IDS Operations
- IDS Synchronization Error Handling
- Troubleshooting LDAP Authentication
- Integrating MiCollab Client Database with USP
- Configure MiCollab Settings
- Configure MiCollab Language
- Vidyo Tenant Credentials
- Configure Networks
- Configure E-mail
- Configure DHCP Server
- Configure Server Date and Time
- Add or Delete Hostnames and Addresses

- Manage Domains and DNS Settings
- Configure IPv6 in IPv4 Tunnel
- Configure SNMP Support
- Configure Network Interface Card Settings
- Review Server Configuration
- Support and Licensing
- Panel Requires Upgrade

Integrated Directory Services are supported for the following integrations:

- MiCollab with MiVoice Business
- MiCollab with MiVoice 5000 or MiVoice MX-ONE
- MiCollab with MiVoice Office 250 or Non-Mitel PBX
- Active Directory Authentication
- External Directory Access

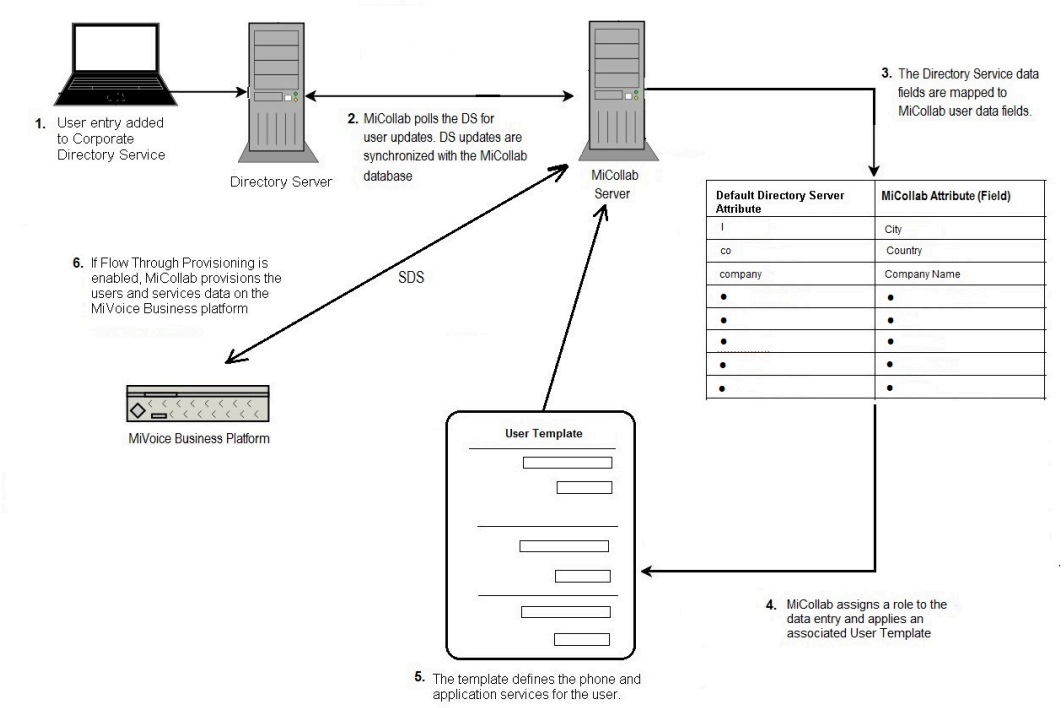
MiCollab with MiVoice Business

You can integrate the user database of a corporate directory service with the MiCollab database to minimize data entry and administration. The user data and MiCollab Client contacts on the corporate directory server are synchronized with the MiCollab database using Lightweight Directory Access Protocol (LDAP). If Flow Through Provisioning is enabled, then MiCollab distributes the user data to the MiVoice Business platforms. Synchronization occurs in one direction only—from the directory server to MiCollab.

On the directory server, you can assign an attribute ("employeeType" by default) to each user data record. The "employeeType" attribute maps to a "role" in the MiCollab database which corresponds to a MiCollab user template. The user template allows you to apply additional personal data, telephone services, and application services to the user entry.

MiCollab detects updates that are made on the directory server via polling. MiCollab polls the directory server on a pre-specified interval or on-demand. Figure 1 illustrates how the directory service data is synchronized with the MiCollab and MiVoice Business.

Figure 8: Directory Service Data Synchronization with MiCollab



If IDS fails to process a directory service update, the operation is sent to the detained queue. Operations in the detained queue can have two states: detained or failed. Detained operations are operation that the system has not yet processed. These only occur if the *detain-all* option is enabled. Failed operations are operations that the system has been unable to process. You manage failed and detained operations from the *Bulk User Provisioning Tool* in the *Users and Services* application.

MiCollab with MiVoice 5000 or MiVoice MX-ONE

For integrations with these communications platforms, Integrated Directory Services supports the provisioning of contacts within the MiCollab Client application so that the contacts appear as entries in the MiCollab Client corporate directory. The contacts from the directory server are provisioned in the MiCollab Client corporate directory so that MiCollab Client users are able to "click-to-call" them. These contacts can be corporate or non-corporate numbers.

- On a site with MiVoice 5000 only, contacts are only synchronized from the directory service in the MiVoice 5000 server.
- On a site with MiVoice 5000 Manager, contacts can be synchronized either from the MiVoice 5000 Manager or from an Active Directory server, but not both.
- On a site with a MiVoice MX-ONE contacts are only synchronized via an Active Directory server.

The contacts are synchronized in one direction only, from the directory service to the MiCollab database. Flow Through Provisioning is not supported.

MiCollab with MiVoice Office 250 or Non-Mitel PBX

For integrations with MiVoice Office 250, or Non-Mitel PBX communications platforms, Integrated Directory Services provisions the MiCollab database with user data and MiCollab Client contacts from the corporate directory server using Lightweight Directory Access Protocol (LDAP).

Data is synchronized in one direction only, from the directory server to the MiCollab database. Flow Through Provisioning is not supported.

Active Directory Authentication

Active Directory authentication is a Windows-based system that authenticates and authorizes users, endpoints, and services to Active Directory. IT teams can use AD authentication to streamline user and rights management while achieving centralized control over devices and user configurations through the AD Group Policy feature.

You can configure the integrations described above with AD Authentication. This feature allows users to log into their MiCollab applications interfaces (for example, MiCollab End User Portal) using their Active Directory server credentials (login name and password). IDS is compatible with AD versions 2016 and 2012 R2. See Configure Active Directory Authentication for details.

30.1 Supported IDS Configurations

IDS is supported for the following configurations:

- MiCollab and MiVoice Business (s) with Flow Through Provisioning
- MiCollab and MiVoice Business (s) without Flow Through Provisioning
- MiCollab and MiVoice Office 250 or Non-Mitel PBX
- Multiple MiCollab Servers and a single MiVoice Business
- Single MiCollab Server and a single MiVoice 5000
- Single MiCollab Server and MiVoice 5000 Network with MiVoice 5000 Manager
- Single MiCollab Server and a single MiVoice MX-ONE
- External Directory Access for MiCollab Client Service

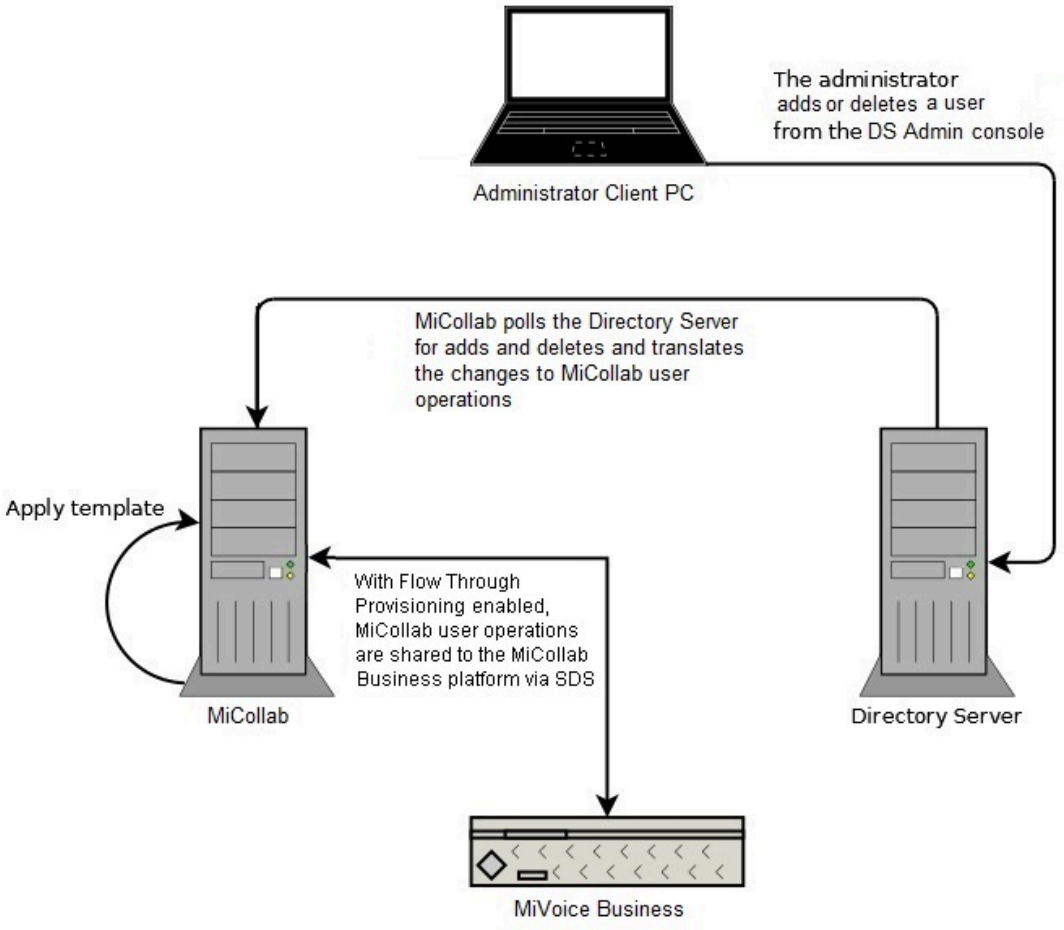
Note:
MiVoice Office 400 does not support an IDS connection to Active Directory.

MiCollab and MiVoice Business (s) with Flow Through Provisioning

If Flow Through Provisioning is enabled to an MiVoice Business system, IDS functions as follows:

1. You create or delete a user entry on the directory service. On the next polling interval all operations collected during the polling process are automatically processed on MiCollab .
2. When operations are processed, the user entries are displayed in the USP directory. If the directory service entry references a role, the corresponding template applies the phone and service data specified in that template to the users and services tabs in USP. If the directory service entry does not reference a role, the operation is sent to the detained queue of the USP Bulk Provisioning Tool.
3. Because Flow Through Provisioning is enabled, the phone services specified in the template are automatically programmed on the MiVoice Business system.

Figure 9: MiCollab and MiVoice Business (s) with Flow Through Provisioning

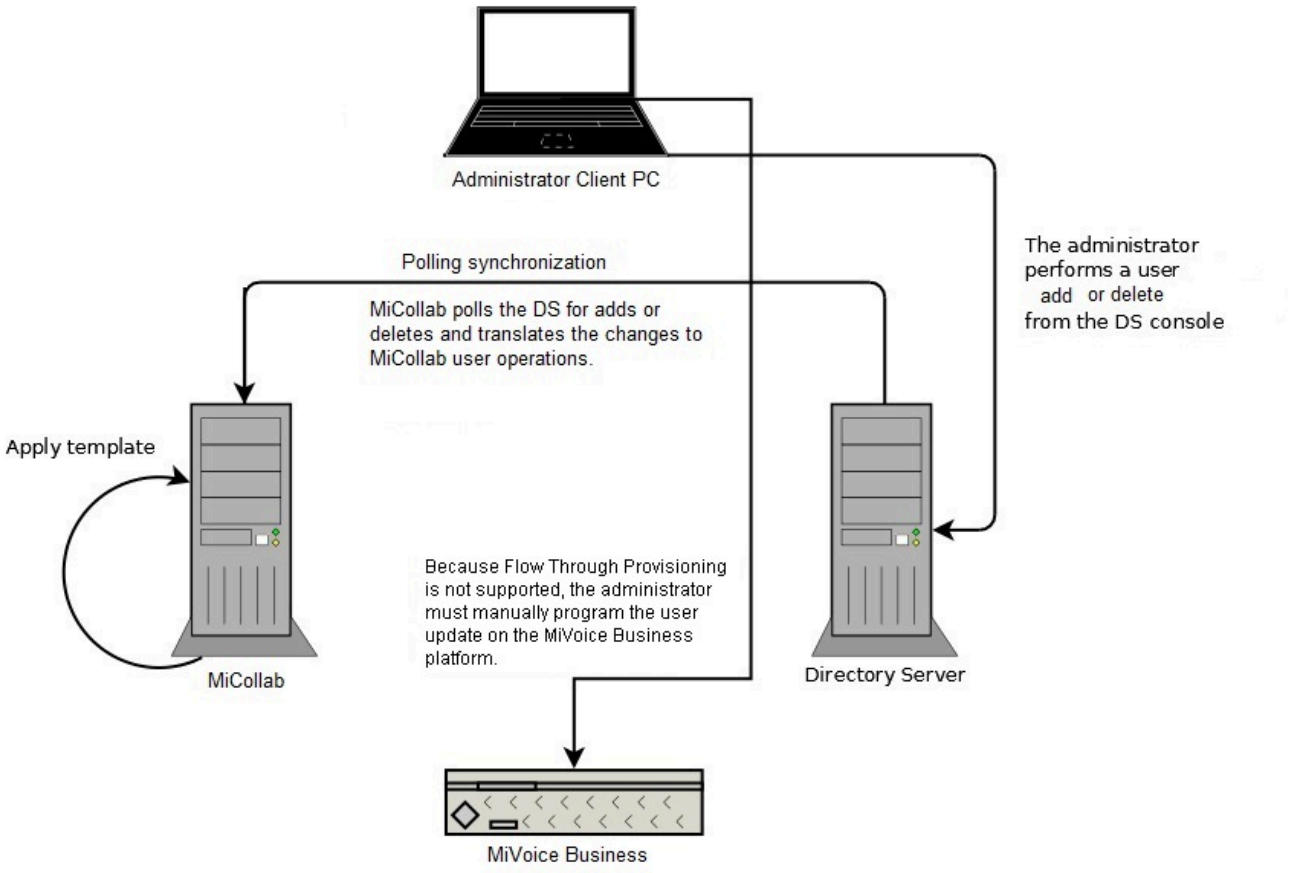


MiCollab and MiVoice Business (s) without Flow Through Provisioning

If Flow Through Provisioning to an MiVoice Business system is **not** enabled on MiCollab , IDS functions as follows:

1. You create or delete a user entry on the directory service. On the next polling interval all operations collected during the polling process are automatically processed on MiCollab .
2. When operations are processed, the user entries are displayed in the USP directory. If the directory service entry references a role, the corresponding template applies the phone and service data specified in that template to the users and services tabs in USP. If the directory service entry does not reference a role, the operation is sent to the detained queue of the USP Bulk Provisioning Tool.
3. Because Flow Through Provisioning is not enabled, the you must manually program the user data and phone services on the MiVoice Business system through the MiVoice Business System Administration Tool.

Figure 10: MiCollab and MiVoice Business (s) without Single Point Provisioning

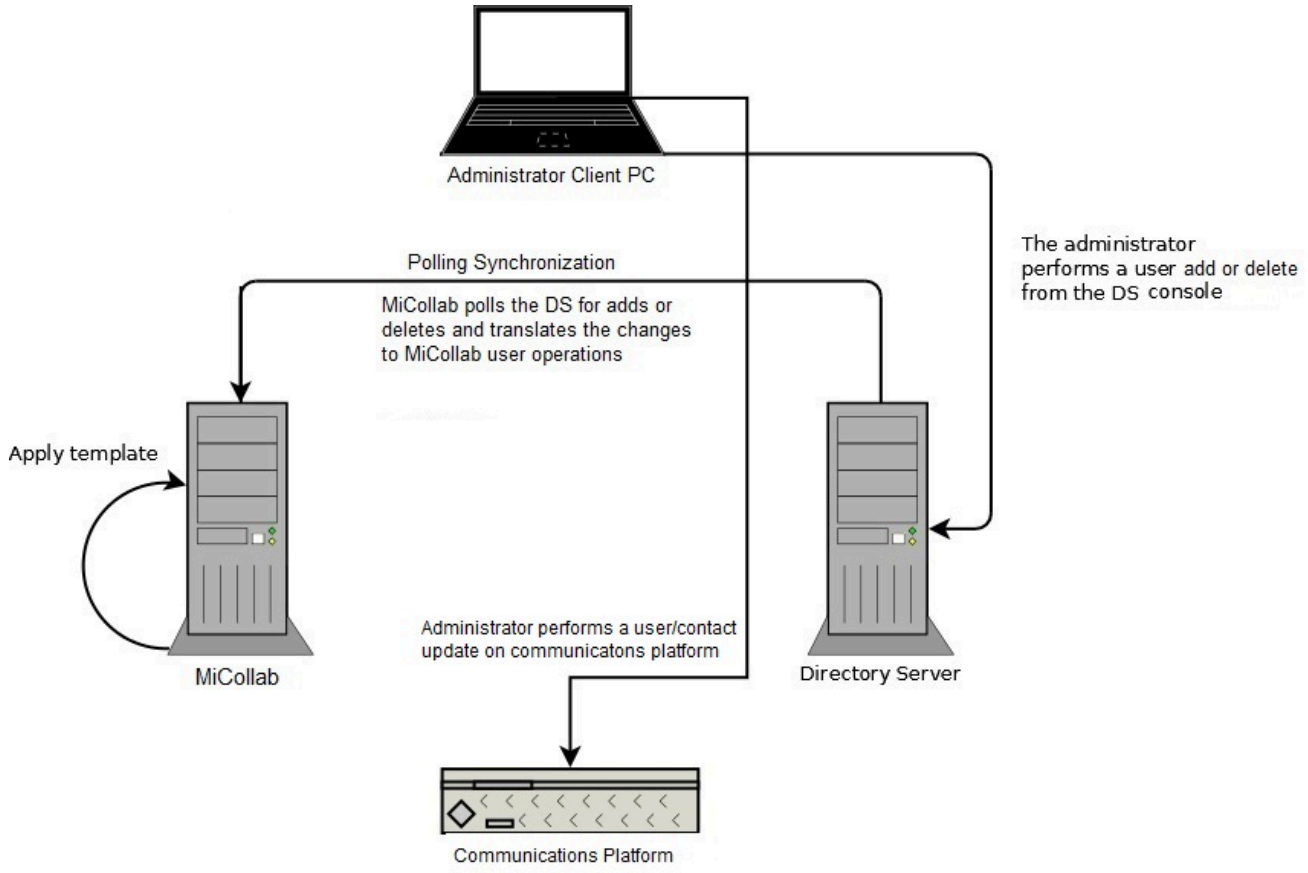


MiCollab and MiVoice Office 250 or Non-Mitel PBX

If MiCollab is deployed with a MiVoice Office 250 or non-Mitel PBX, IDS functions as follows:

1. You create, update, or delete a user/contact entry on the directory service. On the next polling interval all operations collected during the polling process are automatically processed on MiCollab .
2. When operations are processed, the user entries are displayed in the USP directory. If the directory service entry references a role, the corresponding template applies the phone and service data specified in that template to the users and services tabs in USP. If the directory service entry does not reference a role, the operation is sent to the detained queue of the USP Bulk Provisioning Tool.
3. Because Flow Through Provisioning is not supported, you must manually program the user data and phone services on the PBX.

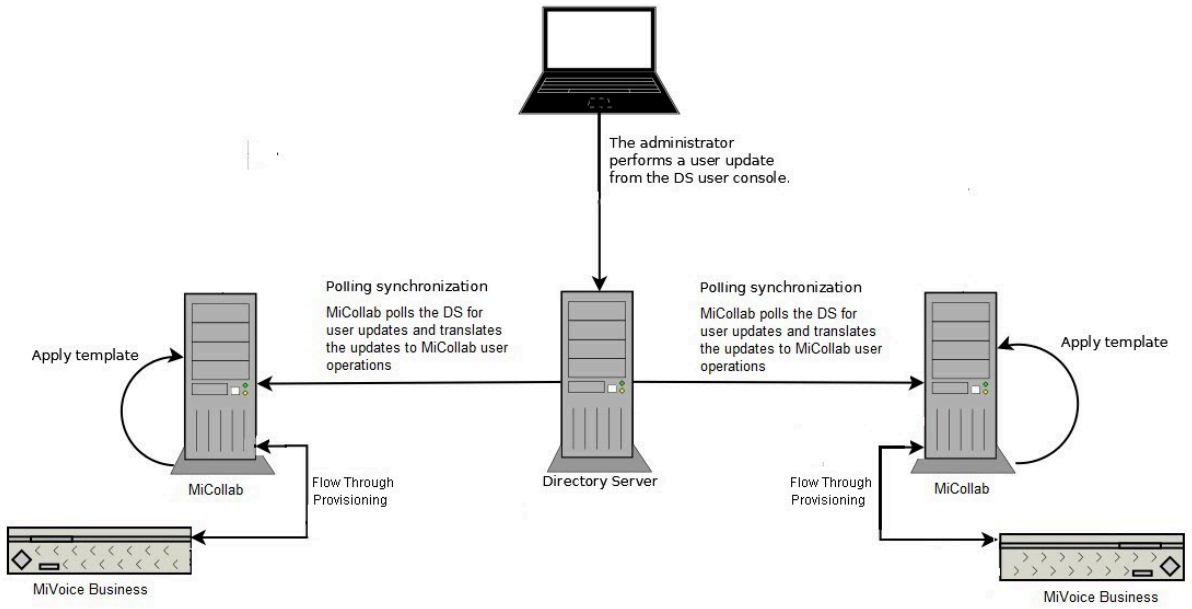
Figure 11: MiCollab and MiVoice Office 250 or Non-Mitel PBX



Multiple MiCollab Systems with Flow Through Provisioning to MiVoice Business

You can deploy multiple MiCollab systems in a network to support load sharing or services segregation among the MiCollab systems.

Figure 12: Multiple MiCollab Servers and Multiple MiVoice Businesses



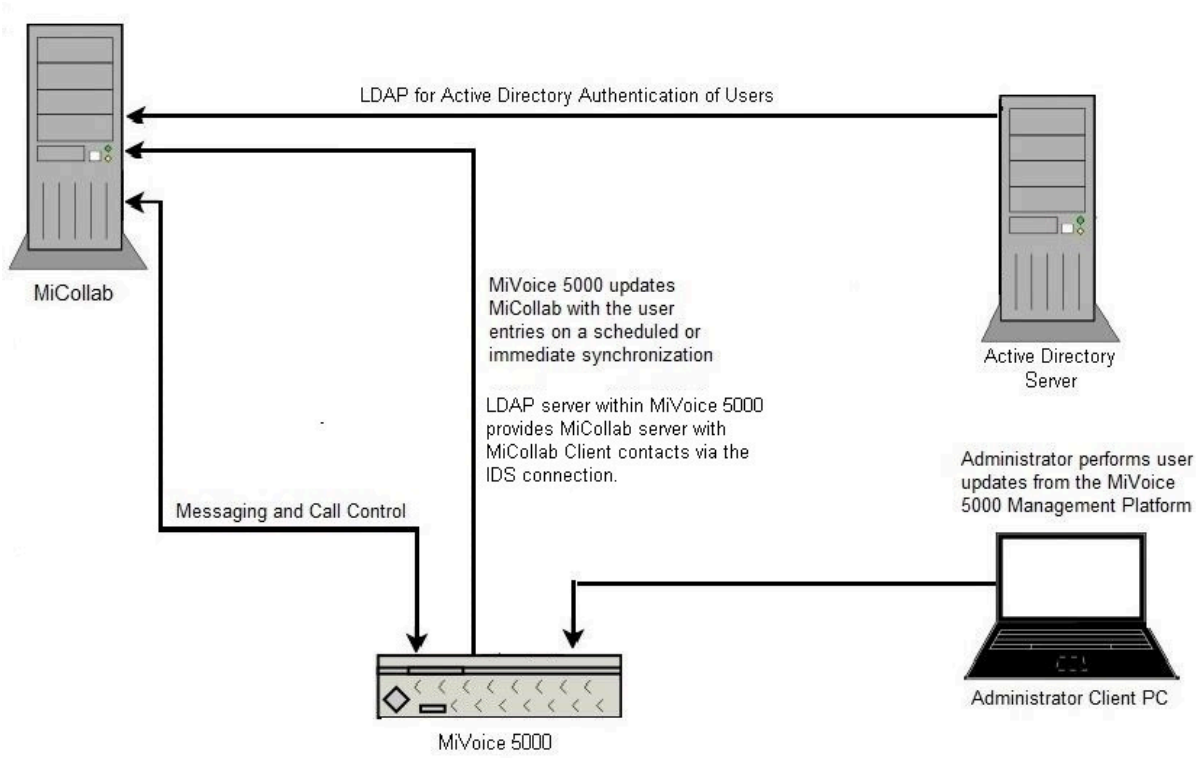
Single MiCollab Server and a Single MiVoice 5000

In this configuration, IDS provides MiCollab Client contact updates and supports Active Directory authentication for MiCollab users.

If MiCollab is deployed with a single MiVoice 5000 , the databases are synchronized as follows:

1. The administrator creates UCC roles and templates on the MiCollab system (or uses the default UCC roles and templates). During an initial synchronization with the MiCollab system, the MiVoice 5000 obtains the roles and templates from MiCollab .
2. After the administrator assigns a role to a user on the MiVoice 5000 , the MiCollab application services specified in the template are applied to the user on the next immediate or scheduled synchronization.
3. The IDS connection updates the MiCollab database with the MiCollab Client contacts from the directory service (within the MiVoice 5000).
4. An optional Active Directory server supports authentication of MiCollab users.

Figure 13: Single MiCollab Server and a Single MiVoice 5000

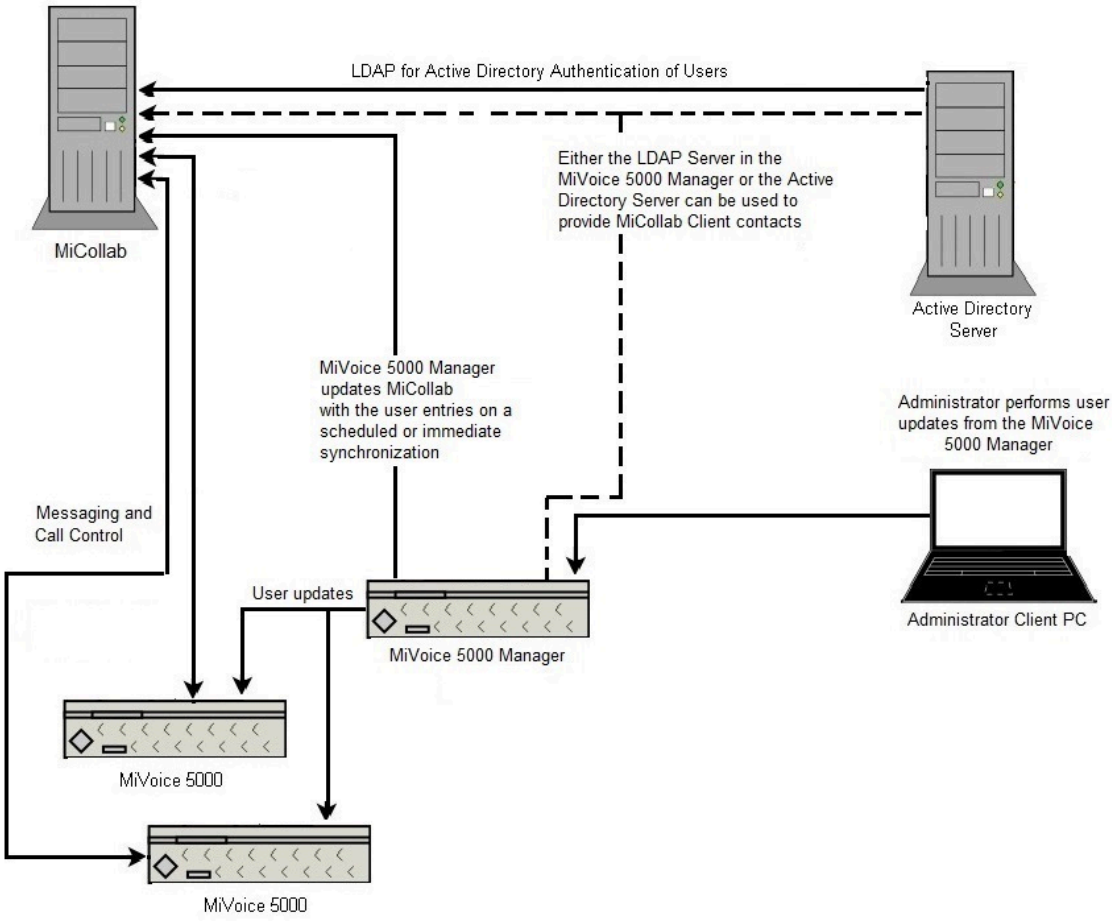


Single MiCollab Server and MiVoice 5000 Network with MiVoice 5000 Manager

In this configuration, IDS provides MiCollab Client contacts to MiCollab and supports the authentication of MiCollab users. If MiCollab is deployed with multiple MiVoice 5000 s the databases are synchronized as follows:

1. The administrator creates UCC roles and templates on the MiCollab system (or uses the default UCC roles and templates). During an initial synchronization with the MiCollab system, the MiVoice 5000 Manager obtains the roles and templates from MiCollab .
2. After the administrator assigns a role to a user on the MiVoice 5000 Manager, the MiCollab application services specified in the template are applied to the user on the next immediate or scheduled synchronization.
3. The IDS connection updates the MiCollab database with the MiCollab Client contacts from either the directory service in the MiVoice 5000 Manager or an optional Active Directory server.
4. An optional Active Directory server supports authentication of MiCollab users.

Figure 14: Single MiCollab Server and Multiple MiVoice 5000 s with MiVoice Manager



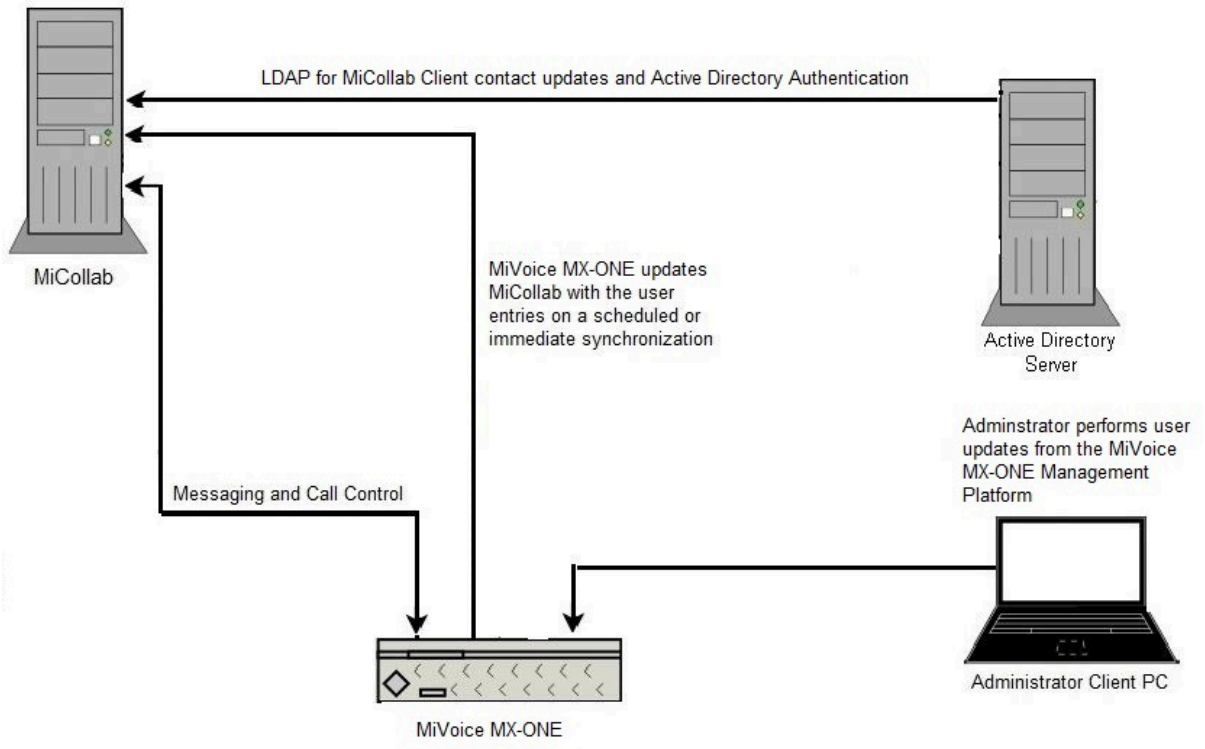
Single MiCollab Server and a Single MiVoice MX-ONE

In this configuration, IDS provides MiCollab Client contact updates and supports the authentication of MiCollab users.

If MiCollab is deployed with MiVoice MX-ONE , the databases are synchronized as follows:

1. The administrator creates UCC roles and templates on the MiCollab system (or uses the default UCC roles and templates). During an initial synchronization with the MiCollab system, the MiVoice MX-ONE obtains the roles and templates from MiCollab .
2. After the administrator assigns a role to a user on the MiVoice MX-ONE , the MiCollab application services specified in the template are applied to the user on the next immediate or scheduled synchronization.
3. The IDS connection updates the MiCollab database with MiCollab Client contacts from the Active Directory server. It also supports authentication of MiCollab users.

Figure 15: Single MiCollab Server and a Single MiVoice MX-ONE



30.2 Guidelines and Limitations

The IDS feature synchronizes the database entries in a corporate directory server with the MiCollab system database. If single point provisioning is enabled on MiCollab, the entries are updated on the MiVoice Business platform. The following guidelines and limitations apply:

General Guidelines

- IDS integration is supported for Active Directory, MiVoice 5000 directory service, MiVoice 5000 Manager directory service, and Generic LDAP servers. IDS connection to the MiVoice Office 400 LDAP server is not supported.

Note:
Generic LDAP support is at the protocol level only.

Note:

The supported versions of Active Directory are 2022, 2019, 2016, and 2012 R2 only.

- Authentication of MiCollab-IDS users is limited to Active Directory.

Note:

Active Directory or LDAP Synchronization is supported by Windows Server.

- MiCollab IDS supports Secure Socket Layer (SSL).
- Do not enable IDS on MiCollab and enable IDS separately for the NuPoint UM SAA, MiCollab Client, or MiCollab Audio, Web, and Video Conferencing applications. These configurations are not supported. IDS must not be running separately on the NuPoint UM SAA, MiCollab Client, or MiCollab Audio, Web, and Video Conferencing applications. In this scenario, MiCollab creates and updates user operations that will fail if the updates were previously processed through the application.
- In order for MiCollab to obtain data from the directory server, you must set up a MiCollab synchronization account (username and password) on the directory server domain with read access.
- From a single MiCollab, you can only create one IDS connection per-directory service domain. Multiple connections from one MiCollab to different directory service domains are supported, however, multiple connections from one MiCollab system to the same directory service domain are not supported. More than one MiCollab system can connect to the same directory service domain.
- Changes made to entries on the directory server are copied to the MiCollab system database. However, changes made in the MiCollab system database are not updated on the directory server.
- Synchronization operations only query the directory server database for changes that have occurred since the last successful synchronization. Full synchronization of all directory server entries with the MiCollab database only occurs on the initial synchronization or if you check the **Re-initialize on next cycle** box in the Manage IDS connections page. Typically this option should only be used to recover the MiCollab database from the directory server. It will most likely result in a large number of detained user updates.
- Ensure telephony fields on the directory server and MiCollab database remain in sync, Data mismatches that occur between telephony fields are not sent to the Managed Detained Queue because they cannot be reconciled from MiCollab. The following telephony fields are ignored during a synchronization update: Home Element, DID Directory Number; Primary Phone Directory Number, and Secondary Phone Directory Number:
- Non-IDS-manageable user service data is applied to a MiCollab entry from a template that is linked to the Role field. A template is applied whenever a new user and device record is added, and whenever new phone service information is added to an existing record. A template is not applied when an existing record that already contains user and phone service information is modified.
- When you create an entry on the directory service, the role and the associated template data is applied to the entry that is added to MiCollab. If you modify a user role on the directory server, it has no

effect on the entry in MiCollab. If you modify an entry on the directory server, the directory update is automatically sent to the detained queue in the Bulk Operating Tool of the USP application

- When you create an entry on the directory service, you must assign a role. Roles are only applied to create operations. If you create an entry without a role, it will be sent to the detained queue.
- The roles specified on MiCollab must match the "employeeTypes" entries on the directory server exactly (case sensitive). IDS cannot reconcile roles if they are different on both the MiCollab and the directory server. If they are different, the entry is sent to the detained queue. Note that the "employeeTypes" is the default directory service attribute mapped to Role. You can customize the attribute mappings (see Manage IDS Attribute Mappings).
- You can configure Active Directory Authentication to allow MiCollab-IDS users to use their directory server credentials (domain login and password) to log into their MiCollab end-user interfaces. In order to support authentication with MiCollab IDS, a Certificate Authority (CA) must be installed on the directory server. If you do not configure Authentication, users on MiCollab are assigned new passwords based upon the assigned role and associated user template.
- When Authentication is enabled, user passwords are maintained on the directory server only. The user password is not stored in the MiCollab database. Therefore, there is no requirement to synchronize user passwords.
- When you add entries from the directory server, any errors that occur on the MiCollab system are not identified in the directory server interface. Errors only appear in the manage detained queue on MiCollab.
- Any non-Mitel PBX phone created in the Users and Services application is distributed to MiCollab Client.

MiVoice Business Specific Guidelines

- IDS is only supported on MiCollab Release 5.0 and later with MiVoice Business Release 5.0 SP1 or later.
- If multiple MiCollab systems are supporting the same MiVoice Business, Flow-Through Provisioning must be enabled on only one of the MiCollab systems.
- MiCollab users can be configured with multiple phones and each phone extension consumes a device (Multi-Device User Group device) on the MiVoice Business system. On a 2500 or 5000-user MiCollab system, it is possible to exceed the device limits of the MiVoice Business system(s). To minimize the possibility of over-provisioning, do not assign users with unnecessary phones. Also, during the initial provisioning of a 2500 or 5000-user MiCollab system, create roles and templates that assign the actual phone requirements for the users. For example, if you have UCC Premium users who only require two phones, create and apply a "UCC Premium - 2 phone" role and template. If you have a MiVB subscription Premier license bundle, which require three phones, create and applu a MiVB SIf you use the default UCC roles and templates, the maximum number of phones are applied, increasing the risk of over-provisioning.
- IDS must not be running separately on any of the MiVoice Business platform(s) that are managed by MiCollab.
- Basic voice mail features are supported for the NuPoint Messenger application. Speech Auto Attendant is not supported. Refer to the MiCollab Installation and Maintenance Guide for a complete list of unsupported features.

MiVoice 5000 and MiVoice MX-ONE Specific Guidelines

- MiVoice 5000 6.1 SP2 or higher is required to support integration with MiCollab Release 7.0 or higher.
- MiVoice MX-ONE 6.0 SP2 or higher is required to support integration with MiCollab Release 7.0 or higher.

- For MiVoice 5000 and MiVoice MX-ONE integrations, the IDS connection is only used to synchronize external and internal contacts (not users). If the IDS connection is via an Active Directory server, the user authentication is also supported.
- You perform user adds, edits, and deletes from the MiVoice 5000 or MiVoice MX-ONE administration interfaces (not from the Users and Services application). The updates can be applied automatically to the MiCollab database on a periodic cycle (scheduled synchronizations) or applied manually if you initiate an immediate synchronization.
- In order to synchronize contacts from Active Directory, create an IDS connection that specifies a query for Active Directory records of type objectClass=contact. In addition, any Active Directory record that has the MiCollab Role of "Contact" is also added to the MiCollab server as a contact record.
- For MiVoice 5000 integrations, a single IDS connection to an Active Directory server can provide both authentication and contact synchronization. In this case, the "Authentication only" box in the "Add a connection to directory server" page is not checked.

Types of MiVoice 5000 and MiVoice MX-ONE Users

- **Users with MiCollab services**: These are users who are assigned MiCollab services. They are provisioned from the MiVoice 5000or MiVoice MX-ONE management interfaces. They have presence monitoring and the functionality provided by MiCollab Client. Typically, a UCC Entry, Standard, or Premium role would is applied during user creation. For this user class, external numbers are not sent to MiCollab Client. End users can provision them in their MiCollab Mobile or Desktop Client.
- **Corporate contacts with monitoring**: Some users may require presence monitoring but not availability or any additional MiCollab services. These users are also provisioned from the MiVoice 5000 or MiVoice MX-ONE management interfaces. Typically these users are created using UCC Basic. For this user class, external numbers are not sent to MiCollab Client. End users can provision them in their MiCollab Mobile or Desktop Client.
- **Corporate contacts without monitoring**: MiVoice Business 5000 and MiVoice Business MX-ONE communications platforms manage more users than a single MiCollab server. To support the click-to-call feature to these non-MiCollab users are added to the MiCollab Client directory as corporate contacts without monitoring. External numbers are sent to MiCollab Client for this user class.
- **Non-corporate contacts**: External contacts are provisioned in MiCollab via a directory services synchronization initiated from MiCollab IDS to either the MiVoice 5000 Manager, MX-ONE Manager Platform, or Active Directory. This synchronization polls the directory and creates updates or deletes contacts as needed in MiCollab Client Service. The external numbers for non-corporate contacts are sent from the directory server to the MiCollab Client Corporate Directory.

30.3 Configure MiCollab or MiVoice Business Express System with IDS

If you are installing a new MiCollab or MiCollab with Voice system on a site with an existing directory service database, use IDS to seed the MiCollab database with the entries from the directory service. After initial configuration, you can manage updates primarily from the directory service. Roles and templates support the configuration of the phone and application services on MiCollab. Single point provisioning automatically applies the user data and phone services to the MiVoice Business system.

To integrate the system database with the corporate directory server database:

1. Review the General Guidelines and Limitations.
2. If IDS is enabled on any MiVoice Business platforms or applications, run a synchronization operation with the directory server to ensure that the MiVoice Business platforms, applications, or both have

the latest updates from the directory server. Refer to *Integrated Directory Services* in the *MiVoice Business System Administration Tool* online help for instructions.

Note:
You must resolve the detained updates from the MiVoice Business on the associated MiCollab. If there are multiple MiCollab systems on site, ensure that you make the required updates on the correct MiCollab.

3. Disable IDS from the MiVoice Business platforms and applications.

   a. To disable IDS on an MiVoice Business system:

      - Log into the MiVoice Business System Administration Tool.
      - Access the Network Element Assignment form and delete the directory server.

   b. To disable IDS (LDAP Integration) for the MiCollab Audio, Web and Video Conferencing application:

      - Click **Audio, Web and Video Conferencing** in the MiCollab server manager.
      - Click **LDAP Configuration**.
      - Clear the **Use LDAP** check box.

   c. To disable IDS (Active Directory/LDAP synchronization) on a MiCollab Client application that is running in integrated mode:

      Note:
      You do not have to disable MiCollab Client-IDS, if MiCollab Client is running in co-located mode.

      - Click **MiCollab Client Service** in the MiCollab server manager.
      - Click **Configure MiCollab Client Service**.
      - Click the **Synchronization** tab.
      - Select **None** and click **Apply**.

4. Create a MiCollab synchronization account on the directory service domain. The account must have read access.
5. If Active Directory Authentication is required, ensure that a valid Certificate Authority (CA) has been configured for Active Directory. If Active Directory Authentication is not required, you assign users new passwords on MiCollab using roles and associated user templates.
6. On the directory server, ensure that the user data fields contain entries for the following attributes: samAccountName, givenName, sn, and distinguishedName. Otherwise, failed update errors are generated on MiCollab during the synchronization. If an employeeType field is not specified the entry is sent to the detained queue.
7. In the MiCollab Users and Services application, create user templates for the various roles in the enterprise. In the templates, assign the phone and application services that you want to apply to the user data that is obtained from the directory server. In the templates, also set a password policy for the user data. You have the option of creating these templates from the UCC default templates.
8. In the MiCollab Users and Services application, create roles that correspond to the employeeType attribute entries on the directory service. You can create these roles from the UCC default roles. Note

that when users are obtained from the directory server, if a user entry has a blank employeeType field, the update is sent to the detained user updates queue.

9. Create a connection to the directory server:

   - Under **Configuration**, click **Integrated Directory Service**.
   - Click **Add connection**. The Add Integrated Directory Service connection page opens.
   - Complete the fields to create a connection. See Manage IDS Connections for field descriptions. At a minimum, you must enter the hostname of the primary directory server, enter the primary directory server username and password, enable **Synchronization**, and then schedule a synchronization interval. It is recommended that you enable the **Defer all operations** option to send all operations to the detained updates queue for the initial synchronization. This option allows you to validate all the updates and then apply or discard updates as required.
   - If Active Directory Authentication is required, the **Synchronization** option must be enabled. Also, set the **Connection Method** to either TLS or TSL/SSL. The **Connection Method** cannot be Unsecured. To use SSL/TLS for IDS, LDAP over SSL must enabled on the active directory server. See the following links for more information:

     - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772393(v=ws.10)?redirectedfrom=MSDN
     - https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
     - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee411009(v=ws.10)?redirectedfrom=MSDN
   - Click **Save**. MiCollab verifies the connection parameters and indicates if any errors are present.

10. Configure Active Directory Authentication if required.

    - Check the **Enable authentication** box beside the desired domain. You can only enable authentication on a single domain. So, if you want to select a different domain, you must first disable the currently selected domain.

    Note:
    Do not enable **Authentication only** for MiVoice Business integrations.

    Note:
    You can connect the Active Directory Authentication to a Global Catalogue on the domain controller. If multiple connections are used, and if those connections point to domains which are under the same forest, you can configure one connection to use the global catalogue. With global catalogue enabled, all users from all connections under the same forest should be able to authenticate. Note that using global catalogue limits the fields that can be used for synchronization.

    - Secure authentication requests are required as part of the IDS connection.
    - Click **Save.**

11. If your server is using the default LDAP attributes, you do not need to modify the IDS Attribute Mappings. If not, clear the **Use default attribute mappings box** and then map the LDAP attributes to

the following IDS attributes: Distinguished Name, First Name, Last Name, and Email. All other fields can have blank LDAP Attributes.

Note:
If you are migrating from MiCollab Client, you must either clear ipPhone attribute from the directory server or enter a different attribute.

12. By default, user service data and Active Directory authentication is synchronized for all users. Specify any user records that you do not want to receive changes from the directory service. To prevent a user record from receiving updates from the directory server:

    - Under **Applications**, click **User and Services**.
    - Locate the user using the **Search** function.
    - On the **User** tab in the **Personal Information** section, clear the **IDS Manageable** box.
    - Click **Save**.

13. Schedule synchronizations with the directory server database to occur on a regular basis during off-business hours (for example: daily at 12:00 am). These re-occurring synchronizations keep the MiCollab database up to date with database changes that are entered on the directory server.

    - Under **Configuration**, click **Integrated Directory Service**.
    - Click Edit next to the directory service connection. The Manage IDS connections page opens.
    - Ensure the **Re-initialize on next cycle** box is clear.
    - In the **Schedule** field, set the schedule using the drop-down menus.
    - Click **Save**.

14. To configure a new MiCollab or MiVoice Business Express system, perform an initial synchronization:

    - Under **Configuration**, click **Integrated Directory Services**.
    - Click the **Sync** link of the connection. The synchronization status is displayed at the top of the screen.
    - At the end of the synchronization, any new users added to the MiCollab USP database are sent a Welcome E-mail. If you configured authentication, the e-mail instructs the users to log into their MAS application interfaces using their directory service credentials

15. To upgrade or reinstall an existing MiCollab or MiCollab with Voice system, perform a full synchronization from MiCollab with the directory server database. Ensure that the **Re-initialize on next cycle box** is enabled. The directory service entries are added to MiCollab.

    - If the directory server and MiCollab system have entries with matching e-mail addresses, the fields in the directory service entry overwrite the fields in the MAS entry.
    - If directory server and MiCollab system have entries with matching login IDs, the fields in the directory service entry overwrite the fields in the MAS entry.
    - If the directory server and MiCollab system have entries with matching e-mail addresses but different login IDs, the fields in the directory service entry overwrite the fields in the MAS entry.

16. After the synchronization is complete, view the IDS Detained Updates in the Bulk Operations Tool and manage the detained updates.
17. If errors are present in the Manage Detained Queue, see Resolve Failed IDS Updates.
18. If single point provisioning is enabled to the MiVoice Business, log into the MiVoice Business System Administration Tool and check the User and Device Configuration forms. Ensure that the required users and phone services have been created in the MiVoice Business database. If single point provisioning is

not enabled or supported for the communications platform, manually update its database with the users and phones services. Use the list of detained updates to identify the required updates.

30.4 Configure MiCollab IDS for MiVoice MX-ONE

If you are installing a new MiCollab system on a site with a directory service database, you can use IDS to seed the MiCollab Client directory with the corporate contacts from the directory service. For single MiVoice MX-ONE system sites, the directory service runs on a separate Active Directory server.

After initial configuration, the MiCollab Client directory receives corporate contacts updates from the directory service during scheduled database synchronizations. You can also use an IDS connection to an Active Directory server to support authentication of users.

Note:
Do not use the IDS connection to Active Directory to create users in MiCollab. Create users from the MiVoice MX-ONE Provisioning Manager first and then synchronize them with the MiCollab database in order keep the data in sync. After you synchronize MiCollab user data (that was created from the MiVoice MX-ONE) from Active Directory, the directory attribute fields will be added to the user.

To configure MiCollab IDS for MiVoice MX-ONE deployments:

1. Review the General Guidelines and Limitations.
2. Create a MiCollab synchronization account on the directory service domain. The account must have read access.
3. If Active Directory Authentication is required, you must create the IDS Connection to an Active Directory server. Ensure that a valid Certificate Authority (CA) has been configured for Active Directory. If Authentication is not configured, you must assign users new passwords from the communications platform.
4. Create a connection to the directory server:
   - Under **Configuration**, click **Integrated Directory Service**.
   - Click **Add connection**. The Add Integrated Directory Service connection page opens.
5. Complete the fields to create a connection. See Manage IDS Connections for field descriptions. At a minimum, you must
   - Select the Directory Server Type.
   - Enter the FQDN or IPv4 Address of the primary directory server
   - Enter the primary directory server username (in DistinguishedName field) and password.
   - If only contact synchronization is required, then check only **Enable synchronization**.
   - If additional attributes are to be mapped to existing users, then check only **Enable synchronization**.
   - If only Active Directory authentication is required, then check only**Enabled Authentication**only.
   - If Active Directory authentication and contact synchronization or additional attributes are required, then check both**Enable synchronization**and**Enable authentication**.
   - Set the **Connection Method** to TLS.

6. Click **Save**. MiCollab verifies the connection parameters and indicates if any errors are present.
7. Configure Authentication for user entries, if required.
8. If your server is using the default LDAP attributes, you do not need to modify the IDS Attribute Mappings. If not, clear the **Use default attribute mappings box** and then map the LDAP attributes to the following IDS attributes: Distinguished Name, First Name, Last Name, and Email. All other fields can have blank LDAP Attributes.

> **Note**:
> Ensure that the contacts on the directory service contain entries in the fields that map to the following IDS attributes: Distinguished Name, First Name, Last Name, and Email.

9. Configure the contacts on the directory server.
10. Schedule synchronizations with the directory server database to occur on a regular basis during off-business hours (for example: daily at 12:00 am). These re-occurring synchronizations keep the MiCollab database up to date with changes that are entered on the directory server.

    - Under **Configuration**, click **Integrated Directory Service**.
    - Click Edit next to the directory service connection. The Manage IDS connections page opens.
    - Ensure the **Re-initialize on next cycle** box is clear.
    - In the **Schedule** field, set the schedule using the drop-down menus.
    - Click **Save**.
11. Perform an initial synchronization:

    - Under **Configuration**, click **Integrated Directory Services**.
    - Click the **Sync** link of the connection. The synchronization status is displayed at the top of the screen.
    - After the synchronization is complete, the contacts from the directory server database are added to the MiCollab Client corporate directory.
    - If you configured authentication, any users with an e-mail address will be sent a Welcome E-mail. The e-mail instructs the users to log into their MiCollab application interfaces using their directory service credentials
12. After the synchronization is complete, view and manage the detained updates from the MiVoice MX-ONE administration interface.

30.5 Configure MiCollab IDS for MiVoice 5000

If you are installing a new MiCollab system on a site with a directory service database, you can use IDS to seed the MiCollab Client directory with the corporate contacts from the directory service:

- For single MiVoice 5000 system sites, the directory service can run on the MiVoice 5000 or on a separate Active Directory server.
- For multi- MiVoice 5000 system sites, the directory service can run either on a standalone Active Directory server or be provided by the MiVoice 5000 Manager.

After initial configuration, the MiCollab Client directory receives corporate contacts updates from the directory service during scheduled database synchronizations.

Note:
Do not use the IDS connection to Active Directory to create users in MiCollab. Create users from the MiVoice 5000 Manager first and then synchronize them with the MiCollab database in order keep the data in sync. After you synchronize MiCollab user data (that was created from the MiVoice 5000) from Active Directory, the directory attribute fields are added to the user.

To configure MiCollab IDS for MiVoice 5000 deployments:

1. Review the General Guidelines and Limitations.
2. Create a MiCollab synchronization account on the directory service domain. The account must have read access.
3. If Active Directory Authentication is required, you must create the IDS Connection to an Active Directory server. Ensure that a valid Certificate Authority (CA) has been configured for Active Directory. If Authentication is not configured, you must assign users new passwords from the communications platform.
4. You can create a connection to the MiVoice 5000 directory service to update the MiCollab database with the MiCollab Client contacts from the directory service (within the MiVoice 5000) and/or create a connection to the Active Directory server to obtain extra attributes. You also have the option of connecting to an Active Directory server to support authentication of MiCollab users.

Note:
You can only use one single set of attribute mappings for the entire system, so you must choose between getting contacts from the MiVoice 5000 or extra attributes from the Active Directory server. You cannot have both.

- Under **Configuration**, click **Integrated Directory Service**.
- Click **Add connection**. The Add Integrated Directory Service connection page opens.

5. Complete the fields to create a connection. See Manage IDS Connections for field descriptions. At a minimum, you must

   - Set the Directory Server Type to "MV5000/MV5000 Manager" for MiCollab Client contacts

     or

     Set the Directory Server Type to "Active Directory" for the additional attributes.
   - Enter the FQDN or IPv4 Address of the primary directory server.
   - Enter the primary directory server username (in DistinguishedName field) and password.
   - For Active Directory authentication select **Enable Authentication**.
   - For additional directory attributes select **Enable Synchronization** for the connection to the Active Directory server.
   - For both Active Directory authentication and extra directory attributes, select **Enable Authentication** and **Enable Synchronization** for the connection.
   - Set the **Connection Method** to TLS.
   - Click **Save**. MiCollab verifies the connection parameters and indicates if any errors are present.
6. Configure Authentication for user entries, if required. The **Enable authentication** check box should not be checked for MiVoice 5000 and Generic LDAP integrations.
7. If your server is using the default LDAP attributes, you do not need to modify the IDS Attribute Mappings. If not, clear the **Use default attribute mappings box** and then map the LDAP attributes to the following IDS attributes: Distinguished Name, First Name, Last Name, and Email. All other fields can have blank LDAP Attributes.

   Note:
   Ensure that the contacts on the directory service contain entries in the fields that map to the following IDS attributes: Distinguished Name, First Name, Last Name, and Email.

8. Configure the contacts on the directory server.
9. Schedule synchronizations with the directory server database to occur on a regular basis during off-business hours (for example: daily at 12:00 am). These re-occurring synchronizations keep the MiCollab database up to date with changes that are entered on the directory server.

   - Under **Configuration**, click **Integrated Directory Service**.
   - Click Edit next to the directory service connection. The Manage IDS connections page opens.
   - Ensure the **Re-initialize on next cycle** box is clear.
   - In the **Schedule** field, set the schedule using the drop-down menus.
   - Click **Save**.

10. Perform an initial synchronization:

    - Under **Configuration**, click **Integrated Directory Services**.
    - Click the **Sync** link of the connection. The synchronization status is displayed at the top of the screen.
    - After the synchronization is complete, the contacts from the directory server database are added to the MiCollab Client corporate directory.
    - If you configured authentication, any users with an email address will be sent a Welcome E-mail. The e-mail instructs the users to log into their MiCollab application interfaces using their directory service credentials
11. After the synchronization is complete, view and manage the detained updates from the MiVoice 5000 administration interface.

30.6 Configure Active Directory Authentication

You can configure Active Directory Authentication to allow MiCollab -IDS users to use their directory server credentials (domain name and password) to log into the following MiCollab end-user interfaces:

- MiCollab End User Portal
- MiCollab Audio, Web and Video Conferencing user login
- MiCollab Client to MiCollab Audio, Web and Video Conferencing collaboration launch (authenticated by MiCollab Audio, Web and Video Conferencing)
- MiCollab Client Thick Windows desktop client
- MiCollab Client Web client
- All currently supported MiCollab Client mobile clients.

The following conditions apply:

- IDS Integration must be configured (enabled) on MiCollab .
- Synchronization is required for Authentication in MiVoice Business integrations.
- Do not enable **Authentication only** in MiVoice Business integrations.
- Periodic synchronizations must be enabled.
- Active Directory authentication is only supported across a single directory service domain.
- The MiCollab domain must be distinguishable from the directory server domain.
- Active Directory authentication is only supported for MiCollab user interfaces; it's not supported for administration interfaces (for example, MiCollab server manager). Also, it is not supported for MiVoice Business user interfaces (for example the MiVoice Business Desktop Programming Tool).
- If Active Directory authentication is configured, users cannot log in with their MiCollab user names and passwords. They must use their directory server credentials.
- Users of the MiCollab End User portal or MiCollab Clients (Desktop Client, Web Client, PC Client, Mobile Client and the Web portal page) cannot change their Active Directory (AD) password. See Change Password Restrictions.
- If connectivity to the directory server is lost, then users will not be able to log into the MiCollab Clients.
- Active Directory v3 authentication is supported.
- If a user does not enter a directory server domain, the system attempts to log the user into the interface using the MiCollab domain.

- To support Active Directory authentication, a MiCollab user must have his or her IDS Manageable option enabled and must be paired with an entry in the directory server. These users will have their password options in the MiCollab applications disabled.
- If you disable the IDS manageable option for a user, Active Directory authentication will cease to function for that user. You must reset the user's password from the USP application. Then send a Welcome E-mail to the user to inform him or her of the password change.
- SMB port 445 must be open from the MSL Server to the SMB File Server.

Note:
If MiCollab Audio, Web and Video Conferencing has previously been configured to use LDAP and is now using MiCollab IDS Users and Services, you must first delete the users from MiCollab Audio, Web and Video Conferencing and create new users under **MiCollab Users and Services**.

- It is not possible to do LDAP authentication with an AD server which uses a certificate with RSASSA-PSS signature algorithm. Renew the CA Certificates to perform the LDAP authentication.

Note:
Active Directory or LDAP Synchronization is supported by Exchange 2019.

Renew and re-issue CA Certificates

1. Renew the certificates.
   - For Root CA:
     a. Remove the alternatesignaturealgorithm=1 line (or change it to 0) in the CAPolicy.inf.
     b. Renew the root CA certificate.
     c. Verify the signature on the certificate to ensure it is RSASHA256.
   - For each Issuing CA:
     a. Remove the alternatesignaturealgorithm=1 line (or change it to 0) in the CAPolicy.inf.
     b. Renew the root CA certificate.
     c. Verify the signature on the certificate to ensure it is RSASHA256.
   - For each certificate template, ensure that you do not enable the option for alternate signature algorithm on the Cryptography tab.
2. Re-issue all affected certificates.

Configuring Active Directory Authentication

1. If you are configuring authentication for a MiVoice 5000 integration:

   - Log into the MiVoice 5000 Management Portal (MMP) or the MiVoice 5000 Manager.
   - Access the **Telephony Service > Subscribers > Terminals and Applications > MiCollab > Connections** menu.
   - Check the **Windows Login for Authentication** box.
2. Log into the MiCollab server manager.
3. Under **Configuration**, under **Integrated Directory Service,** click **Edit** next to the domain. The IDS Connection page opens for the directory server.

   - If a secondary directory server is configured for the domain, authentication requests are automatically directed to the secondary server if the primary is unavailable.
   - Secure authentication requests are required as part of the IDS connection. Set the **Connection Method** to either TLS or SSL. The **Connection Method** cannot be Unsecured.
   - You can only enable Active Directory Authentication on a single domain. Before you can select a different domain, you must first disable the currently selected domain.
4. Check the **Enable authentication** box. Do not check the **Enable authentication** box for MiVoice 5000 and Generic LDAP integrations.
5. Click **Save**. Active Directory authentication does not take effect until after the next periodic synchronization occurs.
6. Click **Sync**.
7. After the synchronization is complete, verify that you can log into a user's End User portal using the user's directory service credentials.
8. The system sends a Welcome Email to all users that you have configured for Active Directory Authentication. The Welcome Email informs the users that they must use their directory server credentials to log into their application interfaces.

Disabling Active Directory Authentication

If you disable Active Directory authentication, users will no longer be able to log into their MiCollab user interfaces using their directory server credentials (domain name and password). You must set a MiCollab temporary replacement password to allow them to log into the MiCollab user interfaces. A user's directory service domain password is not affected by this replacement password.

1. Log into the MiCollab server manager.
2. Under **Configuration**, under **Integrated Directory Service**.
3. Click **Edit** for the desired domain.
4. Clear the **Enable authentication** option.
5. Click **Save**. You are prompted to enter a replacement password for the users.
6. Enter and confirm the password and then click **Save**. A Welcome E-mail which includes the replacement password is sent to the select users.
7. After initial login with this temporary replacement password, users are prompted to change it.

Change Password Restriction

Users of the MiCollab End User portal or MiCollab Clients (Desktop Client, Web Client, PC Client, Mobile Client and the Web portal page) cannot change their Active Directory (AD) password.

There are some situations where an AD password change is enforced by the AD server. Whenever this is the case, users cannot fulfill the request of changing the password from the MiCollab Clients; therefore, they cannot login until they change their password from an Active Directory terminal (for example, from their Windows PC). After their login and password is changed, users are once again able to login via the MiCollab End User portal or MiCollab Client.

The following activities trigger a password change which cannot be automatically resolved from the MiCollab Clients:

- A password lifetime policy which requires the password to be changed within a predefined interval. This is only an issue for the user if the password expires before it is changed on another Active Directory terminals. Windows normally warns a user several days before the password needs to change.
- A new user is created on the AD server and the “User must change password at next logon” is set (see screen below). In this case the user must first log into a terminal which allows a password change.
- The admin resets the password on the AD server and the “User must change password at next logon” option is enabled (see screen below).

30.7 Manage IDS Connections

You add, edit, remove, and synchronize connections between MiCollab and directory server domain controllers to support IDS on MiCollab. The following conditions apply:

- Before you add a directory server connection, ensure that the Integrated Directory Services account is active on the directory server and that you have entered the account User name and Password correctly.
- When you add a new connection, the **Defer all operations** box is checked by default.
- Multiple OUs within the same domain are allowed through one connection:

  For example, to search for objects in the SDS and HR groups,

OU=SDS, OU=RandD, DC=mitel, DC=com; OU=HR, DC=mitel, DC=com;

- Multiple OUs across different domains are **NOT** supported with one connection:

  For example: ou=sales,dc=canada,dc=mitel,dc=com ou=rnd,dc=france,dc=mitel,dc=com
- An IDS connection is locked to one domain.
- Active Directory Authentication can only be enabled for one IDS connection.
- As per the security settings of Microsoft, Port 636 must be used for connection with Active Director server over LDAP.

Note:
LDAPs are not supported in co-located mode.

Note:

If you add more than one MiCollab Server to an active directory server, you must select a different Synchronization schedule. Here the time selected must be in off-hours during lesser traffic on the server.

IDS Connection Examples

- IDS Connection for MiVoice Business with users and contacts synchronized from Active Directory
- IDS Connection for MiVoice 5000 with contacts synchronized from Active Directory
- IDS Connection for MiVoice 5000 with contacts synchronized from a MiVoice 5000 Directory Service
- IDS Connection for MiVoice MX-ONE with contacts synchronized from Active Directory
- IDS Connection for MiVoice 5000 for Authentication only
- IDS Connection for Mitel MetaDirectory
- IDS Connection for Mitel InAttend (BluStar)

Add a Connection

1. Under **Configuration**, click **Integrated Directory Service**.
2. Click **Add connection**. The Add Integrated Directory Service connection page opens.
3. Complete the fields to create a connection. See Add Integrated Directory Services Connection in the table below for field descriptions. At a minimum, you must

   - enter the FQDN or IPv4 Address of the primary directory server
   - enter the primary directory server username (distinguishedName) and password,
   - enable **Synchronization**, and then schedule a synchronization interval.

   It's recommended that you enable the **Defer all operations** option to send all operations to the detained updates queue for the initial synchronization. This option allows you to validate all the updates and then apply or discard updates as required.
4. If Active Directory Authentication is required, set the **Connection Method**. Set the Connection Method to either TLS or TSL/SSL. The **Connection Method** cannot be UnSecured.
5. If desired, partition the MiCollab Client corporate directory.
6. To apply the default attribute mappings, leave the **Use Default Attribute Mappings** box checked. To assign this connection with custom attribute mappings, clear the box and modify the attribute mappings as required.
7. Click **Save**. The system verifies the connection. If the connection fails, an error message is displayed.

Edit a Connection

1. Under **Configuration**, click **Integrated Directory Service**.
2. In the Actions column for the desired domain, click **Edit**. The Integrated Directory Service connection page opens.
3. Edit the fields. See Add Integrated Directory Services Connection in the table below for field descriptions.
4. Click **Save**. The system verifies the connection. If the connection fails, an error message is displayed.
5. If Authentication was enabled, you are prompted to enter a temporary end-user login password to allow users to log in. Enter a temporary password, confirm the password and then click **Save**. The system automatically sends users a Service (Welcome) email with the temporary password.
6. Perform a Full IDS Synchronization. Ensure that the **Re-initialize on next cycle box**is checked when you perform the sync. If you perform a sync with this box unchecked, any existing entries in Active Directory that were not previously synchronized may be skipped.

Remove a Connection

1. Under **Configuration**, click **Integrated Directory Service**.
2. In the Actions column for the desired domain, click **Remove**.
3. Click **Remove**.
4. If Authentication was enabled, you are prompted to enter a temporary end-user login password to allow users to log in. Enter a temporary password, confirm the password and then click **Save**. The system automatically sends users a Service (Welcome) email with the temporary password.

Connection details

Parameter	Description	Default Value
Add a connection	Click to create a connection to a directory service	Not applicable
Manage detained entries (#)	Click to access the Bulk User Provisioning tool in the User and Services application and manage any detained updates. **Note**: The number of detained updates are indicated on the button.	Not applicable
Domain	Read only field that displays the domain name of the MiCollab server	Domain name of the local MiCollab
Last synchronization	Read-only field. Displays the date and time of the last synchronization between the MiCollab IDS client and the directory server. The date and time is obtained from the MiCollab server (MSL).	Time format is day, month, year.

Parameter	Description	Default Value
Status	Indicates the current synchronization connection status. **Created**: The connection has been created. No synchronization have been attempted **Initializing**: The synchronization operation is initializing and has not begun to process user updates. **Started**: The synchronization operation has begun. User updates are being processed. **Stopped**: The synchronization operation has been manually aborted. **Finished**: The synchronization operation has completed.	Not applicable
Summary	Read only summary of the following: • Percentage complete: If a synchronization in progress, this field indicates the progress. • Current synchronization status • Number of update errors	Not applicable
Synchronization enabled	Indicates if periodic synchronization with the directory server is enabled.	Disabled
Authentication enabled Authentication enabled	Indicates if Active Directory Authentication enabled.	Disabled

Parameter	Description	Default Value
Actions	Click the **Edit** link to modify a directory server connection. Click the **Remove** link to remove a directory server connection. Click the **Sync** link to initiate an immediate synchronization operation the directory server. This operation checks for any database changes on the directory server since the previous synchronization and applies the updates to the MiCollab database. After performing a synchronization, click the **Access Detained Updates** link to go to the Bulk User Provisioning tool and manage any failed or detained IDS operations. **Note**: The Action links are disabled while the system is in the process of enabling or disabling Active Directory Authentication for users.	Not Applicable

Add Integrated Directory Service connection

Parameter	Description	Default Value
Directory server type	Select the directory server type: Active Directory, MiVoice 5000 / MiVoice 5000 Manager, Generic LDAP, or ForgeRock Directory Services. The type must be the same for both the Primary and Secondary directory servers.	Active Directory
Primary directory server	Enter the FQDN or IPv4 address of the directory server for the IDS connection. By default, the MiCollab system always connects to the primary directory server during a synchronization operation. **Note**: This is a mandatory field.	Not assigned

Parameter	Description	Default Value
Secondary directory server	Enter the FQDN or IPv4 address of a secondary/backup directory server for the IDS connection. The secondary directory server acts as a backup to the primary server whenever the primary is unreachable. The secondary must be a replica of the primary; otherwise, the synchronization will be problematic. On each interval, the connection always attempts to use the primary server followed by the secondary server. This ensures that the connection reverts to the primary server after the issue has been resolved. **Note**: This field does not apply to MiVoice 5000 or Generic LDAP integrations.	Not assigned
Enable synchronization	Check to allow automatic (scheduled) synchronization with the directory server. The **Enable synchronization** check box should not be checked for MiVoice 5000 or MiVoice MX-ONE.	Disabled
Synchronization Schedule	A set of fields that allow you to schedule synchronizations to occur regularly on a pre-defined time interval. • Select the interval on a per-minute/hour/day/week/month basis from drop-down menus. • Set the time of the synchronization in 24-hour format During a scheduled synchronization, the system checks for any database changes on the directory server since the previous synchronization and applies the updates to the MiCollab database. **Note**: To perform a full synchronization, you must check the **Re-initialize on the next cycle** box.	Daily at midnight 00:00

Parameter	Description	Default Value
Enable authentication	Check to enable Active Directory authentication of end user passwords. To support Authentication, the Enable synchronization option above must also be enabled. **Note**: The **Enable authentication** check box should not be used for MiVoice 5000 and Generic LDAP.	Disabled
Authentication Only	Check to enable Active Directory Authentication of end user passwords **only**. If this box is checked the IDS connection will only support authentication and will not perform any user or contact data synchronization. The 'Authentication Only' check box is not supported for use in a MiVoice Business integration because it disables synchronization and synchronization is the only method for the IDS connection ID and Distinguished Name to be recorded in the database. **Note**: If both Active Directory authentication and user or contact data synchronization is required, check the **Enable authentication** option above and disable this option.	Disabled
Authentication for AD LDS	Check to allow user configuration and to create users through AD LDS. This will cause the authentication to login with the samAccountName only.	Disabled
Skip USNChanged Attribute	Check to enable IDS script to query all users (that are created over multiple ADs) irrespective of whether the users have USNChanged attribute or not.	Disabled
Domain (Domain Name or Connection Name)	For IDS connections that use Active Directory or Generic LDAP, specify the unique domain name used by the directory server. For integrations to Active Directory, the same domain must be used for both the primary and secondary directory server. For IDS connections to the MiVoice 5000 directory service or MiVoice 5000 Manager (AM4750), specify the name of the connection. **Note**: This is a required field.	Blank

Parameter	Description	Default Value
Distinguished name (Directory Server Username)	Every entry in the directory has a distinguished name. The distinguished name uniquely identifies an entry in the directory. Enter the directory server username (in Distinguished name format) required to access the synchronization account on the directory server. Example: • Distinguished Name format – cn=luum, cn= users, dc=ids, dc=com	Blank
Password	Enter the user password required to access the synchronization account on the directory server. All characters are valid, except \ and " and there is no limitation on the password length.	Blank
LDAP port	LDAPS uses its own distinct network port to connect clients and servers. Enter the LDAP port number on the directory server. The default value 636, is the standard LDAP port for secure connection of IDS.	636
Global catalogue port	Global Catalogue (GC) provides a centralized LDAP user view across all domains. The feature provides one connection point for this information. However, the view is limited to a subset of all user attributes. When this option is in use, it reduces the number of fields that are mapped to the MiCollab user records. When a GC LDAP port is specified, only the following user fields are available for synchronization with MiCollab : • telephoneNumber (Prime DN) • ObjectGUID (User ID) • samAccountName (Login) • distinguished name (Domain) • mail (Email) • sn (Last Name) • givenName (First Name) **Note**: If you specify a port for this field, the IDS connections ignore the LDAP port set above. **Note**: This field does not apply to MiVoice 5000 or Generic LDAP integrations.	Blank

Parameter	Description	Default Value
Connection method	Select the security method used to connect to the directory server. The following options are available. This setting determines the level of security in the connection between MiCollab and Active Directory: **Unsecured** - No encryption. **TLS** - Encrypted, LDAP over Transport Layer Security. **SSL** - Encrypted, LDAP over Secure Socket Layer. **Upgraded to Secure (LDAP with start TLS)** **Secure (LDAPS)** Unsecured means that the passwords that are being authenticated between MiCollab server and the Active Directory server are not encrypted and could be read by "sniffing" traffic between them. Note that in the case of the MiVoice 5000, there is no authentication, so passwords, other than the administrator account to log into the MiVoice 5000 directory are not being transmitted. Both TLS and SSL are secure and prevent anyone from easily sniffing the traffic between MiCollab and Active Directory. TLS is the recommended setting. **Note**: • For MiVoice 5000 integrations, this field is disabled and set to Unsecured.	TLS

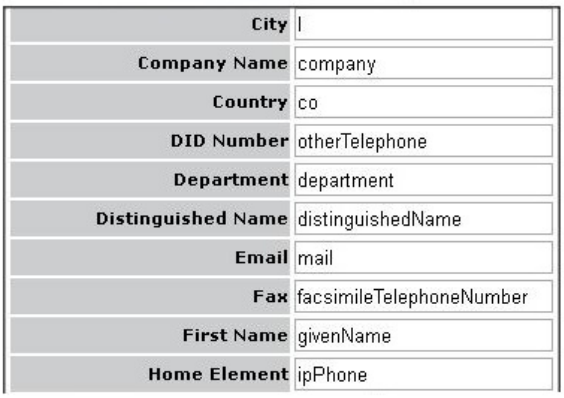
Parameter	Description	Default Value
	• Active Directory supports two methods for establishing an SSL/TLS-protected connection to a DC. The first is to connect a DC on a protected LDAPS port (TCP ports 636 and 3269 in AD DS). The second is to connect to a DC on a regular LDAP port (TCP ports 389 or 3268 in AD DS, and a configuration-specific port in AD LDS), and later sending an LDAP_SERVER_START_TLS_OID extended operation [RFC2830] **Note**: For MiVoice 5000 integrations, this field is disabled and set to Unsecured. **Note**: Active Directory supports two methods for establishing an SSL/TLS-protected connection to a DC. The first is to connect a DC on a protected LDAPS port (TCP ports 636 and 3269 in AD DS). The second is to connect to a DC on a regular LDAP port (TCP ports 389 or 3268 in AD DS, and a configuration-specific port in AD LDS), and later sending an LDAP_SERVER_START_TLS_OID extended operation [RFC2830]. Regardless of the means by which an SSL/TLS-protected connection is established, the IDS client performs a bind using the credentials configured against the connection before searching the directory.	

Parameter	Description	Default Value
	Determines the level of security in the connection between MiCollab and Active Directory. Choose from: • **Unsecured**: Provides no encryption, leaving passwords vulnerable to interception if traffic is sniffed between MiCollab and Active Directory. MiVoice 5000 does not perform any authentication besides the administrator account for logging into the MiVoice 5000 directory. • **TLS (Transport Layer Security)**: TLS encrypts the connection, securing LDAP communications. • **SSL (Secure Socket Layer)**: SSL encrypts the connection, ensuring security for LDAP communications. • **Upgraded to Secure (LDAP with Start TLS)**: Enhances security by upgrading the connection to secure LDAP using Start TLS. • **Secure (LDAPS)**: Used when transitioning from unsecure to secure LDAP during Microsoft security changes. LDAPS should be selected when using the default LDAP port 636. LDAP over TLS can also employ port 389 for a secure connection but requires a certificate to be added to domain controllers. **Notes**: • For MiVoice 5000 integrations, this field is disabled and set to Unsecured. • Active Directory supports two methods for establishing an SSL/TLS-protected connection to a Domain Controller (DC): connecting to a DC on a protected LDAPS port (TCP ports 636 and 3269 in AD DS) or connecting to a DC on a regular LDAP port (TCP ports 389 or 3268 in AD DS) and initiating an LDAP_SERVER_START_TLS_OID extended operation [RFC2830]. • Regardless of the method used to establish an SSL/TLS-protected connection, the IDS client performs a bind using the configured credentials against the connection before searching the directory.	

Parameter	Description	Default Value
Default query string	Enter the default query string used for filtering LDAP searches. **Note**: The Active Directory default setting processes all user accounts and contact records. The MiVoice 5000 default setting processes all internal and external contact records.	Active Directory defaults to |(ObjectClass=user) (ObjectClass=contact) MiVoice 5000 directory service and MiVoice 5000 Manager (AM7405) defaults to (ObjectClass=peopleRecord) (ObjectClass=contactRecord) Generic LDAP defaults to (ObjectClass=person)
Search scope	The Search scope determines the set of directory server data that is applied to MiCollab database during a synchronization event. Select one of the following: • **Sub-tree** : include all child objects as well as the base object. • **Object**: limit the search to the base object. The maximum number of objects returned is always one. • **One level**: limit the search to the immediate children of a base object, but exclude the base object itself. **Note**: This field does not apply to MiVoice 5000 integrations.	Sub-tree
Query page size	Enter the maximum page size of the LDAP search. The permitted range is 100 to 1000 records per page. **Note**: This field does not apply to MiVoice 5000 integrations.	400
Chase LDAP referrals	If the directory server does not hold the target requested by an LDAP search, it will return a referral message that redirects the MiCollab client to another directory server. Check the box to act on the referral message or clear the box to ignore it. **Note**: This field does not apply to MiVoice 5000 integrations.	Disabled

Parameter	Description	Default Value
Search context	Enter the distinguished name of the default location used to search objects on the directory server. If there are multiple locations, use semi-colons to separate the entries. For example, to search for objects in the SDS and HR groups, enter: OU=SDS, OU=RandD, DC=mitel, DC=com; OU=HR, DC=mitel, DC=com; Leave the field blank to begin the search at the domain root container.	Blank
External Search	Check this box to select this connection for use with an external search database, for example Mitel Metadirectory. See Configure Access to External Directory for details.	Unchecked for Active Directory, MiVoice MX-ONE, MiVoice 5000, or MiVoice 5000 Manager server types. Checked for Generic LDAP server type.
External search base	Enter the name of the external search database. The MiCollab Client searches this database when a MiCollab Client user looks up a corporate contact. **Note**: For external search on Active Directory, multiple OUs in the external search base field is NOT supported.	Blank
External search query string	Enter a query string to narrow the search criteria and reduce the number of results from the external directory search, for example: "objectClass=person".	Blank
Public Line Prefix	Public line prefix is the trunk prefix that will be replaced in the number before external lookup and external reverse lookup. For example: 0, 9 (In Nordic countries) etc.	Blank
International Dialing Prefix	International dialing prefix is the international call prefix that will be replaced in the number before external lookup and external reverse lookup. For example: 00, 011, 010, 0011, 810 etc.	Blank
Partition search attribute	Select the IDS mapping attribute that you want to use to partition the directory. See Partition the Corporate Directory for details.	Blank

Parameter	Description	Default Value
Partition method	Select organizational unit to partition the directory based on groups (Organizational unit) or across the entire LDAP directory (Attribute).	Organizational unit or Attribute. Default is Organizational unit.
Enable reverse lookup	Enable reverse lookup resolves number to name at call-to or call-from an external number. **Note**: Lookup/Reverse lookup is not supported if conference call is between external users. Check to enable LDAP reverse lookup function. Before performing the external reverse lookup, MiCollab Client server will replace the two parameters, that is publicLinePrefix and internationDialingPrefix from the searched string. If any of the prefix is found, then the best match is found otherwise an exact match happens.	Unchecked for Active Directory. Checked for Generic LDAP server type.
Dial Digit Count	Dial Digit Count is enabled when the Enable Reverse lookup parameter is checked. The configuration parameters, publicLinePrefix and internationDialingPrefix will not work with Dial Digit Count. If any one of the parameter is configured then the dial digit count setting will get disabled. Prefix settings will override the dial digit count setting.	-
Remove leading digits count	It is used to strip as many digits as configured before lookup. Enter the number of leading digits to be removed in the LDAP search. **Note**: **Removing leading digits count** field is applicable only for reverse lookup functionality and NOT for external search.	0
Re-initialize on next cycle	This option effectively forces a full synchronization on the next scheduled sync event. A full synchronization queries the directory server for the entire set of users. This option can be used to recover the MiCollab database from the directory server. It will most likely result in a large number of detained user updates.	Unchecked

Parameter	Description	Default Value
Defer all operations	When synchronization occurs the system automatically sends all operations to the detained updates queue. Use this option if you want to preview the synchronization updates in the detained updates queue. From the queue, you can view, apply, modify, or cancel (delete) the updates as required. See Resolving Detained and Failed Updates for instructions.	Checked
Use Default Attribute Mappings	By default, this box is checked and the default attribute mappings are applied to a new connection. Note that you can set the default settings (see Set Default IDS Attribute Mappings). **Note**: In case of ForgeRock Directory Services, the Use Default Attribute Mappings box should be unchecked.  To use custom settings, clear the check box and enter the required attributes. See Set Default IDS Attribute Mappings for a description of the attribute fields.	

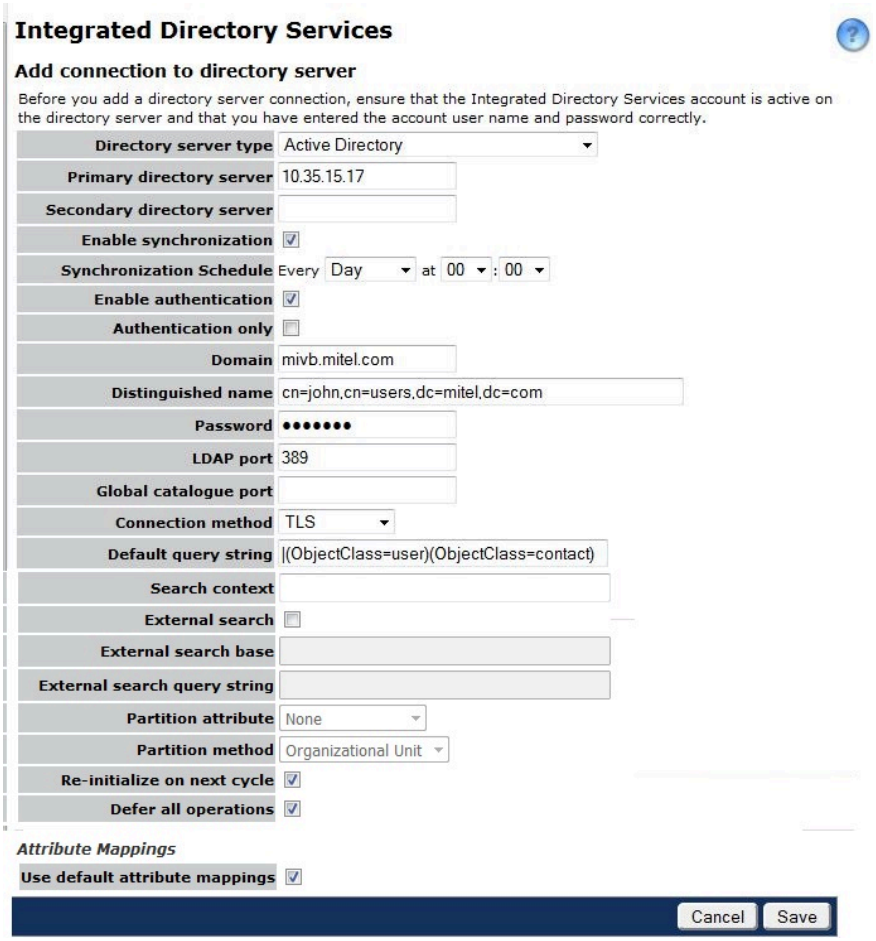
30.7.1 IDS Connection for MiVB Users and Contacts from Active Directory

You can use an IDS connection to synchronize MiVoice Business users and contacts from an Active Directory server, and to provide Active Directory authentication of MiCollab users.

- To synchronize users and contacts from the Active Directory server, create an IDS connection that specifies a query for records of type |(ObjectClass=user)(ObjectClass=contact). In addition, any MiVoice Business record that contains the MiCollab "Contact" role is also added to the MiCollab server database as a contact record.
- To synchronize users only from the Active Directory server, create an IDS connection that specifies a query for records of type: (ObjectClass=user).
- To enable Active Directory authentication of MiCollab users, check the **Enable authentication** box.

Below is an example of the IDS Connection settings required to synchronize users and contacts from an Active Directory server with authentication enabled:

Figure 16: IDS Connection for MiVB Users and Contacts from Active Directory



30.7.2 IDS Connection for MiVoice 5000 Contacts from Active Directory

You can use an IDS connection from an Active Directory server to synchronize contacts (not users) and to provide authentication of MiCollab users.

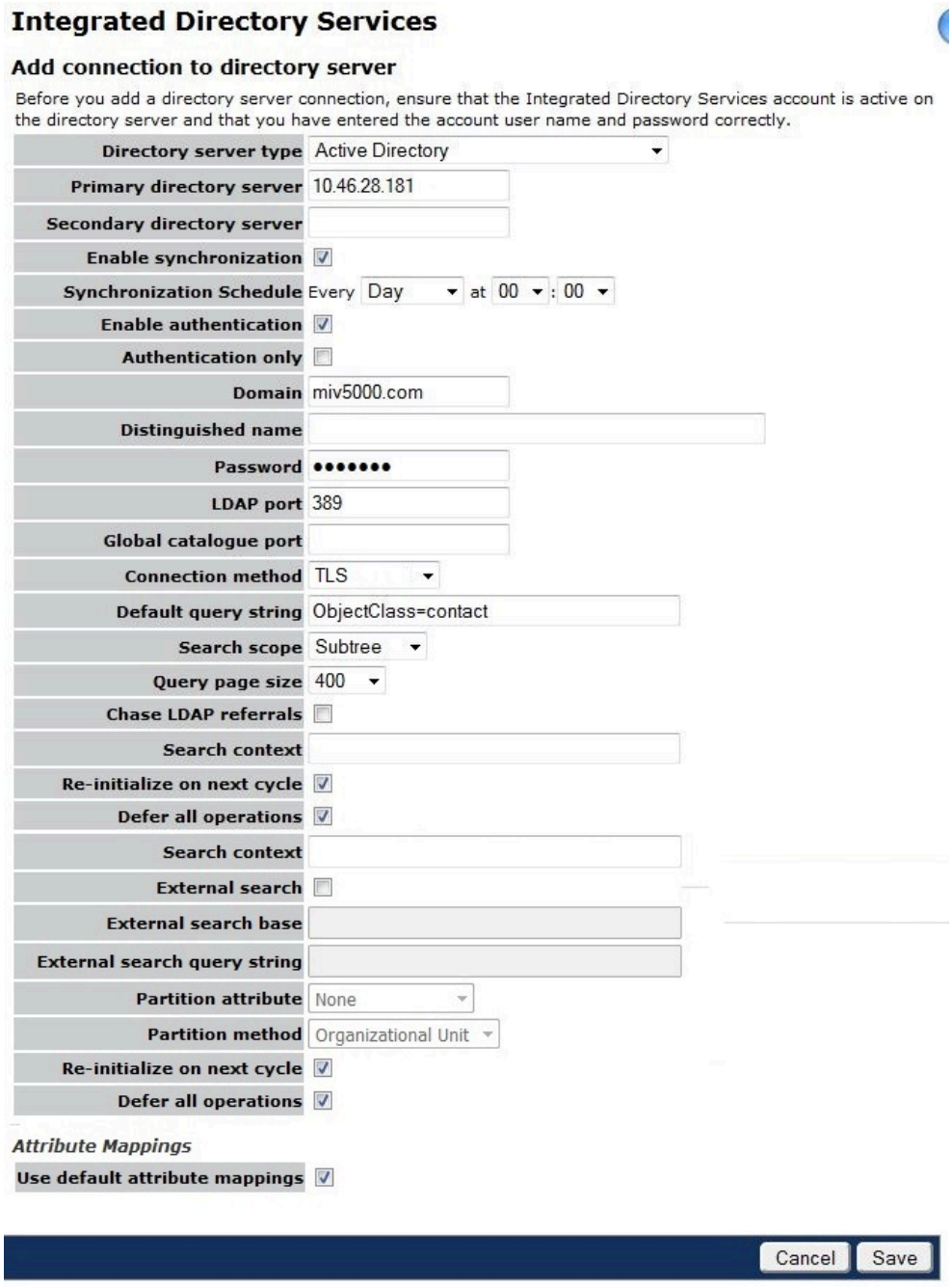
To synchronize contacts from Active Directory, create an IDS connection that specifies a query for records of type (ObjectClass=contact).

Note:
You can configure one IDS connection to an Active Directory server to support both Active Directory authentication and contact synchronization, or create one IDS connection to support contact synchronization with the MiVoice 5000 and another IDS connection to an optional Active Directory server to support Active Directory authentication of MiCollab users. Two connections are supported in this case because the Authentication Only connection does not perform any record synchronization.

Note:
To configure an IDS connection to provide only contact synchronization, check the **Enable synchronization** box and clear the **Enable authentication** box. To configure a connection for to provide both contact synchronization and Active Directory authentication of MiCollab users, check the **Enable synchronization** box and clear the **Authentication only** box.

The following is an example of a single IDS connection that synchronizes contacts and provides Active Directory authentication:

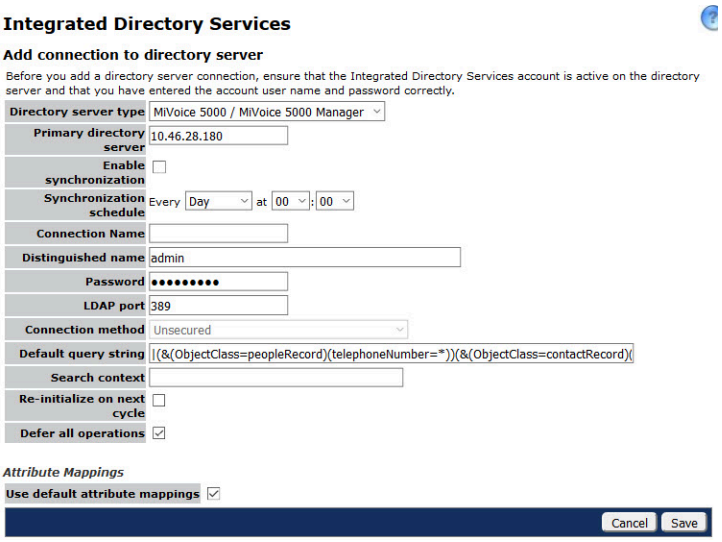
Figure 17: IDS Connection for MiVoice 5000 with Contacts from Active Directory



30.7.3 IDS Connection for MiVoice 5000 with contacts synchronized from a MiVoice 5000 Directory Service

You can use an IDS connection from a MiVoice 5000 Directory server to synchronize contacts (not users). All the entries in a MiVoice 5000 server are considered as contacts in MiCollab.

The following is an example of a single IDS connection for MiVoice 5000 that synchronizes contacts:



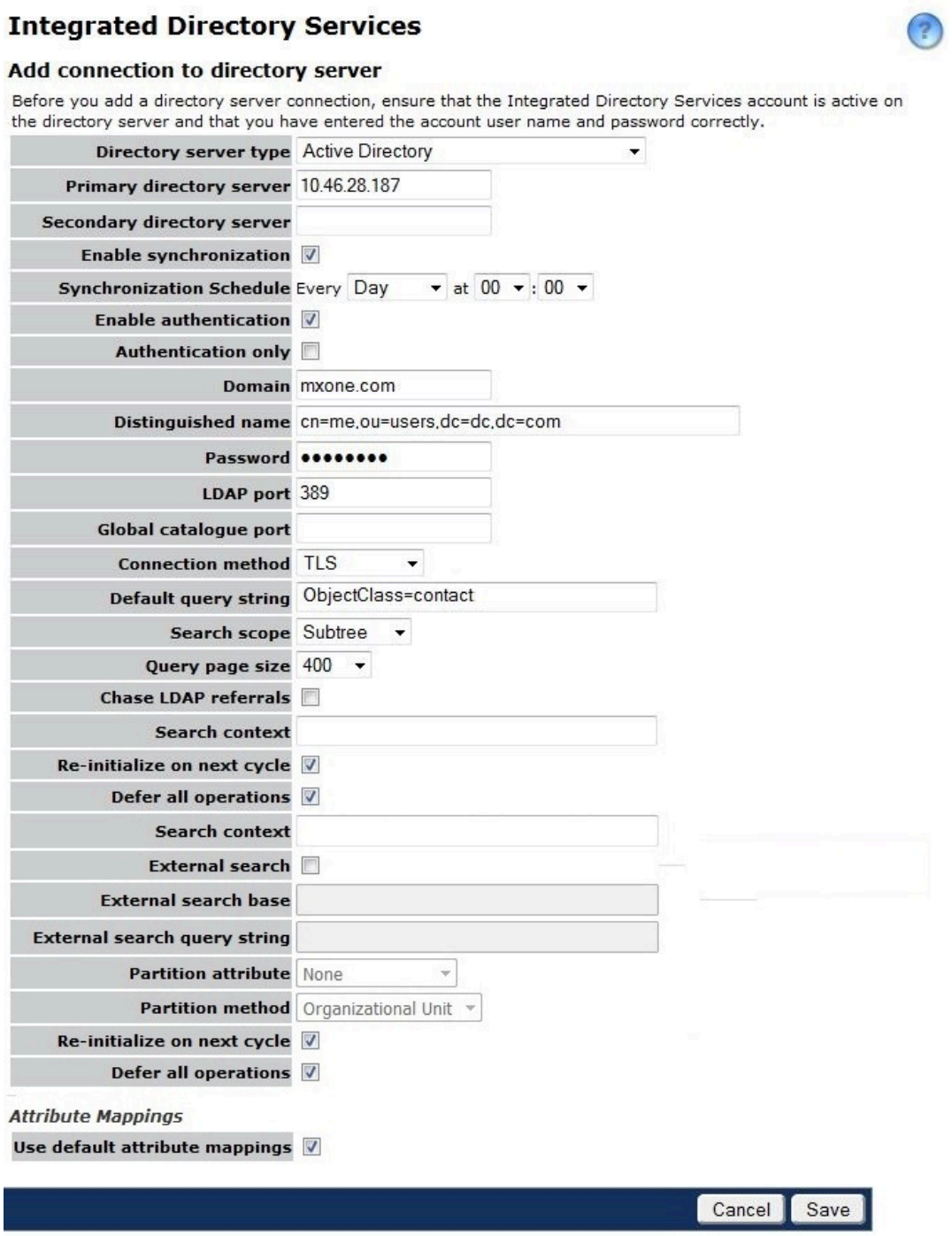
30.7.4 IDS Connection for MiVoice MX-ONE Contacts

You can use an IDS connection to synchronize MiVoice MX-ONE contacts (not users) from an Active Directory server, and to provide LDAP authentication of MiCollab users. To synchronize contacts from Active Directory, create an IDS connection that specifies a query for Active Directory records of type (ObjectClass=contact). In addition, any Active Directory record that contains the MiCollab "Contact" role is also added to the MiCollab server database as a contact record.

Note:
To configure an IDS connection to provide only contact synchronization, check the **Enable synchronization** box and clear the **Enable authentication** box. To configure a connection for to provide both contact synchronization and Active Directory authentication, check the **Enable synchronization** box and clear the **Authentication only** check box.

The following is an example of an IDS connection that provides both contact synchronization and LDAP authentication of MiCollab users:

Figure 18: IDS Connection for MiVoice MX-ONE with Contacts from Active Directory



30.7.5 IDS Connection for Mitel MetaDirectory

When a MetaDirectory setup is created, the default nodes are created under database management . By default it is named as *meta*. We can also create new LDAP nodes if required. The same is configured in MiCollab under the Domain field.

The users are not pushed from MetaDirectory, but only the Contacts get created . If you want the contacts to get directly added in Micollab Client accounts, uncheck the **Defer all operations** checkbox and check the **Reinitialize on next cycle** checkbox.

Below are sample settings for an IDS connection to Mitel MetaDirectory.

Note:
If you do an IDS synchronization with this connection, users will not be created. Only contacts will be created. All entries in Mitel MetaDirectory are treated as contacts in MiCollab.

Field	Setting	
Directory server type	Generic LDAP	
Primary directory server	<FQDN or IP address of Mitel MetaDirectory>	
Enable synchronization	<unchecked>	
Synchronization schedule		
Domain	<domain name>	Name of the node in the Mitel MetaDirectory server
Distinguished name	<username>	User for accessing the Mitel MetaDirectory in distinguished name format, i.e. cn=MiCollab
Password	<password>	The password of the user
LDAP port	712	Mitel MetaDirectory default value
Connection method	Unsecured	
Default query string	ObjectClass=person	
Search context		
External search	<checked>	
External search base		The search base to use for the external directory search for instance 'ou=users,dc=mitel,dc=com'
External search query string		The query string to use for the external directory search for instance 'objectClass=person'
Partition attribute	None	
Partition method	Organizational Unit	
Re-initialize on next cycle	<unchecked>	
Defer all operations	<checked>	

30.7.6 IDS Connection for Mitel InAttend

Below are sample settings for an IDS connection to Mitel InAttend (BluStar).

Field	Setting	
Directory server type	Generic LDAP	
Primary directory server	<FQDN or IP address of BluStar>	
Enable synchronization	<unchecked>	
Synchronization schedule		
Domain	<domain name>	Domain in the BluStar server
Distinguished name	<username>	User for accessing the BluStar in distinguished name format, i.e. cn=manager,dc=domain,dc=com
Password	<password>	The password of the user
LDAP port	389	
Connection method	Unsecured	
Default query string	ObjectClass=person	
Search context		
External search	<unchecked>	
External search base		The search base to use for the external directory search for instance 'ou=users,dc=domain,dc=com'
External search query string		The query string to use for the external directory search for instance 'objectClass=person'
Partition attribute	None	
Partition method	Organizational Unit	
Re-initialize on next cycle	<unchecked>	
Defer all operations	<checked>	

30.8 Set Default IDS Attribute Mappings

The IDS Attribute Mappings page defines the default attributes that will be used for an IDS connection between the directory server user data fields, for instance Active Directory, and the MiCollab server user data fields. It allows you to map the corporate directory service user data fields to the MiCollab data fields. MiCollab uses the connection and attribute mappings to

- write user data and corporate contacts from Active Directory into the MiCollab database,
- write corporate contacts from Active Directory, MiVoice 5000 LDAP directory service, or MiVoice 5000 Manager (AM7450) directory service into the MiCollab Client corporate directory, or
- support access to an external LDAP directory database for directory searches from MiCollab Clients.

30.8.1 Conditions

General

- You can apply the default set of attribute mappings to a connection by leaving the **Use default attribute mappings box** checked, or you can clear the box and assign custom mapping attributes to a connection.
- At minimum, directory server attributes must be set for the User ID, Distinguished Name, First Name, and Last Name fields. All other fields can have blank directory server attributes, which allows the fields to remain blank or to be populated from a template.
- Customized attribute fields are validated when the connection runs. If you enter an attribute incorrectly, the operations will likely fail. The failed operations are listed as errors in the summary and are sent to in the detained updates queue.
- If you change an attribute mapping on MiCollab after the initial full synchronization, another full synchronization is required because regular scheduled synchronizations only detect and apply deltas from the directory service. The directory service is unaware of the change on MiCollab until you perform a full synchronization. A warning message is displayed if you change an attribute on MiCollab after the

initial sync. The warning indicates that another full synchronization is required apply the change to the directory server.

- MiCollab supports UTF-8 format for the directory service attributes with the following exceptions: Email address, Department, and Location. These field attributes do not support UTF-8 format. This limitation applies to the MiVoice Business system also. If one of these fields receives UTF-8 data, the operation fails and is sent to the deferred updates queue.
- If First Name, Last Name, or Department attributes are updated for a user, the updated values will get reflected after 15 minutes in the client call window. It is recommended for users to wait for 15 minutes or restart the system to display the updated values.

Specific Conditions Relating to Users

Directory service attributes that are mapped to user service data must

- be unique
- belong to the user object class - different objects cannot be described by the same set of attributes; otherwise, updates will fail.
- programmable from a user interface such as the Active Directory Users and Computers console.
- be single-valued (not a list of comma-separated values)
- be available (when you select an LDAP attribute to map to user service data, ensure that the attribute in use for some other purpose).

Specific Conditions Relating to Contacts

The attribute mappings of the IDS connection must be set to match the MiVoice 5000 directory schema. The MiVoice 5000 can have different attributes for internal (people) and external (contact) records. Therefore, to support the synchronization of both types of records, the internal and external record attribute tables on the MiVoice 5000 LDAP directory service must match each other for the MiCollab IDS connection to retrieve both types of records.

The MiVoice 5000 and MiVoice 5000 Manager (AM7450) allow you to configure custom attributes in the directory schema in order to provide additional custom information for external records. On the MiVoice 5000 you perform the configuration from the Telephony Service -> Subscribers -> Directory-> Parameters ->Customization menu. On the AM7450 you perform the configuration from the Telephony-> Directory Management-> Customization menu. The custom attributes are named attr1, attr2, attr3, and so forth. MiCollab IDS support mappings to these custom attributes.

Specific Conditions Relating to Mobile Phones

If the Mobile Phone Directory Number field is mapped in the Attribute Mappings table, **when a new user is created** with a mobile number in Active Directory, the mobile number is populated into the External Hot Desk User (EHDU) number in MiVoice Business. It is also sent to MiCollab Client server (UCA) and added to the user's phones list. The user will see this number when they manage their dynamic status and other users will see that number in the corporate directory. The EHDU number is added to the following interfaces:

- User and Services application in MiCollab.
- Phone service in MiVoice Business.
- User's phone service list as presented in the UCA management pages
- End user's account information.
- MiCollab Client corporate directory as presented to other users.

When the **mobile number for an existing user is updated** in Active Directory, then on the next scheduled IDS synchronization cycle, the mobile number change is detected and the new mobile number is shown in bold in the detained queue. If the IDS connection is configured to apply updates immediately (defer all updates is not checked) then the EHDU number will be updated immediately in the interfaces listed above; if not, the EHDU is updated after you save the update in the 'Manage Detained Queue' tool.

Note the following:

- DID numbers and Directory numbers are not updated. Only mobile numbers are updated.
- Whenever you update an Active Directory user (any attribute) if there is a mobile number programmed in Active Directory the number will be synchronized into MiCollab, possibly over-writing end user's provided EHDU number. To avoid overwriting a user's EHDU number, review the change in 'Manage detained queue' and if necessary choose not to apply the change.

- If you do not want mobile numbers that are provisioned in Active Directory to be applied to the MiCollab solution, remove the mobile number mapping from the IDS connection.
- If the EHDU was published, it remains published. If it was not published, it remains unpublished.
- If other fields are also updated in Active Directory at the same time (such as the user's first or last name) these updates are also applied.
- It is not necessary to perform a PBX sync in order for an update to be sent to the MiVoice Business or MiCollab Client.
- The same number format supported in the initial create is supported in the subsequent update.
- To synchronize existing users mobile numbers with Active Directory, check the 'Re-initialize on next cycle' option in the IDS connection and re-run the sync.
- The correct MiVoice Business system username and password must be provisioned in the Network Elements tab in the User and Services application.

30.8.2 Attribute Mapping Descriptions

The following LDAP attributes are mapped from an external Active Directory or LDAP source through the MiCollab IDS integration for

- Users (including Teamwork mode users)
- Contacts

for the following communication platform integrations:

- MiVoice Business
- MiVoice MX-ONE
- MiVoice 5000 and for
- access to an external directory such as Mitel Meta Directory or Mitel InAttend.

Note:
The default attribute mappings are applied to a new connection. To use custom mappings, clear the **Use default attribute mappings box** and enter the required attributes.

Note:
In the Attribute Mapping table, not all the attributes are applicable in the case of ForgeRock Directory Services. See the table below for reference.

Note:
If the user synchronization is enabled from On-Prem AD and authentication is enabled from CloudLink, the Admin must change the IDS mapping for the login id to the “userPrincipalName” field.

MiCollab Attribute	Description	Attribute Mappings			
		Default Active Directory mappings for user data and MiCollab Client Contacts	Default Active Directory mappings MiCollab Client Contacts only	Sample MiVoice 5000/ MiVoice 5000 Manager LDAP Directory Service mappings for MiCollab Client Contacts only	ForgeRock Directory Services Default attributes
City	Enter the directory server attribute for the city.	l	l	l	(unmapped)
Company Name	Enter the directory server attribute for the company name.	company	company	company	(unmapped)
Country	Enter the directory server attribute for the country.	co	co	co	co
DID Number	Enter the directory server attribute for the Direct Inward Dial Number. **Note**: If you change a DID number on the directory server, it is NOT updated on MiCollab.	(unmapped)	(unmapped)	(unmapped)	(unmapped)
Department	Enter the directory server attribute for the department.	department	department	department	department
Distinguished Name	Enter the directory server attribute for the distinguished name. The distinguished name attribute is used by MiCollab Client to group contacts via their organizational unit information.	distinguishedName	distinguishedName	distinguishedName	cn

MiCollab Attribute	Description	Attribute Mappings			
		Default Active Directory mappings for user data and MiCollab Client Contacts	Default Active Directory mappings MiCollab Client Contacts only	Sample MiVoice 5000/ MiVoice 5000 Manager LDAP Directory Service mappings for MiCollab Client Contacts only	ForgeRock Directory Services Default attributes
Email	Enter the directory server attribute for the e-mail address.	mail	mail	mail	mail
Fax	Enter the directory server attribute for the business fax.	facsimileTelephoneNumber	facsimileTelephoneNumber	facsimileTelephoneNumber	facsimileTelephoneNumber
First Name	Enter the directory server attribute for the user first name. This field is mandatory. On the MiVoice 5000 and MiVoice 5000 Manager (AM7450) the first name is typically identified by the displayGn field if UTF8 is supported. Otherwise, use the givenName field.	givenName	givenName	givenName	givenName
Home Element	Specify the directory server attribute for the MiVoice Business system that supports the phone services. You must enter the IP address or hostname of the MiVoice Business system in the specified attribute on the directory server. After you synchronize the directory server database with MiCollab , the user's phone services are assigned to the specified MiVoice Business system. **Note**: You can also apply a role (see below) with an associated template that assigns the MiVoice Business system. **Note**: This field does not apply to MiCollab Client contacts.	ipPhone	ipPhone	ipPhone	(unmapped)

MiCollab Attribute	Description	Attribute Mappings			
		Default Active Directory mappings for user data and MiCollab Client Contacts	Default Active Directory mappings MiCollab Client Contacts only	Sample MiVoice 5000/ MiVoice 5000 Manager LDAP Directory Service mappings for MiCollab Client Contacts only	ForgeRock Directory Services Default attributes
Home Element *continued*	**Note**: The values entered in the **Home Element** and the **System Administrator > Manage Network ElementsIP Address/ FQDN**> fields must be the same. **Note**: The value entered in the **Home Element** field will supersede the pre-defined value in the **IP Address/ FQDN** field, when you select the desired PBX from the MiCollab template.				
Info	Enter a directory server attribute that represents some data that will be searchable in MiCollab Clients.	(unmapped)	(unmapped)	(unmapped)	(unmapped)
Info 2	Enter a directory serve r attribute that represents some data that will be searchable in MiCollab Clients.	(unmapped)	(unmapped)	(unmapped)	(unmapped)
Language	Enter the directory server attribute for the preferred language. **Note**: This field does not apply to MiCollab Client contacts.	preferredLanguage	preferredLanguage	preferredLanguage	preferredLanguage

MiCollab Attribute	Description	Attribute Mappings			
		Default Active Directory mappings for user data and MiCollab Client Contacts	Default Active Directory mappings MiCollab Client Contacts only	Sample MiVoice 5000/ MiVoice 5000 Manager LDAP Directory Service mappings for MiCollab Client Contacts only	ForgeRock Directory Services Default attributes
Last Name	Enter the directory server attribute for the user's last name. This field is mandatory. For MiVoice 5000 and MiVoice MX-ONE integrations, use the "displayName" attribute if UTF8 character support is required. Set the field to "sn" if UTF8 support is not required.	sn	sn	sn	sn
Location	Enter the directory server attribute for the location. This field does not apply to corporate contact records.	physicalDeliveryOfficeName	physicalDeliveryOfficeName	physicalDeliveryOfficeName	physicalDeliveryOfficeName
Login	Enter the directory server attribute for the Login ID field. This field is mandatory. This attribute has a maximum length of 20 characters in the directory service.	samAccountName	not applicable	samAccountName	uid
Mobile Phone Number	Enter the directory server attribute for the mobile phone. **Note**: If you change a mobile number on the directory server, it is updated on MiCollab during the next synchronization.	(unmapped)	(unmapped)	mobile	mobile
Mobile Phone Number 2	Enter the LDAP attribute for the second mobile phone.	(unmapped)	(unmapped)	(unmapped)	(unmapped)
Object Class	Displays the directory server attribute that is used to import users, or contacts, or both, from the directory server using IDS. This field is read-only.	objectClass	objectClass	objectClass	objectClass

MiCollab Attribute	Description	Attribute Mappings			
		Default Active Directory mappings for user data and MiCollab Client Contacts	Default Active Directory mappings MiCollab Client Contacts only	Sample MiVoice 5000/ MiVoice 5000 Manager LDAP Directory Service mappings for MiCollab Client Contacts only	ForgeRock Directory Services Default attributes
Photograph	Enter the directory server attribute for the photograph. Default entry is **thumbnailPhoto**. It also supports **jpegPhoto**. **Note**: Photograph added using the Client or Server Manager will over-ride the AD sync photo.	thumbnailPhoto	thumbnailPhoto	thumbnailPhoto	(unmapped)
Position	Enter the directory server attribute for the position.	(unmapped)	(unmapped)	(unmapped)	(unmapped)
Postal/ZIP Code	Enter the directory server attribute for the postal code or ZIP code.	postalCode	postalCode	postalCode	postalCode
Primary Phone Directory Number	Enter the LDAP attribute for the prime directory number.	telephoneNumber	telephoneNumber	telephoneNumber	telephoneNumber
Role	Enter the directory server attribute for the role. The role field for a contact record is not mandatory. For Active Directory contact synchronization, the role is automatically set to "contact" after a contactRecord is identified or in the case of Active Directory if the objectClass is set to "contact". If the role is present in the directory server, users whose roles are set to 'Contact' will be created as contacts in MiCollab.	employeeType	employeeType	employeeType	description
Secondary Phone Directory Number	Enter the secondary phone directory number.	(unmapped)	otherTelephone	otherTelephone	(unmapped)
Street	Enter the directory server attribute for the street.	streetAddress	streetAddress	streetAddress	streetAddress
Title	Enter the directory server attribute for the title.	title	title	title	title

MiCollab Attribute	Description	Attribute Mappings			
		Default Active Directory mappings for user data and MiCollab Client Contacts	Default Active Directory mappings MiCollab Client Contacts only	Sample MiVoice 5000/ MiVoice 5000 Manager LDAP Directory Service mappings for MiCollab Client Contacts only	ForgeRock Directory Services Default attributes
User Id	Enter the directory server attribute for the Globally Unique Identifier (GUID). For integrations that use Active Directory set this field to "objectGUID". For MiVoice 5000 or MiVoice 5000 Manager, set to "cleUid".	objectGUID	objectGUID	objectGUID	uid

Level of Attribute Support

	Database fields	Default LDAP field	MiVB User	MX-ONE/MiV5000/ MiVO400 User	Contact	Teamwork Mode User
	City	l	✓	✓	✓	✓
	Company Name	company	✓	✓	✓	✓
	Country	co	✓	✓	✓	✓
	DID Number*		⚠	✓	✗	✓
	Department	department	✓	✓	✓	✓
	Distinguished Name	distinguishedName	✓	✓	✓	✓
	E-mail	mail	✓	✓	✓	✓
	Fax	facsimileTelephoneNumber	✓	✓	✓	✓
	First Name	givenName	✓	✓	✓	✓
	Home Element	ipPhone	⚠	✓	N/A	N/A
	Info		✓	✓	✓	✓
	Info 2 (Custom 2)		✓	✓	✓	✓
	Language	preferredLanguage	✓	✓	✗	✓
	Last Name	sn	✓	✓	✓	✓
	Location	physicalDeliveryOfficeName	✓	✓	✓	✓
	Login	samAccountName	✓	✓	✗	✓
	Mobile phone Number	mobile	✓	✗	✓	✓
	Mobile phone Number 2		✓	✓	✓	✓
	Object Class	objectClass	✓	✓	✓	✓
	Photograph	thumbnailPhoto	✓	✓	✓	✓
	Position		✓	✓	✓	✓
	Postal/ZIP code	postalCode	✓	✓	✓	✓
	Primary Phone Directory Number	telephoneNumber	⚠	⚠	✓	✓
	Role	employeeType	⚠	⚠	⚠	⚠
	Secondary Phone Directory Number	otherTelephone	⚠	✗	✓	✓
	Street	streetAddress	✓	✓	✓	✓
	Title	title	✓	✓	✓	✓
	User Id	objectGUID	✓	✓	✓	✓
✓	supported for initial sync and updates					
⚠	updates are not supported from AD, only used for initial creation					
✗	not supported					
*	**Notes**: 1. DID Number attribute is used to update the DID Service Number in Users and Services (only for initial creation) 2. DID Number attribute is used to update the External number (on initial creation and on any update)					

30.9 Set Custom IDS Attribute Mappings

To assign custom attribute mappings to an IDS connection

1. Clear the **Use default attribute mappings** box. The IDS attribute mapping table for this connection is displayed with the default settings.
2. Modify the default mapping attributes as required.
3. Click **Save**.

The following are recommended settings for

- Mitel MetaDirectory Attribute Mappings
- Mitel InAttend (BluStar) Attribute Mappings

30.10 Attribute Mappings for Mitel MetaDirectory

Below are recommended attribute mappings for Mitel MetaDirectory (MMD):

MiCollab field	Mitel MetaDirectory mapping	Notes
City	l	
Company Name	company	
Country	c	
DID Number		Use a custom field in MMD
Department	department	
Distinguished Name	distinguishedName	
Email	mail	
Fax	facsimileTelephoneNumber	
First Name	givenName	
Home Element		
Info	info	
Info2		Use a custom field in MMD
Language		Use a custom field in MMD
Last Name	sn	
Location	physicalDeliveryOfficeName	
Login	sAMAccountName	
Mobile phone number	mobile	
Mobile phone number 2	telephoneCar	
Photograph		Not supported, leave blank
Position		Use custom field in MMD
Postal/Zip code	postalCode	
Primary phone directory number	telephoneNumber	
Role		
Secondary phone directory number	otherTelephone	
Street	streetAddress	
Title	title	
User Id	entryID	

30.11 Attribute Mappings for Mitel InAttend (BluStar)

Below are recommended attribute mappings for Mitel InAttend:

MiCollab field	Mitel InAttend mapping	Notes
City	l	
Company Name	company	
Country	c	
DID Number		Use a custom field in BluStar
Department	department	
Distinguished Name	distinguishedName	
Email	mail	
Fax	facsimileTelephoneNumber	
First Name	givenName	
Home Element	pbxNode	
Info		Use a custom field in BluStar
Info2		Use a custom field in BluStar
Language		Use a custom field in BluStar
Last Name	sn	
Location	physicalDeliveryOfficeName	
Login	accountName	
Mobile phone number	mobileTelephoneNumber	
Mobile phone number 2		Use custom field in BluStar
Photograph		Not supported, leave blank
Position		Use custom field in BluStar
Postal/Zip code	postalCode	
Primary phone directory number	telephoneNumber	
Role		Use custom field in BluStar
Secondary phone directory number	softPhone	
Street	streetAddress	
Title	title	
User Id	objectGUID	

30.12 Disable IDS on MiCollab

If you disable IDS, periodic database synchronization with the directory server is disabled. However, the deferred operation queue will remain as it was at the moment you disabled IDS. If there were any operations in the deferred queue, the system will allow you to process them. No new IDS operations are added to the queue. If authentication was being used, it will be disabled and you will be required to reset the passwords for all users that were paired with directory service entries. The state of the IDS Managed flags are maintained after you disable IDS.

To disable IDS on MiCollab :

1. Under **Configuration**, click **Integrated Directory Service**.
2. Click Remove next to the domain of the directory server.
3. Click **Save**. If Active Directory Authentication was supported for the domain, you are prompted to enter a replacement password for the users.
4. Enter and confirm the password and then click **Save**. A Welcome E-mail which includes the replacement password is sent to the select users.

Later, if you enable IDS on MiCollab again, the deferred operation queue is emptied of IDS operations and a full synchronization occurs.

30.13 Configure Access to External (Off-board) Directory

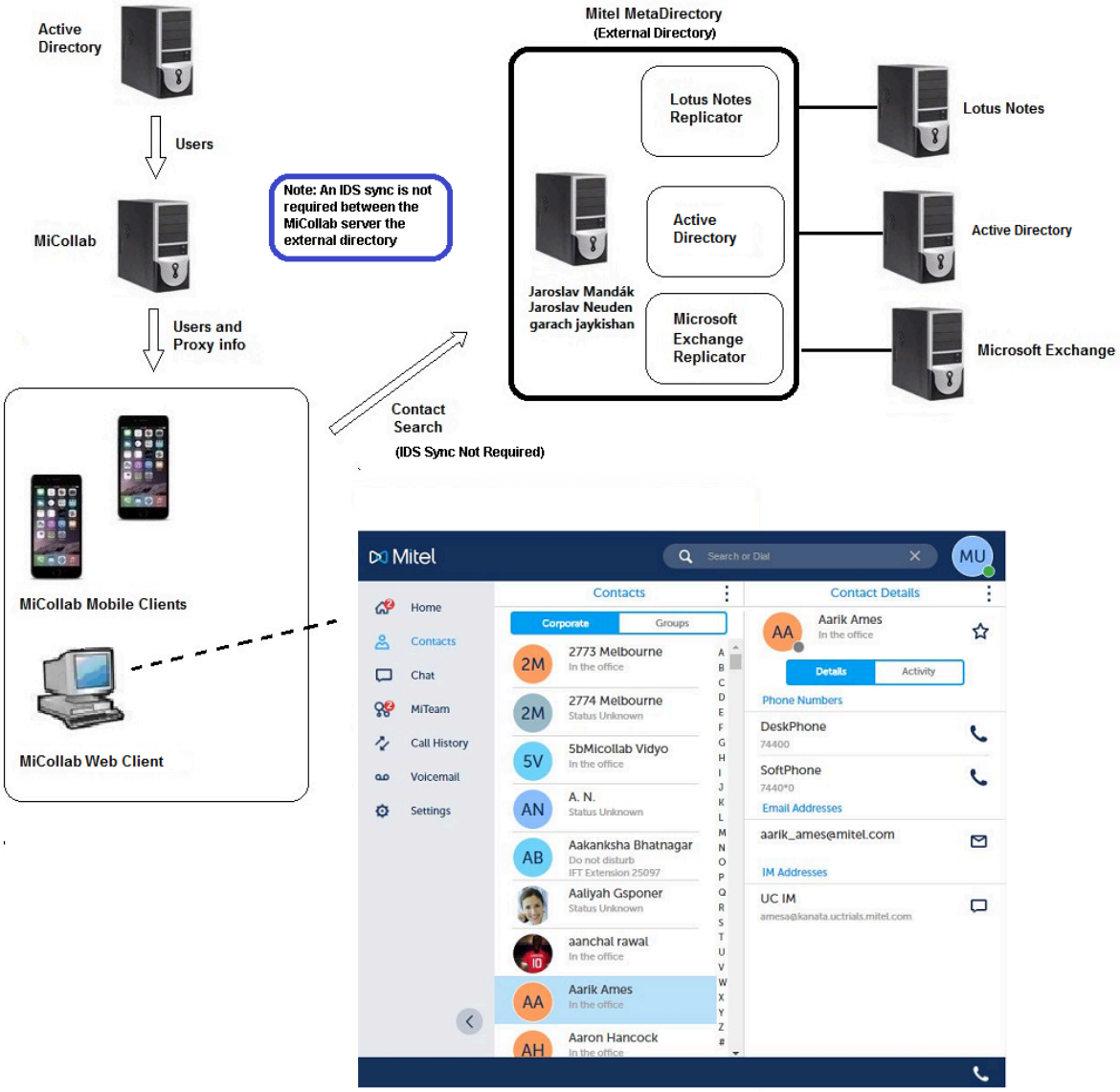
You can configure the MiCollab Client Service with access to a large, external off-board LDAP directory, such as Mitel MetaDirectory. MiCollab Client users can then search for corporate contacts from a very large number of entries.

Note:

External LDAP with MiCollab for Microsoft Client is used only for number lookup on incoming MiCollab calls (only if there is no match in the corporate directory or the PBX). It is not used to search any external LDAP database. You need to integrate the external LDAP directory with the Skype for Business directory to perform the search.

The directory entries from multiple databases, such as Lotus Notes or Microsoft Exchange can be aggregated within the metadirectory. Typically, you would not synchronize contacts from the external directory to the MiCollab Client service.

The following diagram shows an overview of the solution:



Note:

The Mitel MetaDirectory product documentation is integrated in the installation Software-Package as help. After you install it on a host (you can use a temporary host just to access the last online help) you can extract the online-help from “C:\Program Files (x86)\Mitel\MetaDirectory\resources\en-US”.

Conditions

To support connection to an external directory:

- MiCollab Client must be configured in integrated mode.

- An external LDAP solution, such as Mitel MetaDirectory, that aggregates the contents of separate databases into a large central directory, is required.
- You must configure an Integrated Directory Services connection between the MiCollab and the external LDAP solution. Only one connection to an external directory is supported.
- Regardless of the connection method which is enabled (for the IDS connection to the directory server),the external directory search will always use an unsecured channel (non-SSL).
- An IDS synchronization operation is not required to support the external search feature. An IDS synchronization operation imports the accounts from the external directory to the MiCollab server. However, for external searching the accounts are not required on the MiCollab server.

Configuration

To configure access to an external directory:

1. Under **Configuration**, click **Integrated Directory Service**.
2. Click **Add connection**. The Add Integrated Directory Service connection page opens.
3. Complete the fields to create a connection to the external directory. See Manage IDS Connections for field descriptions.

   - Set the Directory server type (for a connection to Mitel MetaDirectory, select Generic LDAP).
   - Select the **External search** box to select this connection as the one that MiCollab Clients will use for external directory searches.
   - Enter the name of the external search base.
   - Enter an external search query string that will narrow the search criteria and reduce the number of results.

   The following are **examples** of the connection settings to Mitel MetaDirectory or Mitel InAttend solutions:

Field	Mitel MetaDirectory Setting	Mitel InAttend Setting	Notes
Directory server type	Generic LDAP	Generic LDAP	
Primary directory server	<FQDN or IP address of Mitel MetaDirectory>	<FQDN or IP address of Blustar server>	
Enable synchronization	<unchecked>	<unchecked>	
Synchronization schedule			
Domain	<domain name>	<domain name>	Name of the node in the Mitel MetaDirectory or Mitel InAttend
Distinguished name	<username>	<username>	User for accessing the Mitel MetaDirectory or Mitel InAttend in distinguished name format, i.e., cn=MiCollab

Field	Mitel MetaDirectory Setting	Mitel InAttend Setting	Notes
Password	<password>	<password>	Password of the user
LDAP Port	712	389	Default value
Connection method	Unsecured	Unsecured	
Default query string	ObjectClass = person	ObjectClass = person	
Search context			
External search	<checked>	<checked>	
External search base			The search base to use for the external directory search, for example: "ou=users,dc=mitel,dc=com"
External search query string			The query string to use for the external directory search, for example: "objectClass=person".
Partition attribute	None	None	
Partition method	Organizational unit	Organizational unit	
Enable reverse lookup	<unchecked>	<unchecked>	Unchecked for Active Directory. Checked for Generic LDAP server type.
Remove leading digits count			Default value is 0.
Re-Initialize on next cycle	<unchecked>	<unchecked>	
Defer all operations	<checked>	<checked>	

4. To use custom attribute mappings for this connection to the external directory, clear the **Use default attribute mappings** box and modify the modify the IDS attribute mapping. you must map LDAP attributes to the following IDS attributes: Distinguished Name, Email, First Name, and Last Name. All other fields can have blank LDAP attributes.

Note:

Ensure that the contacts on the external directory contain entries in the fields that map to the following IDS attributes: Distinguished Name, First Name, Last Name, and Email.

The following is an **example** of custom attribute settings to a Mitel MetaDirectory and InAttend:

MiCollab Field	Mitel MetaDirectory mapping	InAttend mapping	Notes
City	l	l	
Company Name	company	company	
Country	c	c	
DID Number			Use a custom field in Mitel MetaDirectory or Mitel InAttend
Department	department	department	
Distinguished Name	distinguishedName	distinguishedName	
Email	mail	mail	
Fax	facsimileTelephoneNumber	facsimileTelephoneNumber	
First Name	givenName	givenName	
Home Element		pbxNode	
Info	info		
Info2			Use a custom field in Mitel MetaDirectory or Mitel InAttend
Language			Use a custom field in Mitel MetaDirectory or Mitel InAttend

MiCollab Field	Mitel MetaDirectory mapping	InAttend mapping	Notes
Last Name	sn	sn	
Location	physicalDeliveryOfficeName	physicalDeliveryOfficeName	
Login	sAMAccountName	accountName	
Mobile Phone Number	mobile	mobileTelephoneNumber	
Mobile Phone Number 2	telephoneCar		
Photograph			Not supported. Leave blank.
Position			Use a custom field in Mitel MetaDirectory
Postal/ZIP code	postalCode	postalCode	
Primary Phone Directory Number	telephoneNumber	telephoneNumber	
Role			
Secondary Phone Directory Number	otherTelephone	softPhone	
Street	streetAddress	streetAddress	
Title	title	title	
User ID	entryID	objectGUID	

5. Click **Save**.

Note:

When InAttend is configured with a fresh MiCollab server, the MiCollab root certificate should be installed in the Trust Store of InAttend Client, to ensure the correct presence of instant messages.

Test Directory Access from Clients

From a MiCollab Client, check to ensure that contacts stored in the metadirectory are listed in searches.

30.14 Partitioning the External (Off-board) Directory

You can partition (filter) the external corporate directory such that users are only presented a subset of the corporate directory contact entries. For example, supplier contacts could be excluded from the directories of users who do not need to call these numbers.

You can partition the directory by organizational unit or by attribute:

- **Organizational unit**: When users perform a search, the results are only drawn from the entries in their organizational unit.
- **Attribute**: When users perform search, only results that share the same attribute are presented

Conditions

- Directory partitioning is limited to corporate contacts only. It is not supported for users.
- Users can place calls to contacts that do not appear in their directories (that is, users can still place calls to contacts that have been filtered out).
- An SSL connection to the external directory is not supported.
- If you are partitioning an external directory for a deployment that includes MiVoice Business with Flow Through Provisioning enabled, you must configure the organizational units for the department and location containers in the meta directory without accented characters (see Special Accent Handling for Flow Through Provisioning for details).
- MiCollab Client strips the punctuation and performs transliteration (applies accents) when doing external searches on Generic LDAP connections for all PBX integrations to cover MiVoice Business without Flow Through Provisioning and MiVoice MX-ONE cases.

Partition by Organizational Units

To partition (filter) the MiCollab Client corporate contact directory by organizational unit:

1. Under **Configuration**, click **Integrated Directory Service**.
2. In the **Actions** column for the desired domain, click **Edit**. The Integrated Directory Service connection page opens.
3. Check the **External search** box.
4. In the **Partition attribute** field, select the attribute that you want to use to filter out contacts from the corporate directory. You can select one of the following: None, City, Company Name, Country, Department, Info, Info 2, Language, Location, Position, Postal/ZIP Code, Street or Title.
5. In the **Partition method** field, select **organizational unit**.
6. Click **Save**.

Example:

In Active Directory, the following organizational units have been created to contain the contacts for the company:

OU=Contacts,OU=Kanata,DC=Mitel,DC=gov

OU=Contacts,OU=Denver,DC=Mitel,DC=gov

OU=Contacts,OU=Toronto,DC=Mitel,DC=gov

The company directory includes the contact numbers of product suppliers. The majority of users do not call these suppliers; however, the purchasing agents in each city (Kanata, Denver, or Toronto) need access to these contacts to place orders for product. In this case, you want the purchasing agents to only see the supplier contacts that are located in their city.

In Active Directory tag the supplier contacts with a custom "supplier" attribute. Also, tag the purchasing agents who need access to the supplier contacts with the "supplier" attribute. Then, in the MiCollab IDS Mapping form, map the custom "supplier" attribute to an MiCollab IDS attribute (for example, the "Info" attribute).

To partition the corporate directory such that only purchasing agents see the supplier contacts in their city (organizational unit):

- Set the Partition search attribute to "Info".
- Set the Partition method to "organizational unit".

In this case, the system partitions the corporate directory based on the "Info" attribute within each organizational unit. Users with the "Info" attribute will see their local supplier contacts listed in their corporate directories.

Partition by Attribute

When you partition (filter) the external corporate directory by attribute, users who perform a search will only find directory entries that share the same attribute.

To partition the MiCollab Client corporate contact directory by attribute:

1. Under **Configuration**, click **Integrated Directory Service**.
2. In the **Actions** column for the desired domain, click **Edit**. The Integrated Directory Service connection page opens.
3. Check the **External search** box.
4. In the **Partition attribute** field, select the attribute that you want to use to filter out contacts from the corporate directory.
5. In the **Partition method** field, select **attribute**.
6. Click **Save**.

Example:

Users are assigned to one of three departments: Marketing, Sales and Purchasing.

To partition the corporate directory such that users only see the contacts in their own department:

- Set the Partition search attribute to "department".
- Set the Partition method to "attribute".

30.15 Migrate MiCollab with MiVoice Business IDS to MiCollab IDS

Migration of MiVoice Business IDS to MiCollab IDS must be performed manually. You must copy the IDS settings from the MiVoice Business IDS forms to the corresponding fields in the MiCollab IDS Connection and Attribute Mapping pages.

1. Review the General Guidelines and Limitations.
2. Log into MiVoice Business System Administration Tool.
3. Display the MiVoice Business IDS Connection form. The following table maps the MiVoice Business IDS settings to the corresponding MiCollab IDS connection parameters..

MiVoice Business IDS Connection Settings	MiCollab IDS Connection Parameters
Directory Server Type	Directory server type
Client Network Element	
Directory Server	Primary directory server
	Secondary directory server
Domain	Domain
User	Distinguished name
User Password	Password
LDAP Port	LDAP port
GC LDAP Port	Global catalogue port
Connection Method	Connection method
Default Query String	Default Query string
Search Scope	Search context
Maximum Query Time	
Query Page Size	Query page size
Chase Referral	Chase LDAP referrals
Search Context	Search context
Default Container to Add New Users on DS	
Last Sync Time	Last synchronization

4. Display the MiVoice Business "User Service to LDAP" form. The following table maps the MiVoice Business and MiCollab IDS attributes to the corresponding directory service attributes.

MiVoice Business IDS Attribute	Directory Server Default Attributes	MiCollab Attribute
COMMON ATTRIBUTES		
Company	company	Company
	(unmapped)	Direct Inward Dial

MiVoice Business IDS Attribute	Directory Server Default Attributes	MiCollab Attribute
Department	department	Department
Distinguished Name	distinguishedName	Distinguished Name
Email	mail	Email
First Name	givenName	First Name
Home Element	ipPhone	Home Element
Language	preferredLanguage	Language
Last Name	sn	Last Name
Location	physicalDeliveryOfficeName	Location
Login	samAccount Name	Login
Directory Number	telephoneNumber	Primary Phone Directory Number
Role	employeeType	Role
User ID	objectGUID	User ID
	MiCollab ONLY	
	otherTelephone	Secondary Phone Directory Number
	mobile	Mobile Phone Directory Number
	objectClass	Object Class
MiVoice Business ONLY		
Secondary Element	otheripPhone	

Note:
The MiVoice Business Directory Number field may include the Primary Node ID in the directory number (PNI + DN). MiCollab does not accept the PNI. Either remove the PNI from the directory number or create a new field that only has the directory number and map to MiCollab.

5. Ensure that the Login field in the MiVoice Business is mapped to the samAccount Name field.
6. If IDS is enabled on any MiVoice Business platforms or applications, run a synchronization operation with the directory server to ensure that the MiVoice Business platforms, applications, or both have the latest updates from the directory server. Refer to *Integrated Directory Services* in the *MiVoice Business System Administration Tool* online help for instructions.

Note:
You must resolve the detained updates from the MiVoice Business on the associated MiCollab. If there are multiple MiCollab systems on site, ensure that you make the required updates on the correct MiCollab.

7. Disable MiVoice Business IDS:

   - Log into the MiVoice Business System Administration Tool.
   - Access the Network Element Assignment form and delete the directory server.

8. In the USP Network Element tab, disable Single Point Provisioning.
9. Create a MiCollab synchronization account on the directory service domain. The account must have read access.
10. If Active Directory Authentication is required, ensure that a valid Certificate Authority (CA) has been configured for Active Directory. If authentication is not required, you assign users new passwords on MiCollab using roles and associated user templates.
11. On the directory server, ensure that the user data fields contain entries for the following attributes: samAccountName, givenName, sn, and distinguishedName. Otherwise, failed update errors are generated on MiCollab during the synchronization. If an employeeType field is not specified, the entry is sent to the detained queue.
12. In the MiCollab Users and Services application, create user templates for the various roles in the enterprise. In the templates, assign the phone and application services that you want to apply to the user data that is obtained from the directory server. In the templates, also set a password policy for the user data. You have the option of creating these templates from the UCC default templates.
13. In the MiCollab Users and Services application, create roles that correspond to the employeeType attribute entries on the directory service. You can create these roles from the UCC default roles. Note that when users are obtained from the directory server, if a user entry has a blank employeeType field, the update is sent to the detained user updates queue.
14. Create a connection to the directory server:

    - Under **Configuration** , click **Integrated Directory Service** .
    - Click **Add connection** . The Add Integrated Directory Service connection page opens.
    - Complete the fields to create a connection. When you configure the IDS Connection Parameters Current MiVoice Business-IDS Connection Values" that you recorded in the table above into the MiCollab IDS Connection page. See Manage IDS Connections for field descriptions.
    - If Active Directory Authentication is required, the Synchronization option must be enabled. Also, set the **Connection Method** to either TLS or TSL/SSL. The **Connection Method** cannot be Unsecured.

    Note:
    To use SSL/TLS for IDS, LDAP over SSL must enabled on the active directory server. See the following links for more information:

    - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772393(v=ws.10)?redirectedfrom=MSDN
    - https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
    - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee411009(v=ws.10)?redirectedfrom=MSDN

    - Click **Save** . MiCollab verifies the connection parameters and indicates if any errors are present.

15. Configure Active Directory Authentication if required.

    - Check the **Enable authentication** box below the domain. You can only enable authentication on a single domain. So, if you want to select a different domain, you must first disable the currently selected domain.

      Note: You can connect the Active Direcory Authentication to a Global Catalogue on the domain controller. If multiple connections are used, and if those connections point to domains which are under the same forest, you can configure one connection to use the global catalogue. With global catalogue enabled, all users from all connections under the same forest should be able to authenticate. Note that using global catalogue limits the fields that can be used for synchronization.
    - Secure authentication requests are required as part of the IDS connection.
    - Click **Save.**
16. Configure the IDS Attribute Mappings. Transfer any custom Directory Server Attributes into the MiCollab IDS Attributes Mapping page.
17. If user service data and Active Directory Authentication are synchronized for all users, specify any user records that you do not want to receive changes from the directory service. To prevent a user record from receiving updates from the directory server:

    - Under **Applications** , click **Users and Services** .
    - Locate the user using the **Search** function.
    - On the **User** tab in the **Personal Information** section, clear the **IDS Manageable** box.
    - Click **Save** .
18. Schedule synchronizations with the directory server database to occur on a regular basis during off-business hours (for example: daily at 12:00 am). These re-occurring synchronizations keep the MiCollab database up to date with database changes that are entered on the directory server.

    - Under **Configuration** , click **Integrated Directory Service** .
    - Click Edit next to the directory service connection. The Manage IDS connections page opens.
    - Ensure the **Re-initialize on next cycle** box is clear.
    - In the **Schedule** field, set the schedule using the drop-down menus.
    - Click **Save** .
19. Perform a full synchronization from MiCollab with the directory server database..
20. Resolve any detained IDS updates on MiCollab .
21. After the full synchronization is complete and you have resolved the detained updates, both the MiCollab and MiVoice Business databases match the directory server database.

30.16 Migrate MiCollab with MiCollab Audio, Web and Video Conferencing IDS to MiCollab IDS

Migration of MiCollab Audio, Web and Video Conferencing IDS to MiCollab IDS must be performed manually. You must copy the IDS settings from the MiCollab Audio, Web and Video Conferencing AD/LDAP pages to the corresponding fields in the MiCollab IDS Connection and Attribute Mapping pages. Leave any MiCollab IDS fields that don't have corresponding fields at the defaults.

1. Review the General Guidelines and Limitations for MiCollab IDS.
2. Log into MiCollab server manager.

3. Under **Applications** , click **Audio, Web and Video Conferencing**.
4. Under **Configuration** , click **LDAP Configuration.**
5. Display the Lightweight Directory Access Protocol form. Record the current MiCollab Audio, Web and Video Conferencing LDAP Configuration connection values in the third column of the following table. Use the table to match the MiCollab Audio, Web and Video Conferencing LDAP Configuration connection settings to the MiCollab IDS Connection parameters.

MiCollab Audio, Web and Video Conferencing LDAP Configuration Settings	Corresponding MiCollab IDS Connection Parameters	Current MiCollab Audio, Web and Video Conferencing LDAP Configuration Settings
Use LDAP		
LDAP Port Number	LDAP port	
LDAP Admin ID	Distinguished name	
LDAP Uid Field		
Auto Synchronize	Enable synchronization	
LDAP Server Name	Primary directory server	
LDAP Search Base	Search	
LDAP Admin ID Password	Password	
Email Domain		
Sync Interval	Sync schedule	

6. Synchronize the MiCollab Audio, Web and Video Conferencing database with the directory server database.
7. Disable IDS (LDAP Integration) for the MiCollab Audio, Web and Video Conferencing application.
   - Click **Audio, Web and Video Conferencing** in the MiCollab server manager.
   - Click LDAP Configuration.
   - Click User LDAP check box.
8. On MiCollab in the Network Element tab of the Users and Services application, disable Single Point Provisioning.
9. Create a MiCollab synchronization account on the directory service domain. The account must have read access.
10. If LDAP Authentication is required, ensure that a valid Certificate Authority (CA) has been configured for Active Directory. If LDAP Authentication is not required, you assign users new passwords on MiCollab using roles and associated user templates.
11. On the directory server, ensure that the user data fields contain entries for the following attributes: samAccountName, givenName, sn, and distinguishedName. Otherwise, failed update errors are generated on MiCollab during the synchronization. If an employeeType field is not specified the entry is sent to the detained queue.
12. In the MiCollab Users and Services application, create user templates for the various roles in the enterprise. In the templates, assign the phone and application services that you want to apply to the user data that is obtained from the directory server. In the templates, also set a password policy for the user data. You have the option of creating these templates from the UCC default templates.
13. In the MiCollab Users and Services application, create roles that correspond to the employeeType attribute entries on the directory service. You can create these roles from the UCC default roles. Note that when users are obtained from the directory server, if a user entry has a blank employeeType field, the update is sent to the detained user updates queue.

14. Create a connection to the directory server:

    - Under **Configuration** , click **Integrated Directory Service** .
    - Click **Add connection** . The Add Integrated Directory Service connection page opens.
    - Complete the fields to create a connection. When you configure the IDS Connection Parameters on MiCollab, transfer the "Current MiCollab Audio, Web and Video Conferencing LDAP Configuration Settings" that you recorded in the table above into the MiCollab IDS Connection page. See Manage IDS Connections for field descriptions.
    - If Active Directory Authentication is required, the Synchronization option must be enabled. Also, set the **Connection Method** to either TLS or TSL/SSL. The **Connection Method** cannot be Unsecured.

    Note:
    To use SSL/TLS for IDS, LDAP over SSL must enabled on the active directory server. See the following links for more information:

    - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772393(v=ws.10)?redirectedfrom=MSDN
    - https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
    - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee411009(v=ws.10)?redirectedfrom=MSDN
    - Click **Save** . MiCollab verifies the connection parameters and indicates if any errors are present.

15. Configure Active Directory Authentication if required.

    - Check the **Enable authentication** box beside the desired domain. You can only enable Active Directory Authentication on a single domain. So, if you want to select a different domain, you must first disable the currently selected domain.

      Note: You can connect the Active Directory Authentication to a Global Catalogue on the domain controller. If multiple connections are used, and if those connections point to domains which are under the same forest, you can configure one connection to use the global catalogue. With global catalogue enabled, all users from all connections under the same forest should be able to authenticate. Note that using global catalogue limits the fields that can be used for synchronization.
    - Secure authentication requests are required as part of the IDS connection.
    - Click **Save.**

16. If your server is using the default LDAP attributes, you should not need to modify the IDS Attribute Mappings. However, if your server is using non-default LDAP attributes, you must modify the associated attribute mappings.
17. By default, user service data and Active Directory authentication are synchronized for all users. Specify any user records that you do not want to receive changes from the directory service. To prevent a user record from receiving updates from the directory server:

    - Under **Applications** , click **User and Services** .
    - Locate the user using the **Search** function.
    - On the **User** tab in the **Personal Information** section, clear the **IDS Manageable** box.
    - Click **Save**.

18. Schedule synchronizations with the directory server database to occur on a regular basis during off-business hours (for example: daily at 12:00 am). These re-occurring synchronizations keep the MiCollab database up to date with database changes that are entered on the directory server.

    - Under **Configuration** , click **Integrated Directory Service** .
    - Click Edit next to the directory service connection. The Manage IDS connections page opens.
    - Ensure the **Re-initialize on next cycle** box is clear. The re-initialize option is only required for a full synchronization, and by default, is not required during initial configuration. It is typically used to recover from database corruption.
    - In the **Schedule** field, set the schedule using the drop-down menus.
    - Click **Save** .

19. Perform a full synchronization from MiCollab with the directory server database. The user entries are not distributed to the MiVoice Business because SPP is disabled.
20. Resolve any detained IDS updates on MiCollab. After the full synchronization is complete and you have resolved the detained updates, both the MiCollab and MiVoice Business databases match the directory server database.

30.17 Migrate MiCollab with MiCollab Client IDS to MiCollab IDS

Migration of MiCollab Client IDS to MiCollab IDS must be performed manually. You must copy the IDS settings from MiCollab Client into the corresponding fields in the MiCollab IDS Connection page and IDS Attributes Mappings page.

1. Review the General Guidelines and Limitations.
2. Under **Applications**, click **MiCollab Client Service**.
3. Under **Configuration**, click **Configure MiCollab Client Service**.
4. Click the **Synchronization** tab.
5. Click **Active Directory/LDAP Synchronizer** and then click the LDAP link.
6. Click **Connection Settings** to display the AD/LDAP Connection Settings. Use this table to match the MiCollab Client AD/LDAP settings with the corresponding MiCollab IDS Connection page settings.

MiCollab Client AD/LDAP Connection Settings	MiCollab IDS Connection Parameters
Description	Primary Directory Server
Domain name	Domain
Show LDAP Path Assistant	
LDAP path	
Server supports paging results	
Do not import disabled accounts from AD	
Search contents	Search scope
User Query	
Username	Distinguished name

MiCollab Client AD/LDAP Connection Settings	MiCollab IDS Connection Parameters
Password	Password
Default feature profile	
Timestamp	
Timestamp attribute	
Timestamp syntax	

7. Click **Field Mappings** to display the AD/LDAP field attributes. The following table maps the default MiCollab Client IDS field attributes to the MiCollab IDS field attributes..

MiCollab Client Attribute	Directory Server Default Attribute	MiCollab Attribute
COMMON ATTRIBUTES		
		Direct Inward Dial Number
Directory key	objectGUID	User ID
Login ID	samAccountName	Login
distinguishedName	distinguishedName	Distinguished Name
mail	mail	Email
First name	givenName	First Name
Last name	sn	Last Name
Desk phone extension	ipPhone (See Note 1 below)	Home Element
	MiCollab ONLY	
	department	Department
	telephoneNumber	Directory Number
	mobile	Mobile Phone Directory Number
	objectClass	Object Class
	otherTelephone	Secondary Phone Directory Number
	preferredLanguage	Language
	physicalDeliveryOfficeName	Location
	employeeType	Role
MiCollab Client ONLY		
Middle name	initials	
Soft phone extension	otherIpTelephone	
PBX Node	facsimileTelephoneNumber	
Company name	company	
Address	streetAddress	

MiCollab Client Attribute	Directory Server Default Attribute		MiCollab Attribute
City	l		
State/Province	st		
ZIP/Postal code	postal code		
Display picture	jpegPhoto		

Note:
If you are migrating from MiCollab Client , you must either clear ipPhone attribute from the directory server or enter a different attribute.

8. Synchronize the MiCollab Client database with the directory server database.
9. Disable IDS (LDAP Integration) for the MiCollab Client application:
   - Click **MiCollab Client Service** in the MiCollab server manager.
   - Click **Configure MiCollab Client Service**.
   - Click the **Synchronization** tab.
   - Click **None** and click **Apply**.
10. Run the MiCollab Client Integration Wizard.
    - In the MiCollab server manager, under **Configuration** click **MiCollab Client Configuration Wizard**.
    - Follow the screen prompts provided in the wizard screens.
11. On MiCollab in the Network Element tab of the Users and Services application, disable Single Point Provisioning.
12. Create a MiCollab synchronization account on the directory service domain. The account must have read access.
13. If Active Directory Authentication is required, ensure that a valid Certificate Authority (CA) has been configured for Active Directory. If LDAP Authentication is not required, you assign users new passwords on MiCollab using roles and associated user templates.
14. On the directory server, ensure that the user data fields contain entries for the following attributes: samAccountName, givenName, sn, and distinguishedName. Otherwise, failed update errors are generated on MiCollab during the synchronization. If an employeeType field is not specified the entry is sent to the detained queue.
15. In the MiCollab Users and Services application, create user templates for the various roles in the enterprise. In the templates, assign the phone and application services that you want to apply to the user data that is obtained from the directory server. In the templates, also set a password policy for the user data. You have the option of creating these templates from the UCC default templates.
16. In the MiCollab Users and Services application, create roles that correspond to the employeeType attribute entries on the directory service. You can create these roles from the UCC default roles. Note that when users are obtained from the directory server, if a user entry has a blank employeeType field, the update is sent to the detained user updates queue.

17. Create a connection to the directory server:

    - Under **Configuration**, click **Integrated Directory Service**.
    - Click **Add connection**. The Add Integrated Directory Service connection page opens.
    - Complete the fields to create a connection. When you configure the IDS Connection Parameters on MiCollab , transfer the "Current MiCollab ClientAD/LDAP Connection Field Values" that you recorded in the first table into the MiCollab IDS Connection page. See Manage IDS Connections for field descriptions.
    - If Active Directory Authentication is required, the Synchronization option must be enabled. Also, set the **Connection Method** to either TLS or TSL/SSL. The **Connection Method** cannot be Unsecured.

    Note:
    To use SSL/TLS for IDS, LDAP over SSL must enabled on the active directory server. See the following links for more information:

    - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772393(v=ws.10)?redirectedfrom=MSDN
    - https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
    - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee411009(v=ws.10)?redirectedfrom=MSDN
    - Click **Save**. MiCollab verifies the connection parameters and indicates if any errors are present.

18. Configure Active Directory Authentication if required.

    - Check the **Enable authentication** box below the desired domain. You can only enable authentication on a single domain. So, if you want to select a different domain, you must first disable the currently selected domain.

      Note: You can connect the LDAP Authentication to a Global Catalogue on the domain controller. If multiple connections are used, and if those connections point to domains which are under the same forest, you can configure one connection to use the global catalogue. With global catalogue enabled, all users from all connections under the same forest should be able to authenticate. Note that using global catalogue limits the fields that can be used for synchronization.
    - Secure authentication requests are required as part of the IDS connection.
    - Click **Save.**

19. Configure the IDS Attribute Mappings. Transfer any custom Directory Server Attributes that you recorded in the second table into the MiCollab IDS Attributes Mapping page.

    Note:
    If you are migrating from MiCollab Client , you must either clear ipPhone attribute from the directory server or enter a different attribute.

20. By default, user service data and Active Directory authentication is synchronized for all users. Specify any user records that you do not want to receive changes from the directory service. To prevent a user record from receiving updates from the directory server:

    - Under **Applications**, click **User and Services**.
    - Locate the user using the **Search** function.
    - On the **User** tab in the **Personal Information** section, clear the **IDS Manageable** box.
    - Click **Save**.
21. Schedule synchronizations with the directory server database to occur on a regular basis during off-business hours (for example: daily at 12:00 am). These re-occurring synchronizations keep the MiCollab database up to date with database changes that are entered on the directory server.

    - Under **Configuration**, click **Integrated Directory Service**.
    - Click Edit next to the directory service connection. The Manage IDS connections page opens.
    - Ensure the **Re-initialize on next cycle** box is clear.
    - In the **Schedule** field, set the schedule using the drop-down menus.
    - Click **Save**.
22. Perform a full synchronization from MiCollab with the directory server database. The user entries are not distributed to the MiVoice Business because SPP is disabled.
23. Resolve any detained IDS updates on MiCollab .
24. After the full synchronization is complete and you have resolved the detained updates, both the MiCollab and MiVoice Business databases match the directory server database.

30.18 IDS Synchronization Overview

The system automatically determines if user entries in the MiCollab database and the directory server database are a matching pair based on a variety of criteria. If the user entries are identified as a match, the system automatically links the accounts and copies the data from the directory service entry to the MiCollab entry. If minor discrepancies exist between directory service attributes and the user specific fields (e-mail, first name, login ID, and so forth), the directory service data is applied to the MiCollab entry. However, if discrepancies exist between the telephony fields (Prime DN, Other Telephone, or EHDU external number), the MiCollab entries are not updated.

After a user is paired, the mapping is stored on the system. The mapping remains unless the IDS Manageable option is unchecked.

If you create a new user on the directory service and the user name (first name, last name) and login ID match an existing user in the MiCollab database, the update operation will be blocked and fail on MiCollab in the following circumstances:

- **The same user already exists in MiCollab and both users have roles:** At creation time, MiCollab will prompt for domain, user name, and login ID. If these fields match the fields of an existing user, the operation fails.
- **The same user already exists in MiCollab but only the new user has a role:** At creation time, MiCollab will prompt for domain, user name, and login ID. If these fields match an existing user, the operation fails. The role is not applied because the user already exists.
- **Both the new user and current user have the same role but the current user doesn't have all services provisioned for that role:** At creation time, MiCollab prompts for domain, user name, and

login ID. If these fields match an already existing user, the operation fails. The role is not applied because the user already exists.

- **The matching users in the directory service and MiCollab databases have different telephone numbers:** The operation is sent to the detained user updates queue.

30.19 Scheduling IDS Synchronizations

After IDS has been programmed, use the following procedures to schedule data synchronization events:

- **Initial IDS Synchronization** : allows you to seed a new MiCollab system with the entries from the directory service.
- **Incremental IDS Synchronization** : allows you to query the directory server for new and modified user records on a scheduled basis. Because incremental synchronizations do not search for deleted user records, they are quicker than full synchronizations.
- **Full IDS Synchronization** : allows you to perform a full IDS synchronization to query the directory server for new, modified, and deleted user records. Because a full synchronization searches for the full range of updates—deletions as well as new and modified records—it has intensive processing requirements and should only be performed to recover the MiCollab database from the directory service.

To schedule IDS synchronization events, refer to the following procedures:

Note:
It is recommended that you enable the **Detain all operations** option when you schedule an IDS synchronization event. This setting allows you to review the updates before allowing the synchronization to proceed. The synchronization operations are held in the **Manage Detained Queue** until you process them.

Note:
You cannot create users by performing an Integrated Directory Services sync using a connection to a Mitel MetaDirectory because all the entries in MetaDirectory are treated as contacts in MiCollab.

Perform an Initial IDS Synchronization

To perform a initial synchronization after the installation of a new MiCollab system:

1. Under **Configuration**, click **Integrated Directory Service**..
2. Ensure that the **Synchronization** box is checked for the connection.
3. Click the **Sync** link.

Schedule an Incremental IDS Synchronization Event

To create an incremental IDS synchronization event:

1. In the MiCollab server manager interface, under **Configuration**, click **Integrated Directory Service**..
2. Ensure that the **Synchronization** box is checked for the connection.
3. Click **Edit** next to the directory service connection.
4. Ensure the **Re-initialize on next cycle** box is clear.
5. In the **Schedule** field, set the schedule using the drop-down menus.
6. Click **Save**

Schedule a Full IDS Synchronization Event

To schedule a full IDS synchronization event:

1. In the MiCollab server manager interface, under **Configuration**, click **Integrated Directory Service**.
2. Ensure that the **Synchronization** box is checked for the connection.
3. Click **Edit** next to the directory service connection.
4. Check the **Re-initialize on next cycle** box.
5. In the **Schedule** field, set the schedule using the drop-down menus.
6. Click **Save**.

30.20 Add, Edit and Delete Entries using IDS

The following sections describe the effects of adding, editing, and deleting entries from the directory service and from the MiCollab USP application. It's recommended that you add, edit, and delete all IDS managed entries from the directory service and use roles and templates to assign data to the MiCollab fields that are not supported in the directory service.

Adding Entries

Add a Directory Service user: When you add a user entry to the directory service, the user is added to the directory server and the data in the mapped attribute fields are copied to the MiCollab system on the next synchronization event. When creating the entry, ideally complete the following fields:

- givenName,
- sn,
- samAccountName,
- distinguished name,
- telephoneNumber,
- mail,
- employeeType (in this field, assign a MiCollab role that references a template with the desired services. The user data will be updated in the MiCollab USP. The role references a template that assigns the appropriate phone services and applications to the entry on MiCollab. If SPP is enabled, the user and phone services will also be automatically programed on the MiVoice Business platform).

Add a MiCollab user: When you add a user entry in MiCollab USP, the user is created in MiCollab. Even if the IDS managed box is checked, the directory service is not updated with the new entry. Synchronization only occurs from the directory service to MiCollab . However, if a matching user entry is already present in

the directory service, the entries are paired on the next synchronization interval. Additionally, if a role and template are assigned, the services are provisioned for the user.

Editing Entries

If you edit an entry from the directory service:

- **Move the user to another domain**. If both the previous and new domains (domains must belong to the same forest) are managed by IDS, the user's domain is updated in MiCollab to reflect the new directory server domain. If the previous domain was not managed or was not detected by IDS, and the user's new domain is not managed by IDS, the user is deleted from MiCollab.
- **Move the user to another OU**. If both the previous and new OUs are managed by IDS, the user's distinguished name is updated in MiCollab and the user remains synchronized. If the new OU is not managed by IDS, the user is not deleted; however, any future updates will not be synchronized with MiCollab.
- **Update a Directory Server field which is mapped in MiCollab.** The update is applied to the matching entry in MiCollab.
- **Update a Directory Server field which is not mapped in MiCollab**. The update is not applied to the matching MiCollab entry.
- **Edit the Directory Server role attribute.** No changes occur if the user is present in MiCollab. The role is only applied when you create a user in MiCollab using Quick Add or from the Bulk User Provisioning tool.
- **Update telephone Number from the Directory Server:** MiCollab does not update the phone service. The update is ignored.

If you manage entries locally from MiCollab :

- **Mapped fields:** When a user is managed by IDS, the Directory Server update is applied to the MiCollab entry on the next synchronization. Note that if you have made user edits locally on MiCollab through User and Services, those edits will be overwritten with the data from the directory server.
- **Unmapped fields:** The field is updated in MiCollab only. The update is not made to the directory service. Data is only synchronized in one direction, from the directory service to MiCollab.
- **Add, edit, remove role attribute:** When a user is managed by IDS. If the user's role is changed, no changes occur to the user and his services because the user is already provisioned.

Deleting Entries

If you delete a user entry from the directory service:

- **Delete IDS managed user from the Directory Server**: The user is deleted from MiCollab and from the MiVoice Business if SPP is enabled. This includes all services provisioned against that user. Note that voice mails are deleted and cannot be recovered.
- **Clear IDS Managed user field from the Directory Server**: The data in the IDS managed fields is removed from the entry on MiCollab. Synchronization and Authentication will be disabled.
- **Delete telephone Number from the Directory Server**: Deleting a telephone Number field in the DS does not delete the user's phone service on MiCollab. This operation is ignored.

If you delete a user entry locally from MiCollab :

- **Delete IDS managed user from MiCollab.** The user is deleted in MiCollab. However, if the user is detected again in the directory service database during a MiCollab-IDS synchronization, the user is re-created in the MiCollab database.

- **Delete service from IDS user in MiCollab.** The service is removed for that user. Since the user is still in the MiCollab database, the role from subsequent IDS updates are not applied to the record. The service remains deleted.

30.21 Non-Corporate Contacts

Description

Non-corporate contacts are external directory entries, such as material or equipment suppliers that are listed in the MiCollab Client corporate directory. They are not MiCollab system users, and as such, are not assigned with MiCollab application services, and are not listed in the User and Services application directory. Non-corporate contacts are typically configured only with a name, external phone number, and an e-mail address. This type of contact does not have an associated login ID or password and does not consume licenses on the system.

You can assign entries in the Active Directory database as non-corporate contacts and IDS will automatically update the MiCollab Client Corporate Directory with them during the next synchronization event. During the IDS synchronization, the system applies the default "Contact" role and the associated default " MiCollab Client " template to the non-corporate entries. When users start up their MiCollab clients, the system updates the user's Contacts list. Users can then place calls to the non-corporate contacts using "click to call" functionality from their phone clients.

Users and non-corporate contacts that are obtained from the directory service via IDS are organized into groups in the MiCollab Client Enterprise corporate directory based on the Distinguished Name attribute. The Organizational Unit (OU) information in the Distinguished Name attribute defines the group names in the MiCollab Client corporate directory. Non-corporate contacts that are assigned to an Organizational Unit in Active Directory are inserted into a corresponding group in the MiCollab Client corporate directory. Below are examples of Distinguished Names for three non-corporate contacts:

cn=acme heating and cooling, ou=maintenance, dc=maslab, dc=local

cn=vista paper products ltd, ou=suppliers, dc=maslab, dc=local

cn=jy office supplies, ou=suppliers, dc=maslab, dc=local

Conditions

- To support this functionality MiCollab Client must be configured in Integrated Mode.
- By default, MiCollab Release 6.0 SP1 and later systems are configured to synchronize with the users and non-corporate contacts that are contained in the Active Directory database.
- Prior to MiCollab Release 6.0 SP1 only user contacts were synchronized. If you upgrade a pre-Release 6.0 SP1 system to Release 6.0 SP1 or later, you must manually configure the system to synchronize non-corporate contacts.
- The following directory service fields are not imported via MiCollab IDS: Middle name, Address, City, State/Province, ZIP/Postal code, and Display picture.
- A maximum of three phone numbers are supported per non-corporate contact in MiCollab Client .
- Users that you create manually from the USP Add or Quick Add forms are not configured with a Distinguished Name and therefore are not listed in a contact group. Instead, they are listed in the top level of the MiCollab Client corporate directory.
- You cannot import non-corporate contacts via a CSV or LDIF file from the Bulk User Provisioning tool.

- Non-corporate contacts that are synchronized from the directory service are displayed as read-only in the Bulk User Provisioning tool.
- The Manage Detained Queue in the *Bulk User Provisioning* tool lists any non-corporate contacts that have been detained or have failed. The Role field displays "Contact" for non-corporate contacts..
- The default "Contact" role and template are not included in the User Template or User Role lists of USP and you cannot apply the default "Contact" role to a user from the USP Quick Add form. The default Contact role and template are only applied to contacts imported from Active Directory.
- Contacts are not shared with MiVoice Business database even if Single Point Provisioning is enabled.

Define the Non-Corporate Contacts on Active Directory

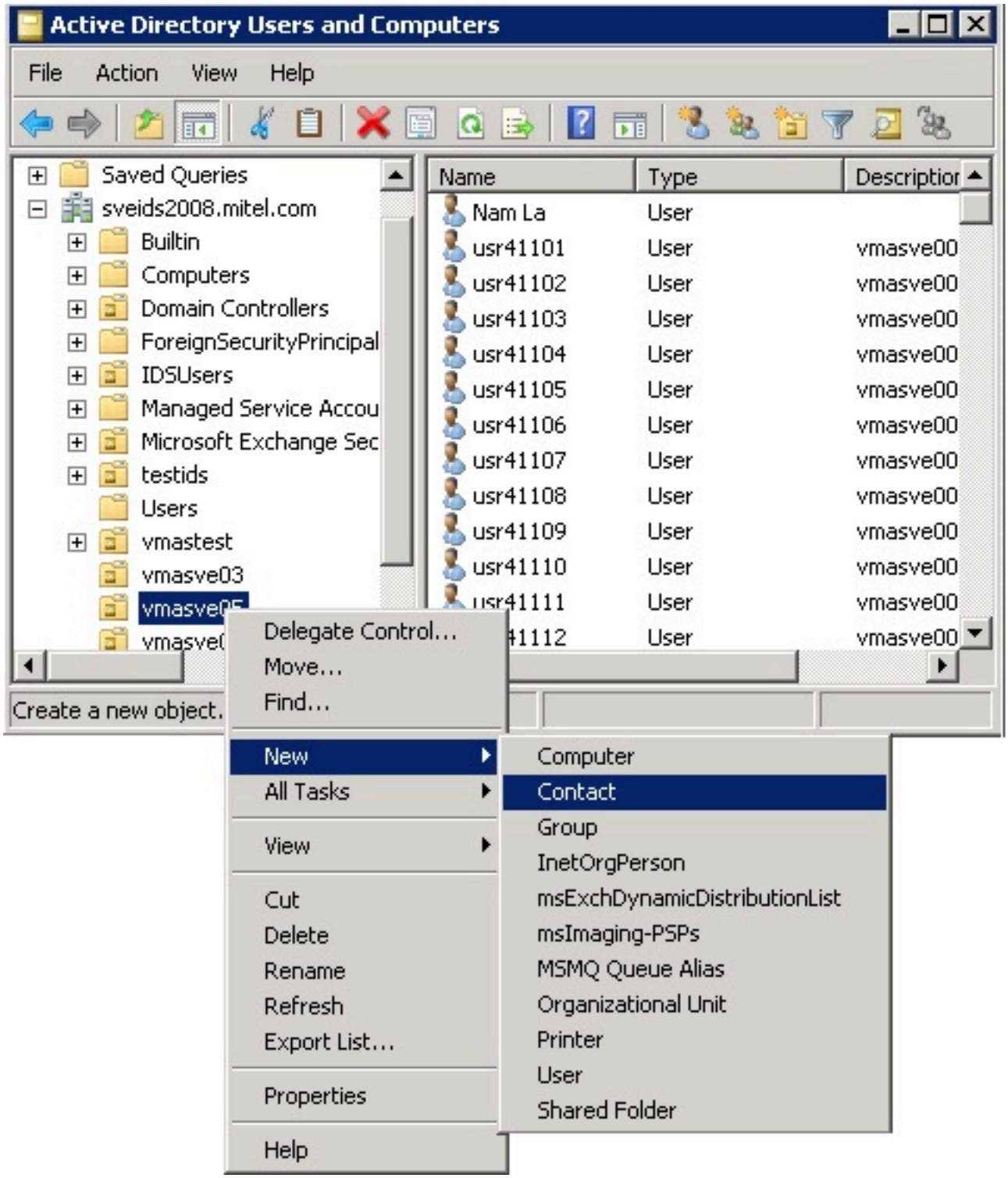
You can specify Active Directory entries as MiCollab Client non-corporate contacts using either of the following methods:

Create a Non-Corporate Contact

To create a non-corporate contact on Active Directory:

1. Log into Active Directory as administrator.
2. Click **Start > Active Directory Users and Computers**.
3. Select the Organizational Unit (OU) for the contacts.

4. Right-click and select **New > Contact**.

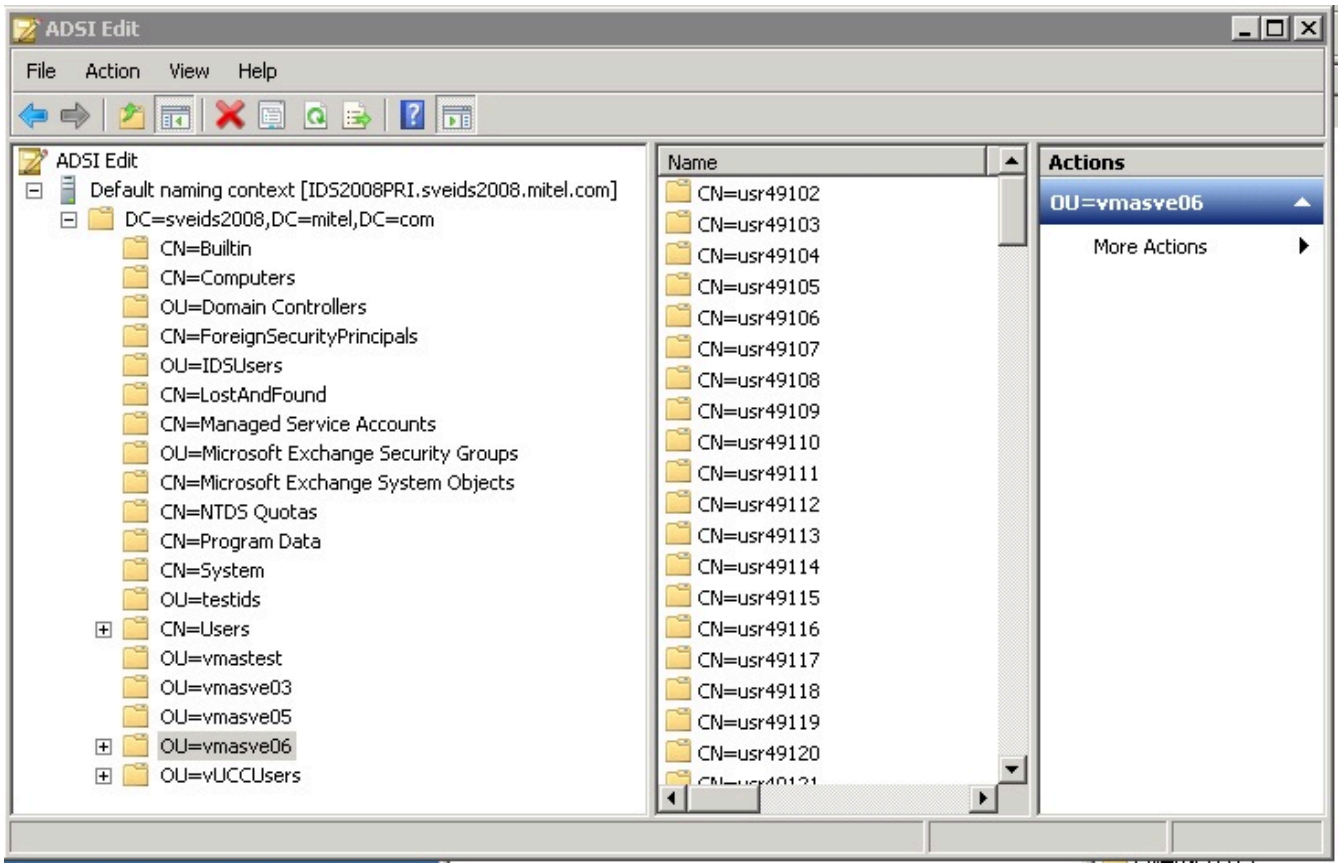


5. Complete the Contact fields. When the databases are synchronized, MiCollab IDS adds the directory entry as a non-corporate contact.

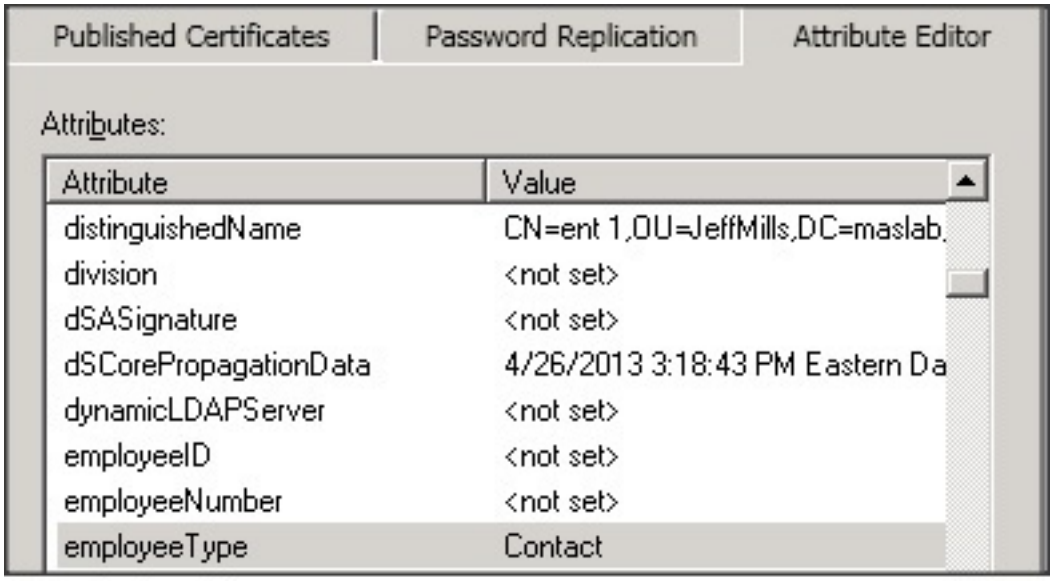
Change an Existing Active Directory Entry to a Non-Corporate Contact

To change an Active Directory user entry to a non-corporate contact.

1. Log into Active Directory as administrator.
2. Click **Start > ADSI Edit**. The ADSI Edit window opens.



3. Open the Organizational Unit (OU) of the users.
4. Select the user.
5. Right-click and select **Properties**. The user's Properties window is displayed.
6. On the **Attribute Editor** tab, set the "employeeType" attribute to "Contact". By default, MiCollab maps the "employeeType" attribute to the "Role" attribute.



7. When the databases are synchronized, MiCollab IDS changes the entry into a non-corporate contact.

Configure MiCollab IDS to Synchronize User Entries and/or Non-Corporate Contacts

By default MiCollab IDS synchronizes the user entries and non-corporate contacts in the directory service database with the MiCollab Client corporate directory. You can configure MiCollab IDS to synchronize only users, only non-corporate contacts, or both users and non-corporate contacts:

1. Log into the MiCollab server manager.
2. Under **Configuration**, click **Integrated Directory Service**.
3. Under **Actions**, click Edit .
4. Set the Default query string field:

To import	Set Default Query String field to . . .	Result
Users and contacts (default)	|(ObjectClass=user)(ObjectClass=contact)	Directory service entries with object Class set to "user" are added to the USP and MiCollab Client directories as user entries; Directory service entries with Object Class set to "contact" are added to the MiCollab Client directory as non-corporate contacts.
Users only	(ObjectClass=user)	Directory service entries with object Class set to "user" are added to the USP and MiCollab Client directories as user entries.
Contacts only	(ObjectClass=contact)	Directory service entries with object Class set to "contact" are added to the MiCollab Client directory as non-corporate contacts.

5. Click **Save**.
6. Perform a Full IDS Synchronization. Ensure that the **Re-initialize on next cycle** box is checked when you perform the sync. If you perform a the sync with this box unchecked, your existing contacts will not be listed in the MiCollab Client corporate directory.

30.22 Teamwork Mode Users

Description

Teamwork Mode allows MiCollab Client users who are not assigned a Mitel phone to have a basic level of MiCollab Client functionality. If a MiCollab Client user has no phones associated with their account, the user is automatically placed in Teamwork Mode. Teamwork Mode supports features such as contact grouping, presence, dynamic status, and chat.

You can assign entries in the Active Directory database as Teamwork Mode users and IDS will automatically update the MiCollab Client Corporate Directory with them during the next synchronization event. During the IDS synchronization, the system applies the default "Teamwork Mode User" role and

the associated default " MiCollab Client Teamwork Mode User" template to Teamwork Mode entries. The template contains the user information and MiCollab Client Service settings. The template applies the Teamwork Mode Feature Profile without any desk phone extension or soft phone extension. It also applies a default password of "default" and a default pass code of "1111" to the Teamwork Mode user.

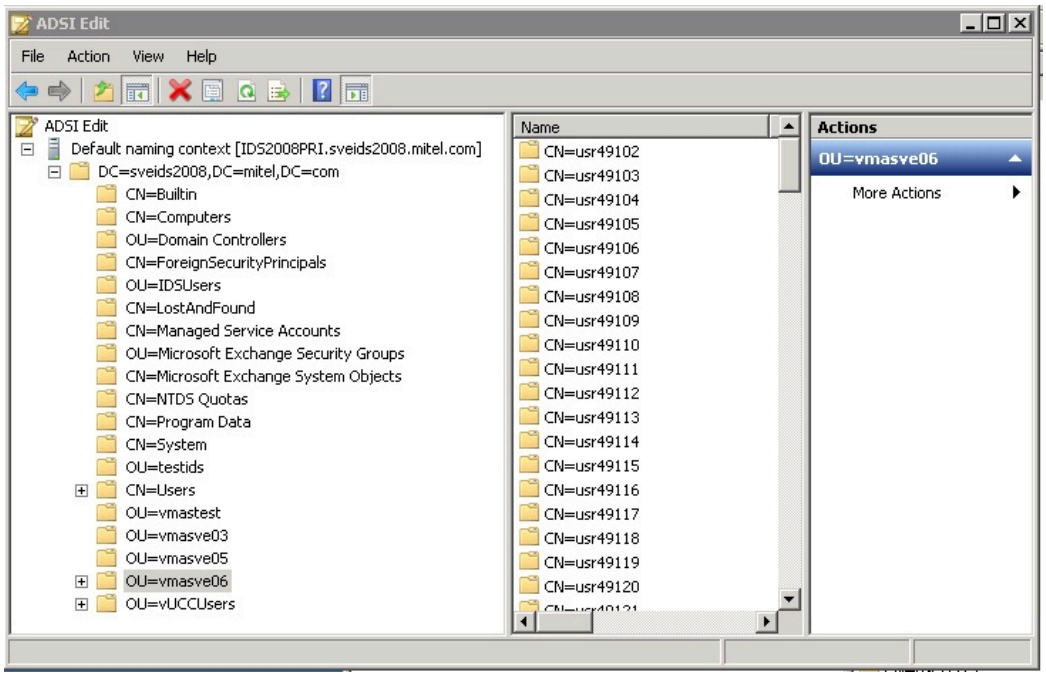
Conditions

- Teamwork Mode users get phone numbers assigned to them from Active Directory.
- To support this functionality MiCollab Client must be configured in Integrated Mode.
- By default an Active Directory entry that has the home element field mapped to the local FQDN of the MiCollab server will have the "Teamwork Mode User" role associated with it.
- During an upgrade to MiCollab Release 6.0 SP1 or later, if the system has an existing role with the name "Teamwork Mode User" or an existing template with the name " MiCollab Client Teamwork Mode User" these templates are renamed "Teamwork Mode User(1)" and " MiCollab Client Teamwork Mode User(1)" respectively.

Assign Teamwork Mode User

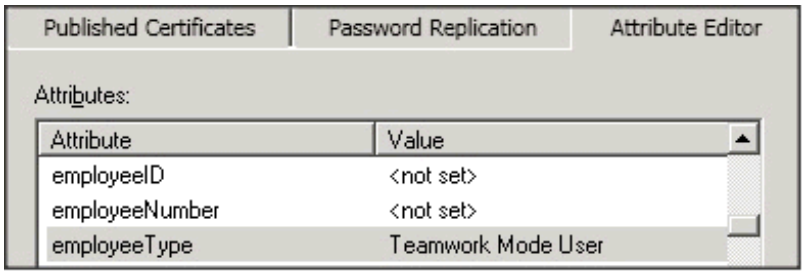
To designate an Active Directory user as a Teamwork Mode user:

1. Log into Active Directory as administrator.
2. Click **Start > ADSI Edit**. The ADSI Edit window opens.



3. Open the Organizational Unit (OU) of the users.
4. Select the user.
5. Right-click and select **Properties**. The user's Properties window is displayed.

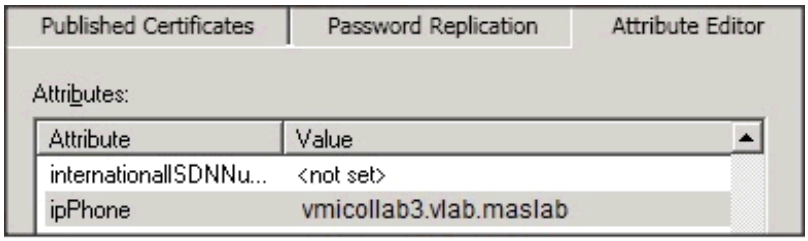
6. On the **Attribute Editor** tab, set the "employeeType" attribute to "Teamwork Mode User". When the databases are synchronized, the user is added to the MiCollab system database in Teamwork Mode. This is the recommended method of designating an Active Directory entry as a Teamwork Mode user.



OR

On the **Attribute Editor** tab, set the "ipPhone" attribute to **<enterpriseID>.local** where <enterpriseID> is the hostname of the MiCollab server. In the following example vmicollab3.vlab.maslab is the hostname of the MiCollab server.

7. When the databases are synchronized, the user is added to the MiCollab system database as a Teamwork Mode user.



30.23 Partitioning the External (Off-board) Directory

You can partition (filter) the external corporate directory such that users are only presented a subset of the corporate directory contact entries. For example, supplier contacts could be excluded from the directories of users who do not need to call these numbers.

You can partition the directory by organizational unit or by attribute:

- **Organizational unit**: When users perform a search, the results are only drawn from the entries in their organizational unit.
- **Attribute**: When users perform search, only results that share the same attribute are presented

Conditions

- Directory partitioning is limited to corporate contacts only. It is not supported for users.
- Users can place calls to contacts that do not appear in their directories (that is, users can still place calls to contacts that have been filtered out).
- An SSL connection to the external directory is not supported.

- If you are partitioning an external directory for a deployment that includes MiVoice Business with Flow Through Provisioning enabled, you must configure the organizational units for the department and location containers in the meta directory without accented characters (see Special Accent Handling for Flow Through Provisioning for details).
- MiCollab Client strips the punctuation and performs transliteration (applies accents) when doing external searches on Generic LDAP connections for all PBX integrations to cover MiVoice Business without Flow Through Provisioning and MiVoice MX-ONE cases.

Partition by Organizational Units

To partition (filter) the MiCollab Client corporate contact directory by organizational unit:

1. Under **Configuration**, click **Integrated Directory Service**.
2. In the **Actions** column for the desired domain, click **Edit**. The Integrated Directory Service connection page opens.
3. Check the **External search** box.
4. In the **Partition attribute** field, select the attribute that you want to use to filter out contacts from the corporate directory. You can select one of the following: None, City, Company Name, Country, Department, Info, Info 2, Language, Location, Position, Postal/ZIP Code, Street or Title.
5. In the **Partition method** field, select **organizational unit**.
6. Click **Save**.

Example:

In Active Directory, the following organizational units have been created to contain the contacts for the company:

OU=Contacts,OU=Kanata,DC=Mitel,DC=gov

OU=Contacts,OU=Denver,DC=Mitel,DC=gov

OU=Contacts,OU=Toronto,DC=Mitel,DC=gov

The company directory includes the contact numbers of product suppliers. The majority of users do not call these suppliers; however, the purchasing agents in each city (Kanata, Denver, or Toronto) need access to these contacts to place orders for product. In this case, you want the purchasing agents to only see the supplier contacts that are located in their city.

In Active Directory tag the supplier contacts with a custom "supplier" attribute. Also, tag the purchasing agents who need access to the supplier contacts with the "supplier" attribute. Then, in the MiCollab IDS Mapping form, map the custom "supplier" attribute to an MiCollab IDS attribute (for example, the "Info" attribute).

To partition the corporate directory such that only purchasing agents see the supplier contacts in their city (organizational unit):

- Set the Partition search attribute to "Info".
- Set the Partition method to "organizational unit".

In this case, the system partitions the corporate directory based on the "Info" attribute within each organizational unit. Users with the "Info" attribute will see their local supplier contacts listed in their corporate directories.

Partition by Attribute

When you partition (filter) the external corporate directory by attribute, users who perform a search will only find directory entries that share the same attribute.

To partition the MiCollab Client corporate contact directory by attribute:

1. Under **Configuration**, click **Integrated Directory Service**.
2. In the **Actions** column for the desired domain, click **Edit**. The Integrated Directory Service connection page opens.
3. Check the **External search** box.
4. In the **Partition attribute** field, select the attribute that you want to use to filter out contacts from the corporate directory.
5. In the **Partition method** field, select **attribute**.
6. Click **Save**.

Example:

Users are assigned to one of three departments: Marketing, Sales and Purchasing.

To partition the corporate directory such that users only see the contacts in their own department:

- Set the Partition search attribute to "department".
- Set the Partition method to "attribute".

30.24 Add External Numbers

You can add external numbers (such as a user's cell phone number or home number) to the MiCollab Client corporate directory so that other MiCollab Client users can place calls to the numbers.

External numbers can be added either

- manually from the Users and Services applications, or
- automatically from Active Directory server via Integrated Directory Services, or
- from a CSV file (see Bulk Import from File)

Requirements and Conditions

- MiCollab must be configured with MiCollab Client in integrated mode.
- For Teamwork Mode users, the primary, secondary, and mobile numbers also appear in the MiCollab Client clients.
- For Integrated Directory Server integrations, any contacts that are imported from the Active Directory server will also have the Mobile Phone 2 number added to their MiCollab Client.

Limitations

- On upgrade to MiCollab Release 7.2 SP1 or later, external numbers for existing ‘Other PBX Phones’ in the MiCollab database are NOT migrated into the MiCollab Client corporate directory. External numbers must be added either manually or via Integrated Directory Services.
- Although you can configure a DID Service Number for the Primary Phone of a MiVoice Business user, this number is not added to the MiCollab Client corporate directory. Only DID numbers that you enter in the ‘Other PBX Phone’ field are added. The DID Service number field and ‘Other PBX Phone’ field are separate and distinct. The numbers in these fields are not synchronized.
- External numbers are available in the corporate directory of MiCollab Clients and are listed under the user's **Account > Phones** tab in MiCollab Client Service administration interface. External numbers are not listed in the Corporate Directory tab.

Adding External Numbers Manually

To add an external number (such as a cell phone) for a user:

Note:
This procedure applies to MiCollab with MiVoice Business platforms only.

1. Access the User and Services user directory.
2. Edit the user record.
3. Click the **Phones** tab.
4. Click **Add New Phone**.
5. Select "Other PBX Phone" as the Phone Type.
6. Enter the external number.
7. Click **Save**. The External number is available in the corporate directory of MiCollab Clients and is listed under the user's **Account > Phones** tab in MiCollab Client Service administration interface.

Adding External Numbers via Active Directory

External numbers can also be added from Active Directory using Integrated Directory Services.

1. Configure Integrated Directory Services.
2. Ensure that the Direct Inward Dial Number and Mobile Phone Number 2 attributes are mapped to the corresponding Active Directory attributes.
3. Perform an IDS synchronization. The DID numbers and the Mobile Phone 2 numbers are automatically created as ‘Other PBX Phones’ for the users in the Users and Services directory. The numbers now appear in the corporate directory of MiCollab Clients.
4. If you change the DID number and Mobile Phone 2 phone in Active Directory, the change is reflected in the MiCollab Client corporate directory.

30.25 Viewing IDS Detained Operations

A detained update is a synchronization operation that has been not been processed on the MiCollab system. Detained operations occur if you enable the **Detain all operations** option when you schedule an IDS synchronization event. This setting allows you to review the updates before allowing the synchronization to proceed.

Detained updates are collected and displayed in the Manage Detained Queue in the Bulk User Provisioning tool of the USP application. Check this tool frequently to

- view the status of IDS data updates
- identify any updates that require your attention because they have been detained or have failed.

The updates that appear in the list have not yet been applied to the MiCollab database; nor have they been distributed to the MiVoice Business platform.

To view the Manage Detained Queue:

1. Under **Applications,** click **Users and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the Mode field, select **Manage Detained Queue**. The IDS detained and failed updates are listed in the grid.
4. Proceed to Managing Detained and Failed IDS operations.

Note:

A primary email address is mandatory to Quick Add users or Add users from the IDS Detained queue.

30.26 Managing LDIF Files

You can use the Bulk Operation Tool to import and export LDAP Data Interchange Format (LDIF) files.

Import LDIF Files

The **Import from File** option on the **Tools** menu in the Bulk User Provisioning tab allows you to add users to the MiCollab system by importing an LDIF file. During the import, all users are processed serially. As in the synchronization process, the system attempts to pair the users if they are present in both MiCollab and the LDIF file. The system provides a progress bar and a summary of errors. If errors detected, you can edit the errors to correct them. See Import from LDIF File for instructions.

Export LDIF Files

The **Export from File** option on the Tools menu in the Bulk User Provisioning tab allows you to generate and export an archive file. This archive file contains the following files in LDIF format:

- IDS managed users with the domain information
- IDS managed users without the domain information, and
- Non-IDS managed user records.

30.27 LDAP Query Basics

Search filters enable you to define search criteria for effective searches. Go to the following web link, for detailed information and examples.

http://technet.microsoft.com/en-us/library/aa996205(v=exchg.65).aspx

30.28 Filtering out Disabled AD Users from IDS

Below is an example of a query string for filtering out disabled users:

&(|(ObjectClass=user)(ObjectClass=contact))(!(UserAccountControl:1.2.840.113556.1.4.803:=2))

30.29 Managing Detained and Failed IDS Operations

The *Manage Detained Queue* in the *Bulk User Provisioning* tool lists the detained and failed IDS operations:

- Detained IDS operations are operations that have been performed on the directory server that have not been applied to the USP database yet.
- Failed IDS operations are directory server updates that the MiCollab system could not apply to the USP database.

Failed IDS operations are also

- listed in the Event log in the MiCollab server manager
- indicated in the Manage IDS Connection page for the last successful sync (if errors were detected, the connection is highlighted in red).

The Manage Detained Queue lists a maximum of 2500 detained entries in the grid. Any additional detained entries beyond the 2500 limit are stored on the system. After you process detained entries, any additional detained entries are added to the grid when you reload the Manage Detained Queue view.

Note:
Data mismatches that occur between telephony fields are not sent to the Managed Detained Queue because they cannot be reconciled from MiCollab . The following telephony fields are ignored during a synchronization update: Role, Home Element, Mobile Phone Directory Number; Primary Phone Directory Number and Secondary Phone Directory Number.

Note:
When you create a new connection to the directory server, the 'detain always' option is enabled by default. Therefore, during a synchronization all users on the directory server (including Administrator and Guest accounts) are sent to the detained queue. You must remove or ignore the administrator or guest entries from the queue.

Managing IDS Operations

To manage detained and failed IDS operations:

1. Under **Applications,** click **Users and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the Mode field, select **Manage Detained Queue**.
4. Click **Tools**, then click **Reload Detained Queue** to refresh the grid with the latest detained entries from the directory server.
5. Review the list of **A** (Add), **U** (Update) and **D** (Delete) operations. Errors are identified by icons. Hover your cursor over the icons for a description of the error.

   For **U** (Update) operations, the field values that will be deleted or modified are indicated by strike though text; the new values appear in **bold** text; and any values that will not be changed appear in normal text. Hover your cursor over an update field to display any additional details.
6. Click
   
   next to an entry to review a detailed summary of the changes that will be applied to the database. If there are any errors associated with the record, a detailed summary of the error is provided. Click **Done**.
7. Correct any errors caused by invalid data.
8. Select any operations that you do not want applied to the database and click **Delete**. Click **OK** to confirm the deletion of the operation from the grid.
9. Select the operations that you want to apply to the database and click **Save**. The Operation Progress window opens and displays the import progress. After the import is complete, the Operation Progress window closes.
10. Perform another IDS sync and check the Manage Detained Queue again to see that the errors are indeed fixed and do not reappear.

Emptying the Detained Queue

You can remove all entries from the Detained Queue quickly using the **Empty Detained Queue** menu option.

To remove all detained entries from queue at once:

1. Under **Applications,** click **Users and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the Mode field, select **Manage Detained Queue**.
4. Click **Tools**, then click **Empty Detained Queue**.

> **Note**:
> If you empty the queue, the entries are removed permanently. You cannot recover them.

5. Click **OK** to proceed. The list is emptied.

30.30 IDS Synchronization Error Handling

Synchronization errors are listed in the server manager Event Logs and identified in the IDS Managed Detained queue.

Synchronization errors are also indicated in the Manage IDS Connections *page. If the domain is invalid, the connection for the domain is highlighted in red, and the Last Synchronization field, indicates that an error occurred.*

If a power outage occurs during synchronization, the system does not attempt to re-synchronize on boot-up. Instead, the system attempts to run the exact same synchronization sequence again on the next interval. You can also click the **Sync** link if you don't want to wait for the next interval. Additionally, any user entries that were created during a synchronization before the power interruption are sent to the detained updates queue, provided that the user already exists in the MiCollab database.

Error	Possible Cause	Corrective Action
Only a subset of the desired directory service data fields are being updated on MiCollab after an IDS synchronization. In the detained queue certain fields are blank even though they are mapped correctly.	If the Global Catalogue Port option is enabled, it reduces the number of fields that are mapped to the MiCollab user records. Certain attributes, for example employeeType, are not visible when connection is made to the global catalogue.	Delete the Global Catalogue Port and perform an IDS synchronization. OR If you want to use global attribute, map the MiCollab attributes to unused attributes in the global catalogue. To determine what attributes are available in the global catalogue, run the following query in the MiCollab server console: ldapsearch -x -h <AD server address> -b "cn=Schema,cn=Configuration,<your domain's DN/distiunguished name>" -D <Distinguished name of account with read priviledges> -w "<password>" "(&(objectClass=attributeSchema)(isMemberOfPartialAttributeSet=TRUE))" lDAPDisplayName
"Failed to contact server(s)"	Mitel Certificate Authority (CA) is not installed on directory server.	Install Mitel Certificate Authority (CA) on directory server. Then, reboot of the AD server

30.31 Troubleshooting LDAP Authentication

Error	Possible Cause	Corrective Action
"Failed to contact server(s)"	Mitel Certificate Authority (CA) is not installed on directory server.	Install Mitel Certificate Authority (CA) on directory server. Then, you must reboot the directory server.
Cannot enable LDAP Authentication	SSL/TLS not enabled on MiCollab	Ensure SSL/TLS is enabled on MiCollab . See Configure LDAP Authentication.
	SSL/TLS not enabled on directory server.	Ensure SSL/TLS is enabled on the directory server.

Error	Possible Cause	Corrective Action
	MiCollab SSL/TLS port settings don't match those on the directory server.	By default, MiCollab IDS uses port 389 for TLS and port 636 for SSL. These defaults are also used by Active Directory. If Active Directory is using different ports, you must change the SSl/TLS port settings in the Manage IDS Connections form to match them. To determine if Active Directory is listening on a specific port, enter the following command from the MiCollab server console: #> telnet <your AD IP> <port #> Example: #> telnet 10.45.102.88 636

30.32 Integrating MiCollab Client Database with USP

The MiCollab Client Integration Wizard allows you to integrate the MiCollab Client Service application database with the USP application database. After the databases are integrated, you can manage MiCollab Client services from the USP application. Single point provisioning of MiCollab Client services from the USP application is supported to the MiVoice Business platforms.

Specifically, the following use cases will no be longer supported by the MiCollab Client Integration Wizard after MiCollab Release 7.0:

- Importing a MiCollab Client Server Database.
- Copying a configuration from MiCollab (UCA) Client Server into MiCollab USP (PBX, accounts).
- Copying a configuration from USP into MiCollab Client Server (Network Elements, Users, Phones).
- Merging MiCollab Client Server database with USP.

If the you need to perform any of these migration tasks, you must do so in MiCollab Release 6.0 SP1 prior to upgrading to MiCollab Release 7.0 or later.

Running the Wizard

1. Before running the wizard, review the requirements and conditions provided in the *MiCollab Client Integration Wizard* chapter of the *MiCollab Installation and Maintenance Guide*.

2. In the server manager menu, under **Configuration**, click **MiCollab Client Integration Wizard**

   or

   Click the MiCollab Client Integration Wizard link in the warning banner at the top of the server manager screens.
3. Follow the instructions provided in the wizard.
4. If you have UCC Premium users or MiVB Subscription Premium and Elite configured, MiTeam is not automatically enabled for them. You must manually enable MiTeam from the MiCollab Client tab of the User and Services application.

30.32.1 Importing User Data from MiVoice Business Platforms

If you are installing a new MiCollab system into an existing site consisting of one or more MiVoice Business platforms, you can use the MiCollab Client Integration wizard to update the MiCollab database with the user and phone data from the MiVoice Business.

Note:
After you run the wizard and synchronize the data, your MiCollab system will be running in MiCollab Client Integrated mode.

Note:
The MiCollab Client Integration Wizard is not supported for MiVoice Office 250 or Axxess platforms.

The following procedure updates the MiCollab database with the user and phone data from the existing MiVoice Business.

1. In the MiCollab server manager, click **MiCollab Client Server**, click **Enterprise** and configure an Enterprise with the following information:

   - Enterprise ID
   - Description
   - Enterprise Domain
   - Default Account Settings
2. Leave the rest of the fields at the default settings.

3. Click PBX Node and add the site MiVoice Business s. At the minimum, enter the following:

   - **Description**: MiVoice Business System Name
   - **IP Address/hostname**: MiVoice Business IP Address
   - **Registration Code**: Registration code that is programmed on the MiVoice Business
   - **Username**: MiVoice Business administrator username
   - **Password**: MiVoice Business administrator password

4. Run the MiCollab Client Integration Wizard:

   - In the Server Manager menu, under **Configuration**, click **MiCollab Client Wizard**.
   - Follow the instructions provided in the wizard.
   - Ensure that you perform a MiCollab Client **PBX Sync**.

The wizard updates the Network Element page with the MiCollab Client PBX Nodes (MiVoice Business) and populates the USP directory with the user and phone data from the MiVoice Business PBX nodes.

30.32.2 Resolving MiCollab Client PBX Sync Errors

The following table contains common MiCollab Client PBX synchronization errors and the corrective actions:

Error	Details	Corrective Action
AuthData Sign failed	MiCollab Client Service security certificate is invalid.	Upgrade MiVoice Business and the MiCollab Client Service to compatible versions.
Authenticate request failed	Verify that the MiCollab Client Service is compatible with MiVoice Business.	
Authentication error		
Soap client context setup error	Internal MiCollab Client Service error.	Restart the MiCollab Client Service .
Soap login failed	Node IP address, Username, or Password is incorrect.	In the MiCollab Client Service PBX Node tab, ensure the IP address, Username, and Password match those on the PBX Node (MiVoice Business) platform. Then sync again.
Soap login rejected		
Invalid number of fields. NTuples failed	MiVoice Business and the MiCollab Client Service versions are incompatible.	Upgrade MiVoice Business and the MiCollab Client Service to compatible versions.
Search first failed with invalid number of fields	Verify that the MiCollab Client Service is compatible with MiVoice Business .	
Search next failed with invalid number of fields	MiVoice Business became non-operational during sync.	Retry sync after 5 minutes.
Search NextTuples failed		
Search NTuples failed		
Server returned Error. NextNTuples failed		
Server returned Error. NTuples failed		

Error	Details	Corrective Action
Server returned failure	View the EPM logs to determine e rror code.	Corrective action based on the error code.
Version request failed	The MiCollab Client Service is not compatible with MiVoice Business version.	Upgrade MiVoice Business and the MiCollab Client Service to compatib le versions.
Version fetch failed		
DSM internal error	MiCollab Client Service internal er ror.	Capture the MiCollab Client Service dsm.log and contact support.
# instances: Subscriber creation fai led: There are currently no licenses for the feature <FEATURE NAME> in the <ENTERPRISE NAME>	You don't have enough feature li censes on the MAS system to supp ort the number of users that are bei ng imported from the MiVoice Bus iness s. The # of instances indicate s the number of required feature lic enses.	Obtain the required licenses and run the wizard: 1. Obtain the required number of MiCollab Client deskphone and softphone licenses from the AMC for MiVB or for other PBXs from SLS License Server as applicable. 2. Apply the licenses to the users through the MiCollab Client Service **Accounts** tab. 3. Run the wizard again. OR Run the wizard and apply licenses later: 1. In server manager, click **MiCollab Client Server**. 2. Click **Configure MiCollab Client Server**. 3. Click the **Synchronization** tab. 4. Set the feature profile to "Default Feature Profile". All users will be imported with all features disabled (no licenses applied). 5. Retry the wizard. 6. After you have run the wizard successfully, assign the deskphones and softphones through the USP application. 7. Assign MiCollab Client features to each user through the MiCollab Client Service Accounts tab.

30.33 Configure MiCollab Settings

This form allows you to perform the following:

- Change the strength of the MiCollab login password for the MiCollab End User portal
- Configure a Service Information (Welcome) E-mail that informs users of their MiCollab account information
- Collect application and server logs in a file
- Enable MiCollab Client Deployment for External Hot Desk Users and set the default deployment profile
- Add new users to MiCollab when created or updated in MiVoice Business and enable Reach Through feature
- Enable CloudLink chat integration with MiCollab.

30.33.1 Change Password Strength

By default, password strength is set to **Strong**. To set password strength:

1. Under **Configuration**, click **MiCollab Settings**.
2. Click **Password Strength** tab.
3. Select the desired strength:

   Weak passwords must

   - be from 6 to 20 characters in length (alphabet, numeric, or a combination of both)
   - not contain your old password or your Login ID
   - not be the same as recently used 1 password.

   Medium passwords must:

   - be from 7 to 20 characters in length (alphabet, numeric, or a combination of both)
   - not be too simple (cannot contain a word from a dictionary or be too repetitive)
   - not contain your old password or your Login ID
   - not be the same as recently used 3 passwords.

   Strong passwords must:

   - be from 8 to 20 characters in length
   - not be too simple (cannot contain a word from a dictionary or be too repetitive)
   - contain at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character (for example #)
   - not contain your old password or your Login ID
   - not be the same as recently used 5 passwords.

Note:
For Teleworker enabled user, you must set a strong password.

4. Click **Save**.

Conditions and Limitations

- If the administrator resets the password from the Server Manager, the password that is reset is stored in the passwords history.

  The end-user can now reset their password to **(N-1)** password onwards.

  where **N** is the password strength; N=1 for Weak password, N=3 for Medium password, and N=5 for Strong password.

- If you change the Password Strength rules, the new rules will take into effect only if the end-user changes the password to a new one as per the policy.

  For example, if the password strength for an user is changed from **Strong** to **Weak**, the user will still not be able to reset the password to recently used five passwords. The **Weak** policy is effective only if the user changes the password to a new one.

30.33.2 Configure Service Information E-mail

You can configure MiCollab to automatically send Service Information e-mails to your system users. This e-mail feature provides users with communication settings information, such as:

- Login ID
- Password
- Passcode
- Phone Type and Number

The system sends an e-mail, whenever you

- select a user in the Users and Services Directory page and click the **Send Service Info E-mail** button
- create a new user (either from MiCollab USP or from the directory server if MiCollab IDS is enabled)
- create an MiCollab Audio, Web and Video Conferencing user, or
- reset a user's password or passcode.

If you select a user in the Users and Services Directory page and click the **Send Service Info E-mail** button, the system sends a user a Service Information E-mail that contains all of the user's service information.

If you create a new user, the system automatically sends an e-mail to the user that contains the user's login ID, password, and a link to the MiCollab Web Client .

If you reset a user's password in the Users and Services application, the system sends the user an e-mail that contains only the new password.

You can send the e-mail with a default or custom greeting message. With the exception of the custom greeting, the information can be sent in two languages.

Conditions

- The Service Information e-mail feature is enabled by default.
- The Service Information e-mail is sent to the user's primary e-mail address that is entered in the User tab of Users and Services application.
- MiCollab sends a Service Information e-mail whenever any of the following methods are used to create a new user or reset a user's password:
  - Users and Services Add, Edit, or Quick Add User
  - Mitel Integrated Configuration Wizard
  - Users and Services Bulk Import
- The password is only included in the e-mail during the initial creation of a user or whenever the administrator resets the user’s password.
- If you create a user without an e-mail address, the system does not send a Service Information e-mail.
- If you disable the Service Information e-mail feature, all Service Information e-mails sent prior to the disabling of this feature are still delivered to the users.
- If you modify a user's password, a Service Information e-mail is sent with the new password. Note that an e-mail is not sent if a user modifies his or her own password.
- If you select a user in the USP directory and click the **Send Service Info E-mail** button, an e-mail is sent regardless of whether or not services are assigned to the user, providing the user is assigned an E-mail address.
- If you click the **Send Service Info E-mail** button in the USP directory page, all service information for the user is provided in a single e-mail. If you want the MiCollab Speech Auto Attendant Pilot/Access number numbers to be listed in the Service Information e-mail, you must enter these numbers in the Network Elements tab of the Users and Services application. The system takes the pilot/access numbers that you enter in the Network Elements tab and lists them in e-mail for the end users. If you do not enter the numbers in the Network Element tab, they will not be included in the e-mail.
- If MiCollab services are added to users who were originally created in a MiVoice Business system administration tool, a Service Information e-mail is not sent automatically, even if an e-mail address is provided for the user.

Configure Service Information E-mails

1. Configure the MiCollab server e-mail settings.
2. Under **Configuration**, click **MiCollab Settings**.
3. Click the **Welcome E-mail** tab.
4. Ensure that the **Send Welcome E-mail** option is **Enabled**.
5. By default, the MiCollab for Mobile deployment e-mail is sent to that application's users. Click the link if you do not want to distribute that e-mail. See *Mobile Client deployment e-mail* in **MiCollab Client Deployment** help for information about configuring the MiCollab for Mobile welcome e-mail.
6. Enter a valid e-mail address for the Sender account. This address appears in the "From:" header of the e-mail. It is recommended that you enter an e-mail address that will not be monitored (for example: do_not_reply@example.com).
7. By default, the **Append Do Not Reply Closing Message** option is set to **Enabled**. This option includes a note at the end of the Welcome e-mail that instructs users not to reply to the e-mail. If you want to receive replies from users at the Sender e-mail account, set this option to **Disabled**.

8. You can include a default greeting or a custom greeting in the Service Information e-mail:

   To use a the default greeting message, click **Default**.

   or

   To create a custom message, click **Custom** and enter a greeting message up to 2000 characters in length. Note that it is recommended that you include a link to the MiCollab Web Client at https://<host name of MiCollab server>/portal in your custom message. If the e-mail is required in multiple languages, you must enter the greeting message in each required language.

> **Note**:
> If you select the **Default** option while you have text entered in the Custom Message box, your text will be cleared.

> **Note**:
> To include a hyperlink in a custom message, you must include a space before and after the hyperlink, even if the hyperlink is on a separate line. Otherwise, the link may not function for all users.

9. Specify the service information that you want included in the e-mail by clicking the associated check boxes. If a service is checked, but the user does not have that particular service, no information for that service is included in the welcome e-mail. By default, all service information is checked.

   - The check boxes are available for MiCollab Microsoft Outlook Plugin, Legacy MiVoice for Skype for Business Plugin, MiCollab for Microsoft Client, and End User Portal Link.
   - MiCollab for PC Client download link will be included in the deployment e-mail. For MiCollab Servers that are upgraded from an older version to 8.0 or higher, the administrator must load the default deployment text or add the link **[####winpc####]** manually in the custom deployment text.
   - If you select the **Legacy MiCollab PC Client** checkbox, MiCollab Desktop Client download link will be included in welcome e-mail. By default, this checkbox will be selected in case of an upgrade or a new installation.

> **Note**:
> Select the **MiCollab Client Service** checkbox, to enable the **Legacy MiCollab PC Client** option.

10. Select up to two languages (First and Second Language). The e-mail information will be sent in both languages (sequentially in the selected order).

> **Note**:
> The system does not translate custom greeting messages.

11. Enter a valid destination e-mail address in the **Test E-mail Address** that you can access (for example your work e-mail address). To enter multiple addresses, separate each address with a semi-colon. After you click **Save**, an e-mail is automatically sent to the address or addresses that are entered in this field.
12. Click **Save**.
13. Open the e-mail account and check that the e-mail was received. Ensure that the e-mail contains the desired information.

Send Service Information

To send a Service Info E-mail that contains all of the user's service information from the Users and Services application directory:

1. Under **Applications**, click **Users and Services.**
2. Click **Users**.
3. Search for a specific user or click **Show all.**
4. Select the check boxes of the desired users.
5. Click **Send Service Info E-mail**.
6. Click **Ok**.

Disable Service Info E-mails

1. Under **Configuration**, click **MiCollab Settings.**
2. Click the **Welcome E-mail** tab**.**
3. Set **Send Welcome E-mail** option to **Disabled**.

30.33.3 Collect Logs and Diagnostic Data

This utility allows system-level logs to be collected for the server platform and then saved to another location such as your local PC. Logs can be selected for collection from specific applications.

These logs contain system data that is not available in the Logs Viewer. These logs are intended for use by Mitel Technical Support.

Note:
Although this utility is available from the MiCollab Administrator Portal, it is recommended to use the MSL Server Manager to collect logs and diagnostic data.

To collect and save log files:

1. Under **Configuration**, click **MiCollab Settings**.
2. Click the **Collect Logs** tab.
3. Select which categories you wish to log. To minimize the size of the log file, uncheck categories you do not require.
4. Click **Start**. A progress indicator appears while the logs are being collected.

Note:
The log collection process can take a few minutes. You can navigate to other screens without interrupting the process.

5. When the log collection process finishes, the indicator changes to "Complete / 100%" and the archived log file is listed on the screen. Depending on which type of web browser you are using, a copy of the file will be downloaded automatically or you will be prompted to save it.
6. You can manage the list of archived log files as follows:
   - To save a file, click **Save**, navigate to the location you wish to store the file, and then click **Save**. A tar file with the filename " sosreport-<file>-tar.bz2" is saved to the specified folder.
   - To delete a file, click **Delete**, and then click **OK**. The archived log file is deleted from the server.
7. After saving an archived log file, send it to Mitel Product Support for analysis.

Note:
- Archived log files are automatically deleted from the server after 72 hours.
- You can also manage the archived log files from the MSL shell. The files are located on the server in / var/cache/e-smith/ logcollector.

30.33.4 Set Default Deployment Profile for EHDU

This page allows you to set the default MiCollab Client Deployment profile for External Hot Desk Users. By default, the deployment profile for EHDU is set to **Do Not Deploy**.

1. Select the desired deployment profile.

2. Click **Save**.

   Any EHDU phone which is not already deployed is updated to use the selected deployment profile.
3. Deploy the Mobile Clients for EHDU.

30.33.5 CloudLink Integration

The CloudLink chat integration with MiCollab is a two-step process.

1. In the first step, a connection is established between CloudLink and MiCollab and MiCollab users are activated on the CloudLink platform.
2. In the second step the CloudLink chat is activated for the MiCollab users.

Note:
CloudLink chat is disabled for users using the Basic MiCollab UCC bundle.

Important:
If CloudLink integration is deactivated, MS Teams integration will also be disabled. Within the MiCollab Client Service, all users assigned to the "Default MS Teams User Profile" will be reassigned to the "Default User Profile." Additionally, for users assigned to custom profiles with Status/Presence integration enabled, their MS Teams statuses will transition to Non-MS Teams statuses, and Status/Presence integration will be disabled across all custom user profiles. Refer to the MS Teams Configuration Settings in the MiCollab Client Administrator Console for more details.

Enable CloudLink Integration

Prerequisite: As a MiCollab administrator, you can enable CloudLink Chat on MiCollab if you have the credentials for your administrator account on CloudLink. If you do not have the credentials, contact the Mitel channel partner. Also, ensure that the MiCollab server is in Integrated Mode.

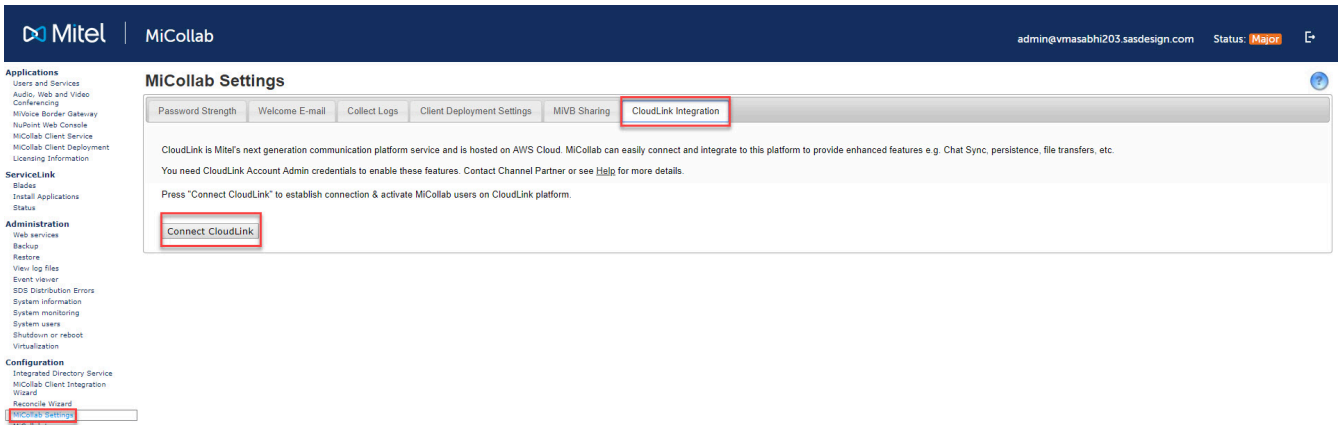
1. In the MiCollab Administrator portal, under **Configuration** click **MiCollab Settings.**

   On the right pane, the MiCollab Settings page opens.
2. In the **CloudLink Integration** tab, click the **Connect CloudLink** button.

   A confirmation message appears that you are being redirected to the Mitel Authentication Portal for authentication.

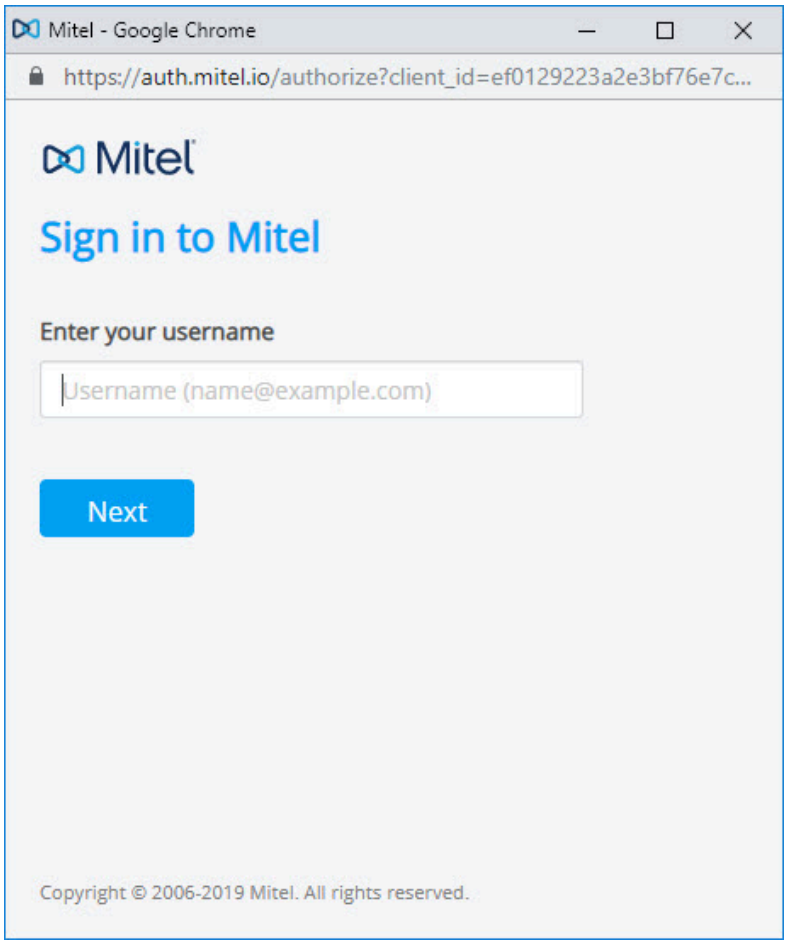
Note:
Ensure that the web browser pop-up blocker is disabled. This is mentioned in the confirmation message which redirects to the Auth Portal.

Note:
If the Mitel Auth portal opens in an IE browser, the user should enable the **Protected Mode** (navigate to **Internet options>Security>Protected Mode**), otherwise the browser stops working after the credentials are entered and does not proceed with the authorization



3. Click **OK** to proceed.

4. In the **Mitel Authorization Portal,** enter your CloudLink account admin username (as given in the welcome E-mail that you received during CloudLink account creation) and then click **Next**.



5. Enter the CloudLink account admin password and click **Next**.

   The authentication process begins.

   When the authentication is completed successfully, as indicated in the authentication status, MiCollab automatically starts the process of activating all the MiCollab users on CloudLink.

Note:
If the authentication fails for reasons such as – auth portal pop-up time-out, token generation failed in the background, admin closed portal pop-up during the process, or no response from portal due to network issues, the error status notifies authentication has failed. If this happens, repeat the steps of this procedure from Step 2.

6. When the authentication is completed, MiCollab automatically starts the process of activating all MiCollab users on CloudLink.

   The MiCollab admin can monitor the progress on the number of failed and successful users activated from the **CloudLink Activation Summary.**

> **Note**:
> Users, who are on two different peered servers, having the same e-mail address, will be treated as a single user on CloudLink.

> **Note**:
> After the integration is complete, the users who are on MiCollab Server but not on DeployU are not automatically synced (**Deployment Profile** status **Un-Deployed**). Import the users into DeployU by performing a manual import function (**MiCollab Client Deployment** > **Import Users**) or deploy the users manually from **MiCollab Server Manager** > **Applications** > **Users and Services**.

Failed User Report

If the activation process fails, the MiCollab administrator can view a list of users for whom it failed and the reasons for the failure by downloading the **Failed User Report**, from the CloudLink User Activation Summary. After reviewing the report, the admin can apply below steps for resolving the errors.

For CloudLink chat, at network firewall level, certain firewall related exception must be considered. For Network Configuration prerequisites, refer to these sections in the *CloudLink Gateway User Guide*:

- Configuration Prerequisites
- Network View
- Accounts Console
- CloudLink Chat Integration
- CloudLink Platform IP Address Ranges

These network connections as defined in the referenced sections should be reachable from the following:

- MiCollab Server
- Admin PC used to access the MiCollab Server for enabling CloudLink integration, which are used for opening the MiCollab Administrator Portal
- End-user PCs and mobile devices where the MiCollab end-user client is running

For successful CloudLink chat integration with MiCollab, it is essential to configure the network firewall and proxy settings correctly. In addition to the previously mentioned, refer to the AWS General Reference

documentation that provides information on obtaining the AWS IP address ranges, which might be required for the firewall configuration.

Proxy Exception List

If your organization uses a web proxy, you may need to add the CloudLink server address to your proxy exceptions list. Refer to the *CloudLink Solution Guide* for more information on proxy exception list.

Enable and disable CloudLink Chat

Once user activation is done, proceed to the next step and click on the **Enable CloudLink Chat** button to start CloudLink Chat for the activated MiCollab users.

Enabling CloudLink chat automatically disables MiCollab chat. All existing MiCollab chats will be archived and will be available to users as read-only.

CloudLink chat is not supported for failed users (failed due to reasons stated above), users with legacy clients or users running earlier version of Next Gen Clients (Releases earlier to 9.0).

Note:

At a time, either MiCollab chat or CloudLink chat will be enabled. Chat between peer servers will not work if CloudLink chat is not enabled on all servers or if the servers are not using the same CloudLink account.

The **Disable CloudLink Chat** option disables CloudLink chat for MiCollab users. Disabling CloudLink chat for MiCollab users automatically enables MiCollab chat back for the users.

Note:

It is recommended that the operations of enabling or disabling CloudLink chat be done during off hours because the process might impact the server performance.

Deactivate CloudLink Integration

The **Disconnect CloudLink** option terminates the connection between the CloudLink platform and MiCollab and disables the CloudLink features for all MiCollab users. To re-connect to CloudLink Platform, you must enable CloudLink integration from the MiCollab Administrator portal. See, Procedure: To enable CloudLink Integration.

MiCollab administrator can reconnect to CloudLink chat as long as the CloudLink account created for CloudLink chat integration with MiCollab is not deleted by the CloudLink administrator from the Mitel Administration.

Note:
When the CloudLink is disconnected, the account details, user detail, and chat history remain preserved in the CloudLink. The CloudLink administrator can delete the user information (deletion of user will also delete their chats) from CloudLink through the **Mitel Administration**.

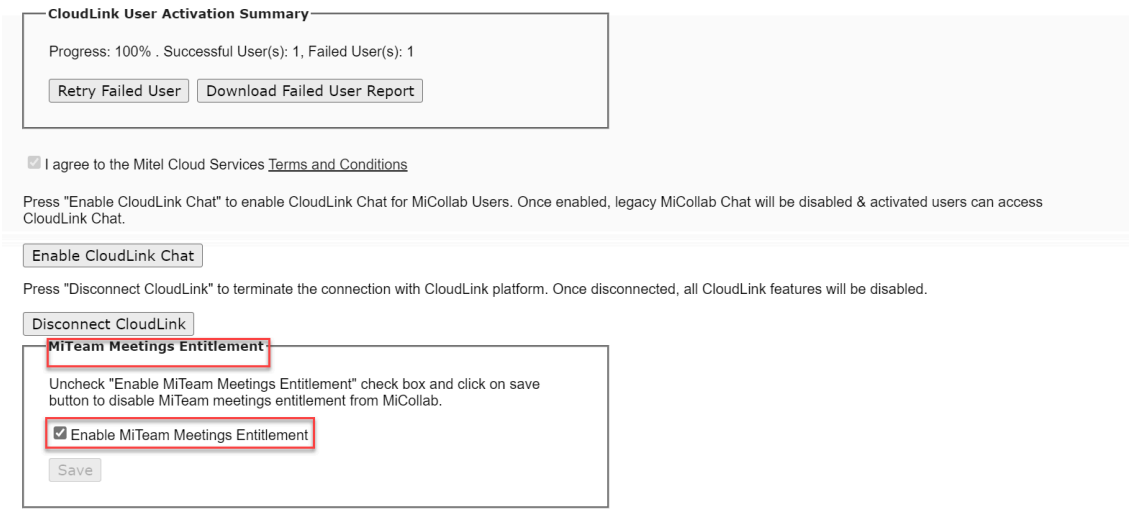
Note:
To deactivate or delete the CloudLink account information, Mitel partners need to be contacted. Account deletion will delete all the users' information (including their chats) from the CloudLink account.

Note:
If the users and their account information are retained in CloudLink, the users chat history is preserved securely in the CloudLink. To retrieve the chat history of one or more users, the partner or the administrator can make a legal request to Mitel in compliance with GDPR or local laws.

MiTeam Meetings Entitlement

Checking the **Enable MiTeam Meetings Entitlement** check-box provides the MiTeam Meetings permission from MiCollab, which means the end-users can use the Meetings feature from the MiCollab client. Once this check-box is enabled, the MiTeam Meetings check-boxes appear under the **Users and Services > User Templates** and **Users** tab.

Note:
CloudLink Integration should be enabled for the MiTeam Meetings Entitlement setting to be visible.



Re-establish CloudLink Connection

The CloudLink connection tokens are preserved securely in the MiCollab. In error conditions or when the connection tokens are lost, the following warning message is displayed.



To re-establish the connection, the account administrator must login again using CloudLink administrative account credentials.

Troubleshooting

Scenario	Resolution
When two accounts (for example, personal and IP console) have the same email ids, the users using the IP console would see the chat conversation of the user and vice versa	Use a separate email id for two different accounts which is not used by any other user in the setup. Accounts with the same email id would be treated as a single chat account.

Scenario	Resolution
Multiple user accounts with same primary email id When two user accounts (for example, MiTeam guest user and MiCollab user) have the same primary email id, the second user will be created without a primary email. This impacts all the features (such as, CloudLink Chat, MiTeam, and so on) which depend on primary email and will not work for the user. For example, If a MiTeam guest user exists on MiCollab Client server with primary email (for example, john@xyz.com), then you create a MiCollab user on MiCollab Server with the same primary email. This will create a user on MiCollab Client server but without a primary email for the user. This happens because the same primary email is being used for another account (MiTeam guest user account).	1. Delete the MiTeam guest user account from **Applications** > **MiCollab Client Service** > **Configure MiCollab Client Service** > **Account** tab. 2. Delete and recreate the user on MiCollab from **Applications** > **Users and Services** tab.

The below section addresses the errors in the failed user report (csv import) and possible corrective action. For any other issues, please contact the Mitel Support with issues and log details.

Failure reason/ Error in CSV Report	Possible correction step to admin
UCA Error - 412,Server not in integrated mode	The MiCollab server is not in an integrated mode. Change the server to Integrated and retry the process.
UCA Error - 400,Validation Error: User info must not be empty	Check the user information in MiCollab Client Service. User information must not be null or blank.
UCA Error - 400,Validation Error: Cloud Link GUID missing	Check the user information in MiCollab Client Service. Try to delete and recreate the user.
UCA Error - 400,Validation Error: Primary Email missing	Check the user's primary email information in MiCollab Client Service. User’s email id should not be null, and it should be a valid id.

Failure reason/ Error in CSV Report	Possible correction step to admin
UCA Error - 500,No user found with email: <email_id>	Check the user's existence with the available email addresses in MiCollab Client Service.
UCA Error - 500,Multiple users found with email: <email_id>	Check the number of users associated with that particular email address in MiCollab Client Service. Only one user should be associated with one email address.
UCA Error - 500,<THIS STRING WILL VARY BASED ON THE EXCEPTION SCENARIO>	Unexpected error occurred at MiCollab Client Service. Try restarting the UCA services and retry the process.
SAS Error – User's Email/UC service not available	Edit the user from USP and add/update the email address of the user if it is not pre-existing.
	Edit the user from USP and provide the login id to enable the user for UCA service.
CloudLink Error - 500,Email address is invalid	Check and update the correct email id of the user from the USP page. Once the correct email id is provided, the MiCollab server will auto-trigger the user activation in CloudLink.
CloudLink Error - 400, Missing Unique Identifier	Click the **Retry Failed User** button available under **MiCollab Setting** > **CloudLink Integration**
CloudLink Error - 500,Internal server error	Click the **Retry Failed User** button available under **MiCollab Setting** > **CloudLink Integration**. If the issue still persists, check the public internet connectivity from MiCollab server.
CloudLink Error - 401,Unauthorized	Click the **Retry Failed User** button available under **MiCollab Setting > CloudLink Integration.**
CloudLink Error - 404,Account Not Found	Click the **Retry Failed User** button available under **MiCollab Setting > CloudLink Integration**. Check the accounts existence on Mitel Administration.

Failure reason/ Error in CSV Report	Possible correction step to admin
CloudLink Error - 409,User Already Exists	Check whether the user exist in Mitel Administration.

30.34 Configure MiCollab Language

This page allows you to configure the following settings:

- **System Language**: Select the language of the Telephone User Interfaces (TUIs) for the MiCollab application end-users. End-users can also set their own prompt language on the Settings page of their MiCollab End User Portal. After the initial installation of a new system, the System Language defaults to US English.
- **NuPoint UM Prompt Languages**: Select the other languages for the NuPoint UM prompts. When users call into the NuPoint UM system through the Message Center auto attendant or Receptionist application, they are asked to select the language of the NuPoint UM prompts for the duration of their call. Users can select either the primary prompt language or one of the other languages. The primary (first) language is determined by the System Language setting above; the other languages are determined by the settings in these fields. For example, the primary system language could be English (United Kingdom); the second language; French (Canada), the third language Swedish (Sweden), and so on.

  You must record your corporate "Welcome" greeting in all the selected languages for incoming calls to the NuPoint UM system. When an external caller connects with the voice mail hunt group pilot number, the system plays your bilingual or multi-lingual corporate greeting and then prompts the caller to select the desired language. For example:

  System "Welcome" Greeting:"Welcome to Mitel Networks, Bienvenue à Mitel Networks".

  System Prompt: "For Service in English press 1; Pour le service en français, appuyez sur 2”.

  Users should also record their mailbox greetings in the required languages. When a caller reaches a user's mailbox, the system plays the mailbox greeting. For example:“You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message”.
- **Use NuPoint UM Mnemonic English Prompt**: When the System Language or Secondary NuPoint UM Prompt Language is set to English (United States), check this box if you want the NuPoint UM voice mail system to use English mnemonic prompts. By default, the system uses English numeric prompts.

Change System Language

To change the system language:

1. Under **Configuration**, click **MiCollab Language**.
2. Select the desired language from the **System Language** drop-down box.

3. If you set the system to use "English (United States)", you can choose to use numeric (default) or mnemonic prompts for NuPoint UM voice mail:

   - Check the **Use NuPoint Mnemonic English Prompt** box if you want the voice mail system to prompt users to enter letters to select actions. For example, "Press P to play";
   - Clear the box if you want the voice mail system to prompt users to enter numbers to select actions. For example "Press 7 to play".

> **Note**:
> The **Use NuPoint Mnemonic English Prompt** box is only presented if the NuPoint UM application is installed.

4. Click **Save**.

The following conditions apply to the System Language:

- The Line Group language setting and LCOS language setting use the MiCollab system default language. In the interface, the Line Group language setting is set to "undefined" and the LCOS language setting is set to "default". If you set the system language in the Line Group, it overrides the MiCollab system language setting and the MiCollab secondary NuPoint UM prompt language setting. Note that the LCOS language overrides the Line Group language and the MiCollab System language.
- The language of the Call Director application is not controlled by the system language setting.
- MiVoice Business phone displays are not controlled by the system language setting.
- For MiCollab Audio, Web and Video Conferencing , the Telephone User Interface language (TUI) is set on a system-wide basis for all users (that is, each user cannot set his or her own TUI language for MiCollab Audio, Web and Video Conferencing).
- The MiCollab End User Portal login page is displayed to the user in the language of the user's browser. If the browser language is not supported, the login page is displayed in the system language.
- The prompt language for call flows in Call Director default to the MiCollab language setting. However, users can set the prompt language for a call flow independently of the MiCollab language setting through the **Action** menu in the Call Director application.
- The System Language setting does not control the language used by the MiCollab End User Portal or Speech Auto Attendant application. The MiCollab Speech Auto Attendant only supports two languages: UK English and NA English. To change the Speech Auto Attendant language:

  1. Under **Applications**, click **NuPoint Web Console**.
  2. Under **Auto Attendant**, click **Misc. Parameters**.
  3. Select the desired **Primary Language**, and then click **Save**.
  4. Under **Auto Attendant**, click **Data Source**.
  5. Click **Force Update**.
- The **Use NuPoint Mnemonic English Prompt** box is displayed only when either System Language or Secondary NuPoint UM Prompt Language is set to English (United States).
- MiCollab Client supports additional languages that are not supported by MiCollab. However, MiCollab Client users can use these additional languages when MiCollab Client is deployed as an application on MiCollab , even though these languages are not supported by MiCollab .

Configure NuPoint UM Prompt Language

To configure a prompt language for the NuPoint UM system:

1. Ensure NuPoint UM FCOS feature bit 51 "Do Not Switch Languages for Outside Caller" is assigned to the users' voice mailboxes.
2. Under **Configuration**, click **Application Suite Language**.
3. Select the desired languages from the **NuPoint Prompt Language** drop-down box.
4. Record a bilingual or multilingual corporate greeting for the NuPoint UM system hunt group pilot number though the NuPoint UM administrator mailbox. Record the greeting in the "System Language" followed by the same greeting in the other selected languages; for example: “Welcome to Mitel Networks, Bienvenue à Mitel Networks; Bienvenido a Mitel Networks; Willkommen bei Mitel Networks”
5. Call into the NuPoint UM system hunt group pilot number and ensure that the prompts are played correctly.
6. Instruct mailbox users to record bilingual (or multilingual) greetings for their mailboxes as required. Again, users should record their mailbox greetings in the "System Language" followed by the same greeting in the other languages; for example: “You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message; Usted ha llegado al buzón de voz de Jean Julian , por favor deje un mensaje; Sie sind auf der Sprachmailbox von Jean Julian erreichen, hinterlassen Sie bitte eine Nachricht”.

The following conditions apply to the other NuPoint UM prompt languages:

- NuPoint UM FCOS feature bit 51 "Do Not Switch Languages for Outside Caller" must be assigned to the users' voice mailboxes.
- The NuPoint UM Line Group language setting and LCOS language setting use the MiCollab system default language. In the interface, the Line Group language setting is set to "undefined" and the LCOS language setting is set to "default". If you set the system language in the Line Group, it will override MiCollab system language setting and the MiCollab NuPoint UM prompt language.
- The "NuPoint Prompt Language" field is only displayed if NuPoint UM is installed.
- This prompt language feature does not apply to Speech Auto Attendant (SAA).

- Callers select the desired language for NuPoint prompts at the system-level only, not at the mailbox level.
- The system plays the languages in the order of the language choices. For example, if you selected the English as the "System Language" and then French, the system generated prompt plays: *"For service in English, press 1; Pour le service en français, appuyez sur 2."*
- This feature applies to calls to the NuPoint UM voice mail hunt group pilot number. The caller only selects the prompt language once, before the first system prompt is played.
- Mailbox owners are not prompted to select a prompt language when they log into their mailboxes.
- In MiCollab , the language selection prompts are system generated. MiCollab does not provide you with the ability to record and import a custom language selection prompt.
- An "SAA Warning" is displayed in the server manager interface if the "System Language" or one of the other language selections is not English.

30.35 Vidyo Tenant Credentials

Use this page to enter the parameters required to establish a connection between MiCollab and the Vidyo Portal:

1. Complete the following pre-requisites. Refer to the *Vidyo Product Documentation* and the *MiCollab Vidyo Quick Reference Administrator Guide* for instructions:

   - Deploy and license the Vidyo Portal. Licensing is not controlled from the Mitel Application Management Center (AMC). You must install the Vidyo licenses on the Vidyo system.
   - Assign the Vidyo Portal with a Fully Qualified Domain Name (FQDN) that is resolvable within the network.
   - Create a Vidyo administrator account.
   - Configure **Authentication Type** and **Authentication using Web Service** settings in Vidyo administration. Refer to the *MiCollab Vidyo Quick Reference Administrator Guide.*
2. Enter the Tenant Name and Tenant URL.
3. Enter the Tenant Dialing Prefix. The tenant dialing prefix must match the prefix that is programmed on the Vidyo Portal.
4. Enter an administrator username and password.
5. Confirm the password.
6. Click **Save**. After you enable the Vidyo settings, the UCC Premium User template is updated with Vidyo services settings.
7. Add Vidyo services to UCC Premium users.

Vidyo Field Descriptions

Field	Description	Values
Tenant Identification		
Tenant Name	Enter a name for the Vidyo Tenant.	Maximum of 32 alphanumeric characters.
Tenant URL	Enter the URL to the Vidyo Portal. For security, it is recommended that you use an HTTPS URL.	Maximum of 64 alphanumeric characters. The entry in this field must conform to URL format (for example: https://hostname.com)

Field	Description	Values
Tenant Dial Prefix	Enter the Vidyo tenant dialing prefix. The Vidyo Gateway uses the tenant dialing prefix to route external audio participants to the Vidyo meeting room. **Note**: You can only change this field if there are no MiCollab users configured with the Vidyo service. **Note**: You can only connect one MiCollab to one Vidyo tenant. Multiple tenants are not supported. The tenant dialing prefix that you enter into this field must match the prefix that is programmed on the Vidyo Portal. If the prefixes do not match, you will receive an error when you attempt to enable Vidyo service for MiCollab users. The error message states that the extension does not start with the Tenant prefix.	Maximum of five digits.
Administrator Credentials		
Username	Enter the username of the Vidyo Portal administrator account.	Maximum of 32 alphanumeric characters.
Password	Enter the password for the Vidyo Portal administrator account.	
Confirm Password	Confirm the password entered above.	

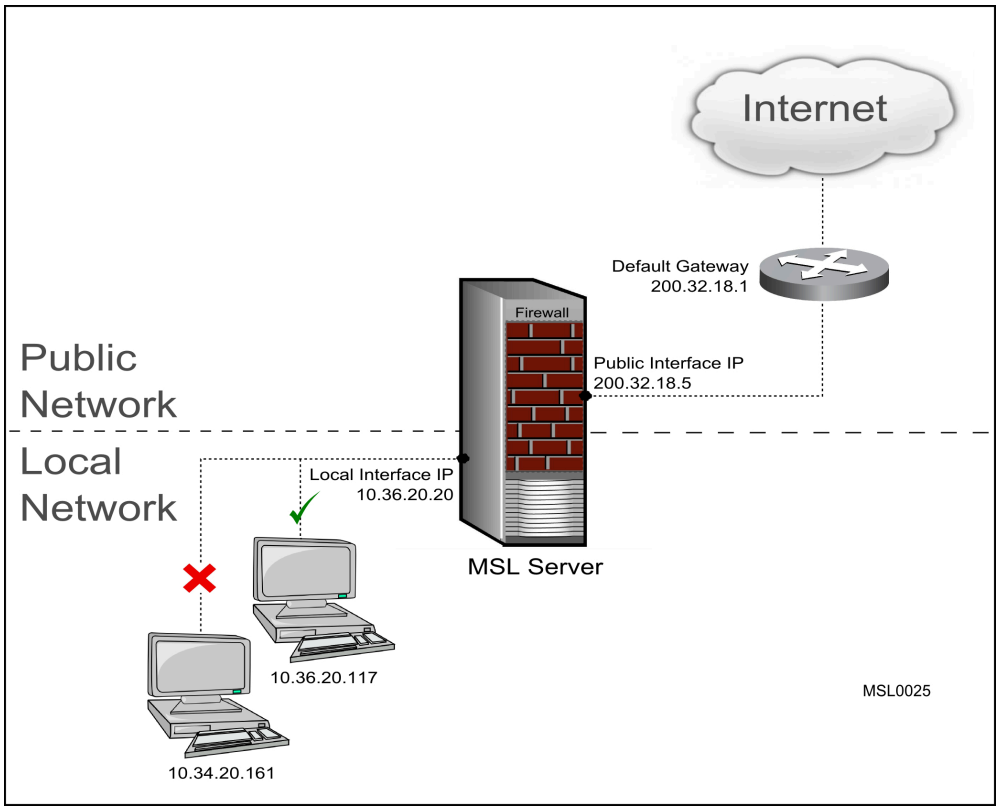
30.36 Configure Networks

Grant Access Privileges to Trusted Local Networks

By default, several MSL services, including server manager access, SSH and system monitoring, are accessible only from computers that are located on the same network where the MSL server is installed. If you need to manage the server from a different subnet on the LAN, then you must configure the other subnet as a "Trusted Network." This configuration opens the firewall and allows access to the services on the MSL server.

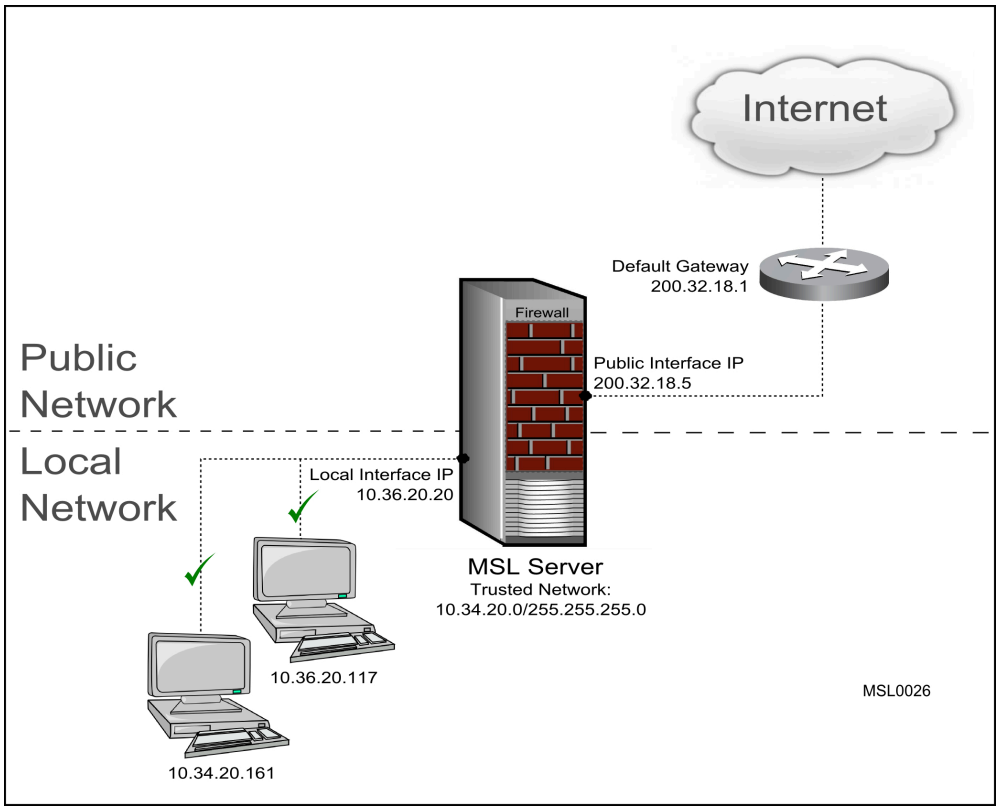
Example of Default Routing Configuration

In the example illustrated below, the LAN interface of the MSL server has an IP address of 10.36.20.20. Accordingly, the server will accept traffic *only* from the 10.36.20.x network while blocking traffic from all other subnets on the LAN.



Example of Trusted Network Configuration

In the example illustrated below, the MSL server has been configured an IP address of 10.36.20.20 on its LAN interface and with a "trusted network" of 10.34.20.0/255.255.255.0. Accordingly, the server will accept traffic from both the 10.36.20.x and 1034.20.x subnets.



Note:

- If only one network is being serviced by the server, you do not need to add any information here.
- Adding a "trusted network" automatically opens the firewall:
  - allows access to the HTTP services on the MSL server
  - allows access to all MiVoice Business network services
- If your server has an IPv6 address configured on its LAN interface, then you can extend privileges to IPv6 networks as well as IPv4 networks. (IPv6 is not supported by MiVoice Business)
- Use the **Secure Shells Settings** topic in **MSL Server Manager** document to control access to HTTP and SSH services to specified networks..
- If you only need to enable traffic to/from remote (or "untrusted") servers but not want them to access MSL services, simply add a network route.
- Depending on the architecture of your network infrastructure, the instructions for configuring the clients on an additional network may be different than the following instructions. For more information about adding networks, contact your authorized Mitel Reseller.

To extend privileges to one or more additional networks:

1. Under **Configuration**, click **Networks**.

2. Click **Add a new trusted network**.
3. In the **Network Address** field, enter the IPv4 or IPv6 address of the network to designate as “local”.
4. In the **Subnet mask or network prefix length** field, enter the dot-decimal subnet mask or CIDR network prefix to apply to the Network Address. If this field is blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks.

Note:
If you are using the Mitel Performance Analytics (MPA) application for analyzing the MiVoice Business system, then:

- Refer the **Secure Shells Settings** topic in **MSL Server Manager** document to enable Secure Shells for trusted and remote management networks.
- Add trusted network for the MPA with **Network** as the IP address of MPA and **Subnet mask or network prefix length** as 255.255.255.255.

5. In the **Router** field, enter the IP address of the router you will use to access the newly-added network.
6. Click **Add**.

Add Network Routes

Use this procedure to add new routes to the MSL server's routing table. This configuration opens the firewall and enables traffic to flow to/from remote servers but does *not* grant access to the MSL services (as would adding a trusted network).

Note:

- The additional network routes are firewalled.
- Adding additional network routes is an advanced option and should only be used if you have a thorough understanding of both routing and your network topology.

To add additional network routes:

1. Under **Configuration**, click **Networks**.
2. Click **Add a new network route**.
3. In the **Network Address** field, enter the IPv4 or IPv6 address of the network route.
4. In the **Subnet mask or network prefix length** field, enter the subnet mask or CIDR prefix to apply to the Network Address. If this field is left blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks.

5. In the **Router** field, enter the IP address of the router you will use to access the newly-added network.
6. Click **Add**.

30.37 Configure E-mail

This page allows you to configure the server e-mail settings.

1. Under **Configuration**, click **E-mail Settings**.
2. Click the **Change** button beside the setting you want to change.
3. Configure the settings as required and then click **Save**:

Setting	Description
Server to use for outbound SMTP	The server can deliver outgoing messages via a corporate or Internet service provider's SMTP server, or can deliver messages directly to their destination (by looking up mail exchanger records in DNS). If using a specific SMTP server, specify its hostname or IP address. Otherwise leave this field blank.
Destination port for outbound SMTP	If you have specified a server to use for outbound SMTP, select the destination port for outbound SMTP messaging: • **Port 25** (use cleartext; default) • **Port 465** (SSL encryption) • **Port 587** (TLS encryption)
Mail Server User ID	If you are using secure SMTP (port 465 or 587), enter the user ID required by the SMTP server. This ID must be configured and licensed in the SMTP server.
Mail Server Password	If you are using secure SMTP (port 465 or 587), enter the password required by the SMTP server. This password must be configured in the SMTP server.

Setting	Description
SMTP e-mail injection restrictions	Controls which networks will be allowed to send mail through this server via SMTP. Choose from one of the following three settings: • **Localhost only** – accept e-mail only from applications installed on the server (default setting). • **Accept only from trusted networks** – accept e-mail from trusted local networks that are directly connected to the LAN. (These networks are on the same subnet as the server's private interface.) • **Accept from anywhere** - accept all e-mail
Forwarding address for administrative e-mail	By default, e-mail to the administrator is sent to the user " admin" at the domain name configured on the server. You can override the default by entering an e-mail address in this field. **Note**: RAID array event notifications are sent to this e-mail address. We recommend that you configure a valid address here.
E-mail sent for events:	Check the system events for which you want to receive e-mail notifications. The e-mails are sent to the " admin" mailbox. To turn off e-mail notifications clear all the event boxes.

30.38 Configure DHCP Server

Use the Dynamic Host Configuration Protocol (DHCP) panel to configure and manage the behavior of the internal DHCP server.

Note:
Do not enable the internal DHCP server if another DHCP server exists on the network.

To enable DHCP:

1. On the **DHCP Service** tab, click **Edit**.
2. Click **Enable DHCP Service** to enable the internal DHCP server.
3. Click **Allow BootP** to allow network clients to obtain IP addresses using the Bootstrap Protocol.

DHCP Configuration

To add a subnet:

1. On the **Subnets** tab, click **Add subnet.**
2. In the **Name** field, enter the name to apply to this subnet.
3. In the **Subnet IP address**, enter the IP address of the subnet to add.
4. In the **Subnet Mask** field, enter the mask to apply to this IP address.
5. (Optional) In the **Router** field, enter the IP address of the router used to access the subnet.
6. Click **Save**.

To remove a subnet:

1. On the **Subnets** tab, click the Remove link associated with the subnet you want to remove.
2. Click **Save**.

To add a subnet range:

If you have enabled DHCP and added a subnet, you must provide a subnet range.

1. On the **Subnets** tab, click **Add range**.
2. In the **Range start** field, enter the IP address at which to start the range of IP addresses available for assignment.
3. In the **Range end** field, enter the IP address at which to end the range.
4. In the **Lease time** field, enter the number of seconds to hold DHCP leases or accept the default setting.
5. Click **Save**.

To add a Static Host:

1. On the **Static Hosts** tab, click **Add Host**.
2. In the **Hostname** field, enter a name for the static host.
3. In the **Host IP** field, enter the static IP address of the host.
4. In the **MAC address** field, enter the MAC address of the host.
5. In the **Client ID (type, value)** field, select a type and enter a corresponding value.

6. Click **Save**.

To add DHCP options:

1. In the **Scope** field, select the scope to apply to this option. (Global, Subnet, Range, or Host)
2. Select the option type for this option (Standard, Vendor, or Site-local).
3. Do one of the following:
4. For **Standard** options, select an option number from the list.
5. For **Vendor** options, select a vendor option from the list.
6. For **Site-local** options, enter an option number between 224 and 254. Click **Next** and then enter **Name**, **Format**, and **value** for the new option.
7. Click **Save**.

To view the state of all dynamic leases:

- On the **Lease View** tab, click **Refresh** to see the most recent version of the list.

30.39 Configure Server Date and Time

You can configure the date and time:

- manually, or
- by configuring the server to obtain the date and time from a Network Time Server on the internet. A network time server communicates the time to other computers over the Internet using Network Time Protocol (NTP).

To set your date and time manually:

1. Under **Configuration**, click **Date and Time**.
2. Click **Set System Time Zone** and select your time zone from the list.
3. Enter the date and time in the fields provided.
4. Select **Enable Network Time Server** to instruct the server to periodically synchronize the system clock to a network time protocol (NTP) server. If you select this option, enter the hostname or IP address of the NTP server in the field provided.
5. Click **Save**.

To obtain the date and time from a Network Time Server:

1. Click **Enable Network Time Server**.
2. Enter the hostname or IP address of a Network Time Server.
3. Click **Save**.

Note:

For more information about using a network time server, visit http://www.ntp.org/. You can also find a list of publicly available time servers at http://www.eecis.udel.edu/~mills/ntp/servers.dita. You should always use a secondary time server (also called a stratum 2 server) to lighten the load on the primary time servers.

To verify that your network time protocol server is set up properly:

1. After you have **saved** the hostname or IP address of a new Network Time Server, click the **Query** button. Clicking the **Query** button issues the **ntpq -c peers** Linux command.



2. The command results are displayed for the NTP server (or for a list of servers if a pool is referenced by the specified hostname or IP address).

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*70.83.139.168	.PPS.	1	u	772	1024	XYYXYYYX	46.318	1.385	5.691
+142.137.247.109	129.6.15.29	2	u	45m	1024	YXXYYYXX	45.903	10.427	1.691
+192.95.20.208	18.26.4.105	2	u	547	1024	YYYYYYYY	31.142	11.086	5.981

3. After a few minutes, press **Query**again. An * appears in front of one of the NTP servers. The * indicates that the system time is being synchronized with that NTP server.

   The following table provides the meaning of the command output:

Command output	Meaning
remote	The hostnames or IP addresses of the remote NTP servers to which the system can be synchronized (based on the pool of available NTP servers). The character that precedes the hostname or IP address indicates the following:

Command output	Meaning	
	*	The system time is being synchronized with the NTP server.
	#	The host is selected for synchronization, but distance from the host to the server exceeds the maximum value.
	o	The host is selected for synchronization, and the PPS signal is in use.
	+	The host included in the final synchronization selection set.
	x	The host is the designated false ticker by the intersection algorithm.
	.	The host is selected from the end of the candidate list.
	-	A host discarded by the clustering algorithm.
	blank	Indicates a host is discarded due to high stratum and/or failed sanity checks.
refid		The current source of the synchronization for the remote host.

Command output	Meaning	
st		The stratum used by the remote host. The lower the number, the closer you are to the time source. Stratum 16 indicates that the system is not synchronized with a time server.
t		The type of clock used on the NTP server (L stands for local clock; u for an Internet clock).
when		The number of seconds since the last poll.
poll		The number of seconds between NTP transactions. When this time expires, the NTP daemon polls the remote time server. The polling results are displayed in the "reach" field.
reach		The status of the last eight NTP transactions, with each transaction represented by a colored letter. The letter "Y" in green indicates that a response was successfully received from the remote time server. The letter "X" in red indicates that a response was not received. Since this field is a circular log buffer, it is continually refreshed, with the most recent result on the right and the oldest on the left. Example: If the field contains XXXXXXYY, the two most recent NTP transactions have been successful while the previous six have failed.

Command output	Meaning	
delay		Indicates the time, in milliseconds, between an NTP request and the answer.
offset		The difference in milliseconds between the time on your local computer and that on the NTP server.
Jitter		The error rate in your local clock, expressed in milliseconds.

To switch from a Network Time Server to a manual time zone configuration:

1. Click **Disable Network Time Server** and then click **Save**.
2. Select your time zone.
3. Enter the date and time in the fields provided.
4. Click **Save**.

Note:
A reboot is required to update any running applications with new date/time information.

30.40 Add or Delete Hostnames and Addresses

You can add or delete devices (servers, computers, printers) to your network by adding the hostname or IP address to the MSL server.

Under **Configuration**, click **Hostnames and Addresses**. The form lists hostnames and addresses of the devices that are currently in the managed network.

Field	Description
Hostname	Displays the hostname of the device.

Field	Description
Location	**Local**: a hostname with an IP on a local network **Remote**: a hostname with an IP on a remote network **Self**: alternative hostname for this host
IP Address	IP address on local network.
Ethernet Address	IP address accessible from Internet.

To add the hostname of a network device:

1. Under **Configuration**, click **Hostnames and Addresses**
2. Click **Add Hostname**.
3. Enter the **Hostname**. The hostname must start with a letter or number and must contain only letters, numbers, and hyphens.
4. From the **Domain** list, select the Domain where this host resides.
5. In the **Location** list, select visibility (Local, Remote, Self).
6. Click **Next**.
7. Confirm the details and then click **Add**.

To edit the location of a hostname:

1. Under **Configuration**, click **Hostnames and Addresses**.
2. In the current list of hostnames, click the Modify link that corresponds to the hostname you want to modify.
3. Edit Location and then click **Next**.
4. Confirm the details and then click **Save**.

To remove the hostname of a network device:

1. Under **Configuration**, click **Hostnames and Addresses.**
2. In the current list of hostnames, click **Remove** in the Action column.
3. Click **Remove**.

30.41 Manage Domains and DNS Settings

This form allows you to define the Domain Name Service (DNS) that will be associated with the MSL server. This name will be the default domain for the email and web server. You can also use this form to configure other virtual domains in the network.

Caution: Do not change the primary domain name after you have set it up. If you do, you will have to reboot the server and all of the clients, and users may have to manually modify items such as Web browser bookmarks that point to the server.

To define the DNS name for the MSL server:

1. Under **Configuration**, click **Domains**
2. Click **Modify Corporate DNS settings**.
3. Enter the primary and secondary DNS server IP addresses if this server does not have access to the Internet, or if you have special requirements for DNS resolution. Leave these fields blank unless you have a specific reason to configure other DNS servers. Do not enter the address of your ISP's DNS servers because the server is capable of resolving all Internet DNS names without this additional configuration.
4. Click **Save**.

To configure other virtual domains:

1. Click **Add Domain**.
2. Enter the **Domain Name** and a brief description.
3. For the web site, you may choose your primary web site or any i-bay as the content.
4. Select whether this domain is **Resolved locally**, passed to the **Corporate DNS servers**, or resolved by the **Internet DNS servers**. The default will be correct for most networks.
5. Click **Add**.

30.42 Configure IPv6 in IPv4 Tunnel

To enable isolated IPv6 hosts and networks to reach each other over an existing IPv4 network infrastructure, you can configure an IPv4-in-IPv6 tunnel. At the tunnel head end, IPv6 packets are encapsulated into IPv4 packets and sent to the remote tunnel destination. At the destination, the IPv4 packet headers are stripped and the original IPv6 packets are forwarded into the IPv6 cloud.

Until the IPv4 and IPv6 protocols are able to run on the same network infrastructure using dual-stack technology, a transitional mechanism such IPv4in-IPv6 tunnelling is required to facilitate communication.

Note:
Similar to Port Forwarding, this feature is not available in a server-only configuration. It is only available when the server is operating in server-gateway mode.

Preconditions

- The IPv4 address of the remote endpoint must be reachable via ICMP (Internet Control Message Protocol).
- If you are behind a firewall, please make sure it allows passage of Internet Protocol 41. This protocol is contained in the IPv4 header and indicates that an IPv6 packet is encapsulated within the IPv4 packet.

To configure an IPv4-in-IPv6 tunnel:

1. Under **Configuration**, click **IPv6-inIPv4**.
2. Configure the settings as required and then click **Save**:

Setting	Description
IPv4 Address of the Remote End	Enter the IPv4 address of tunnel destination. This address must be routable on the IPv4 network. Typically, it is the external interface of the router located at the destination.
IPv6 Address of the Tunnel (Optional)	If the MSL server is functioning as a gateway to the internet, you can configure its external tunnel interface with an IPv6 address. This enables the interface to be addressable by IPv6 traffic. You may configure only one address on this interface. If this field is left blank, no address will be assigned to the external tunnel interface on the MSL server. **Note**: Your service provider provides this IPv6 address.
IPv6 Networks	Enter one or more IPv6 network addresses for the destination. Based on these entries, the system creates a routing table that defines the ultimate destination of the IPv6 packets that are being tunneled. You can enter a single address or a block of addresses (specified by writing a slash (/) followed by a number which defines the length of the network prefix in bits). Use commas to separate multiple entries.

30.43 Configure SNMP Support

SNMP (Simple Network Management Protocol) provides a set of operations and a protocol to permit remote management and remote monitoring of a network device and/or its services. This server currently offers support for remote monitoring via get requests and traps using both IPv4 and IPv6 protocols.

Note:
SNMP service is disabled by default.

Configure SNMP Settings

To configure SNMP support:

1. Under **Configuration**, click **SNMP**.
2. Set **Service status** to **Enabled** to support SNMPv1, SNMPv2c, and SNMPv3.
3. Complete the following fields as required and then click **Save**.

Field	Description
SNMPv2c community string for read-only access	Enter the community string that SNMPv2c clients use to monitor this server via get requests and traps. The community string defaults to "public".
SNMPv2c network access setting	Select the network access setting for SNMPv2 services: • Localhost only - Default setting. • Immediate local network only - Allows access to local networks that are directly connected to the LAN. (These networks are on the same subnet as the server's private interface.) • All configured trusted networks - Allows access to all networks that are configured in the Networks panel. These networks may not be on the same subnet as the server (that is, they may be attached via a router).

Field	Description
SNMPv3 Settings	To facilitate SNMPv3 communication, you must add a user account to the MSL server that matches an account on the SNMP manager. This "User-based Security Model" (USM) enables unique authentication and encryption settings to be configured for each account. For instructions, see Configure SNMPv3 Users.
System contact address	Specify the email address to which all system notifications should go. • If Email service is enabled, and this field is blank, the address defaults to the Admin forwarding address. • If Email service is not set, the address defaults or to the local-admin account.
System location	Enter a string that identifies the location of the system. (ie. Server room 2, rack 1)
Vital process monitoring	To monitor the server's vital processes, like the web server, secure shell daemon, mail server (with the 6040 blade), and so forth, leave this option at its default of "Enabled". If any problems are detected, an error message and description will be added to the 1.3.6.1.4.1.2021.2.1.100 and 1.3.6.1.4.1.2021.2.1.101 MIB columns, respectively, available via a GET request.
Monitor disk usage	To monitor disk space usage on your server's root partition, leave this option at its default of "Enabled". If any problems are detected, an error message and description will be set in the 1.3.6.1.4.1.2021.9.1.100 and 1.3.6.1.4.1.2021.9.1.101 MIB columns, respectively, available via GET request.

Field	Description
Disk space threshold	If you are monitoring disk space usage on your server's root partition, you need to decide upon a threshold value at which the issue will be flagged at the predefined OID. You may leave this at the default value of 5%, or supply a value. If you supply a value of your own, it may be a numerical percentage of the overall disk space, followed by a percent sign (no spaces), or you may provide an absolute value in bytes.
Monitor CPU usage	To monitor the server's use of the CPU, leave the following setting at "Enabled". If any problems are detected, and error message and description will be set in the 1.3.6.1.4.1.2021.10.1.100 and 1.3.6.1.4.1.2021.10.1.101 MIB columns, respectively, available via GET request.
One minute CPU threshold	If you have CPU monitoring enabled, you must choose a threshold value for the one minute load average, above which this server will flag the error at the previously mentioned OID. The value must be a positive real number with no more than two decimal places of precision.
Five minute CPU threshold	If you have CPU monitoring enabled, you must choose a threshold value for the five minute load average, above which this server will flag the error at the previously mentioned OID. The value must be a positive real number with no more than two decimal places of precision.
Fifteen minute CPU threshold	If you have CPU monitoring enabled, you must choose a threshold value for the fifteen minute load average, above which this server will flag the error at the previously mentioned OID. The value must be a positive real number with no more than two decimal places of precision.

Field	Description
Trap host or address	If you wish to send trap messages to a remote host or hosts, whenever the server boots, the snmpd daemon starts and for authentication failures with the snmpd daemon, enter the hostname or IP address of the host designated to receive these trap messages. If this is left blank, traps will not be sent. To send traps to more than one host, enter the hostnames and/or IP addresses separated by commas.
SNMPv2c Trap community string	Enter the trap community string to use when sending trap messages. If you do not enter a trap community string, the community string for read-only access will be used.
SNMPv3 Trap username	
Download Mitel enterprise MIBs	If you have network management software that you would like to use to monitor this server via SNMP, and would like to import Mitel's enterprise MIBs into it, download them by clicking **Download**. **Note**: The file you receive is a zip file, so you require appropriate software to open it. Additionally, the MIB files are in Unix file format, so the MS Windows Notepad is not an appropriate application to use in opening them.

SNMP Trap Details

The SNMP trap details are listed below :

```
<application name="sas" oid =".1.3.6.1.4.1.1027.1.7.8">

<TrapSeverity>2</TrapSeverity>

<eventtype name="MOM Startup">

<severity>2</severity>
```

```
<traptype>status</traptype>

</eventtype>

<eventtype name="MOM Crash">

<severity>5</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="LdapFailed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="IDS status">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="IDS error">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="SDS Join Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="SDS Join Completed">

<severity>2</severity>

<traptype>status</traptype>
```

```
</eventtype>

<eventtype name="Device Data Notifications Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Device Data Notifications Completed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Device Data Notifications Failed">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="User Sync Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="User Sync Completed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Device Sync Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>
```

```
<eventtype name="Device Sync Completed">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Device Sync Failed">
<severity>4</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Problem Detected">
<severity>4</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Reconcile Startup Error">
<severity>4</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Reconcile Conflicts Detected">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Reconcile Analysis Started">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Reconcile Analysis Completed">
```

```
<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Analysis Failed">

<severity>4</severity>

<traptype>status</traptype>

</eventtype> <eventtype name="Reconcile Execution Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Execution Completed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Execution Failed">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="SDS Sync Required">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Unsupported MiVoice Business">

<severity>4</severity>

<traptype>status</traptype>
```

```
</eventtype>

<eventtype name="User Sync Incomplete">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

</application>
```

Configure SNMPv3 Users

If you implement support for SNMPv3, you must add at least one user account that matches an account on the SNMP manager. As part of this configuration, you can enable authentication and encryption.

To add an SNMPv3 user:

1. Under **Configuration**, click **SNMP**.
2. Under **SNMPv3 Settings** , click **Configure SNMPv3 Users** .
3. Complete the following fields as required and then click **Add**.

Field	Description
User name	Type a user name (also known as "securityname") for the SNMPv3 user.
Authentication Type	Select the Authentication Type that matches SNMP manager/agent configuration: • MD5 • SHA1 • None (no authentication)
Authentication Password	If you selected an Authentication Type (MD5 or SHA1), you must enter an authentication password (also known as "authentication passphrase") at least eight characters long.
Privacy Protocol	Select the Privacy Protocol that matches SNMP manager/agent configuration: • DES • None (no encryption)

Field	Description
Privacy Password	If you selected a Privacy Protocol (DES), you must enter a privacy password.
Engine ID (Optional)	If the SNMP manager requires a hard-coded Engine ID, enter it here. Otherwise, leave this field blank and the SNMP manager will discover the Engine ID automatically.

30.44 Configure Network Interface Card Settings

This panel allows you to configure the speed and duplex settings for the Network Interface Cards (NIC) that have been enabled in the server. MSL supports the following combinations of NICs:

- a "Local" adaptor for connection to the Local Area Network (LAN-only mode) or
- a "Local" adaptor for connection to the Local Area Network AND a "WAN" adapter for connection to the Wide Area Network (Network Edge mode) or
- a "Local" adaptor for connection to the Local Area Network AND a "WAN" adapter for connection to the Wide Area Network AND a “WAN” adapter bridged to the WAN interface of the firewall (Server-gateway with bridged interface mode).

To configure the Speed and Duplex settings of a NIC:

Note:
For virtual deployments, the fields are read-only. You cannot configure the settings from this page.

1. Under **Configuration**, click **Ethernet Cards**.
2. Set the **Auto Configuration** field to **Off**, and then click **Save**.
3. Set the **Speed** and **Duplex** parameters, and then click **Save**. All other settings are read only. See the following table for descriptions of the settings.

Note:
Speed and Duplex are read only if the Ethernet card does not support multiple options.

Setting	Description
Link detected	**Yes**: NIC is connected to the network. **No**: NIC is not connected to the network.
MAC Address	Media Access Control address of the Network Interface Card
Driver	Driver (for example: tg3) of the Network Interface Card.
Speed	Data transfer rate. Available settings are determined by the Ethernet card. Only supported settings are displayed.
Duplex	**Half-duplex**: uses only one wire pair with a digital signal running in both directions on the wire. **Full-duplex**: uses two pairs of wires to establish a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device. Full-duplex data transfer provides faster data transmissions than half duplex.
Auto Negotiation	Auto Negotiation is an Ethernet process that allows two connected devices to choose common transmission parameters, such as speed, duplex mode, and flow control. During this process, the connected devices first share these parameters and then choose the fastest transmission mode they both support. Select **On** to apply Auto Negotiation; select **Off** to configure the Speed and Duplex settings.

30.45 Review Server Configuration

To review the server configuration information, under Configuration, click Review configuration. The following data for the MSL server is displayed:

Networking Parameters

- Local Adaptor IPv4 address/subnet mask and optional IPv6 address

- Internet visible IPv4 address and optional IPv6 address
- Gateway IPv4 address and and optional IPv6 address
- Additional trusted local networks
- DHCP server

Server names

- DNS server
- Web server
- Proxy server
- FTP server
- SMTP, POP, and IMAP mail servers

Domain information

- Primary domain
- Virtual domains
- Primary web site
- Server manager
- User password pane
- Email Addresses

30.46 Support and Licensing

License Server

MiCollab solutions with MiVoice MX-ONE, MiVoice 5000 and MiVoice Office 400 will use the Licenses & Services Application (SLS Licenses Server), whereas MiCollab solution with MiVoice Business and MiVoice 250 will be licensed through Licenses & Services AMC Application (Application Management Center).

Both the License Servers can be accessed through Mitel MiAccess portal.

About AMC Licensing

MiCollab solution with MiVoice Business supports licensing through the Mitel AMC. The Mitel AMC manages the software licensing and entitlement of the Software Assurance Program.

After you obtain an Application Record ID (ARID) from the AMC, the AMC uses your Application Record ID (ARID) to provide you with access to licenses, software releases, and upgrades. With the AMC license server, the following changes will be seen:

- All new or existing installation of MiCollab solution with MiVoice Business and MiVoice Office 250 will be licensed using AMC license server.

About SLS Licensing

MiCollab Solution with MiVoice MX-ONE, MiVoice 5000 and MiVoice Office 400 are licensed on SLS License Server. MiVoice Business Subscription Edition 2, (only available for new/greenfield deployments),

uses the SLS License Server (sync.sls.mitel.com). In SLS license server, the ARID is called as ServiceLink ID. The ServiceLink ID for the MiCollab server is where all license parts including UCC User Licenses are applied.

With the license server migration towards SLS the following changes will be seen:

- All the **new installations** of MiCollab servers connected with a MiVoice MX-ONE, MiVoice 5000, or MiVoice Office 400 will receive their Licenses from the SLS License server available on MiAccess from the **Licenses & Services** link.
- **All the existing installations** of MiCollab servers connected with a MiVoice MX-ONE, MiVoice 5000 or MiVoice Office 400 would be capable to continue receiving their licenses from the AMC License Server available on MiAccess **until** the site administrator adds or changes licensing (e.g. UCC licenses, SWA, etc) for the customer site.
- The MiCollab administrator **must manually** set the license server FQDN of the SLS license server for all the MiCollab Solutions with MiVoice MX-ONE, MiVoice 5000, and MiVoice Office 400. FQDN is empty in case of AMC.

For more information on licensing, see the Installation and Maintenance Guide for the respective PBXs.

About MS Office 365 licensing

The Microsoft Office 365 supported licenses are as follows:

- E3 - Office 365 Basic and Office 365 OAuth2.0
- E5 - Office 365 Basic and Office 365 OAuth2.0
- Office 365 Government GCC - Office 365 OAuth2.0
- O365 Business Premium - Office 365 Basic and Office 365 OAuth2.0
- Office365 Business Standard - Office 365 Basic and Office 365 OAuth2.0

30.47 Panel Requires Upgrade

Server Manager pages display "Panel requires update" if the associated applications must be upgraded to run on the currently installed version of MSL. You will see this message displayed after you upgrade MSL to a new version, but before you have upgraded the installed applications blades to the required version.

For MiCollab and MiVoice Business Express systems, you must upgrade the MiCollab applications from the server conso l e. Refer to the *MiCollab Installation and Maintenance Guide* or the *MiVoice Business Express Deployment Guide* for instructions.

For MSL systems, upgrade the blades from the Blades panel.

Cloud Service Provider 31

This chapter contains the following sections:

- Google
- Microsoft

31.1 Google

31.1.1 Google Gadget Configuration

Google provides a framework for users and third parties to implement enhancements to Google Apps called "gadgets." MiCollab Audio, Web and Video Conferencing provides a gadget which users can employ to transform their Google Calendar events into one-time conferences with a simple click.

Note:
For complete instructions concerning how to implement the Google gadget, see the Google Apps Integration for AWV topic.

Address Configuration

Use this procedure to configure the publicly accessible address of the gadget service. Typically, this is external address of the firewall (IP address or FQDN), which should be configured to forward HTTP requests to the gadget service.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Google Apps**.
3. Select the **Gadget Configuration** tab.
4. Click **Edit**.
5. Enter the **External FQDN or IP address** of the MSL server. Typically, this is the publicly accessible address configured on the enterprise firewall configured to forward requests to the MSL server. The MiVoice Border Gateway can provide this service if it is configured to function as a web proxy for the Google Calendar integration to AWV.

Note:
Google gadget users will receive a link to this address in their Service Information (Welcome) Email

6. Click **Save**.

31.1.2 Google Apps Integration for MiCollab Audio, Web and Video Conferencing

With this release, MiCollab Audio, Web and Video Conferencing can be integrated with Google Apps. This enables users to transform their Google Calendar events into one-time conferences simply by clicking a gadget. In future releases, more features will be added such as the ability to initiate calls from Google Calendar.

Preconditions:

- In the System Options, select **Use HTTPS Only**. You must then configure a third-party SSL certificate in the MSL Server Manager. Note that you may not employ the self-signed certificate; using it will cause Google Apps integration to fail.
- In the Web Conferencing Settings, enter 80 for the **Internal Port** and 443 for the **External Port**.

Administrator tasks

Enable Google Apps Integration with MiCollab Audio, Web and Video Conferencing

The administrator must do the following:

1. Configure OAuth 2.0 for Service Accounts on page 2013

   When you set up an OAuth 2.0 API project with a service account for the Google Calendar application, you enable MiCollab Audio, Web and Video Conferencing to prove its identity to Google. The two systems can then communicate without involving end users.
2. Configure the Gadget Address

   The gadget address is the publicly accessible FQDN or IP address of the gadget service. After you configure it on the MSL server, users can download the Google- MiCollab Audio, Web and Video Conferencing gadget and transform their Google Calendar events into conferences with a single click. Users will receive a link to the address in their Welcome Email (see next step).
3. Send the Service Information (Welcome) Email

   The Welcome Email contains communications settings such as the user's login credentials, email address and phone number, along with instructions on how to download and configure the Google-MiCollab Audio, Web and Video Conferencing gadget. You should ensure that the Welcome Email is sent to all new and existing users.

4. Configure the Web Proxy

   You must configure your web proxy server to provide a secure interface between Google on the Internet and the MiCollab server on the LAN. If your enterprise is using MiVoice Border Gateway as a proxy server, access the LAN server proxy list and select **MiCollab** as the LAN server and **Google Calendar Integration to AWV** as the user interface (for configuration details, refer to the *MBG online help*). If your enterprise is using a proxy server from another manufacturer, configure it to forward Google Apps traffic (i.e. traffic that includes "google" as part of the FQDN in HTTPS requests) to the MiCollab server.

End-User tasks

Change the Password and Enable MiCollab Audio, Web and Video Conferencing Conference Functionality

Each user must do the following:

1. In your Welcome Email, click the link to the MiCollab End User Portal : https://< MiCollab server address>/portal
2. Log in to the portal using your account information (ID and password).
3. Change your password:

   - Select **Portal Password**.
   - Enter your old password and your new password in the appropriate fields.
   - Confirm your new password and then click **Save**.
4. In your Welcome Email, click the link to enable MiCollab Audio, Web and Video Conferencing conference functionality in your Google Calendar.
5. Select **Yes** to download and install the gadget.
6. Configure the gadget for use:

   - Click **Permissions** and then, in response to the prompt, click **Allow access**.
   - Enter your **Login ID** and **Password**.
   - Click **Save** to complete the configuration.

To create an MiCollab Audio, Web and Video Conferencing conference, access your Google Calendar, select a one-time or recurring event and click **Collaboration** check box in the gadget.

After setup is complete, you can join the conference simply by clicking on the event. Any changes you make to the event, such as adding more guests or changing the start time, will be reflected in the MiCollab Audio, Web and Video Conferencing conference.

Note:

- If you have just upgraded your system to include Google Apps integration, re-send the Welcome Email to all existing users.
- A conference that was created using the Google- MiCollab Audio, Web and Video Conferencing gadget can be viewed on the My Conferences Tab of the MiCollab Audio, Web and Video Conferencing Web Interface. However, if you edit this conference in the MiCollab Audio, Web and Video Conferencing interface, your updates will *not* be reflected in the Google Calendar.

- The Google- MiCollab Audio, Web and Video Conferencing gadget is available only for English variants of the product.
- To enable Google- MiCollab Audio, Web and Video Conferencing conferencing functionality, you must complete all three steps of the above-noted procedure.
- This feature can be expected to behave differently on different devices and browsers. It is optimized for operation on Google Chrome in a desktop environment. If you are using Internet Explorer and the MiCollab server is not equipped with proper certificates, you will need to install the Mitel Root Certificate in your browser.

Internet Explorer

Note:
Steps may vary based on your browser, but the intent is to install the Mitel Root Certificate in the **Trusted Root Certification Authorities** store.

1. Save the Mitel Root Certificate on your PC hard drive.
2. Launch Internet Explorer.
3. Select **Tools** and then click **Internet Options**.
4. Click the **Content** tab and then click the **Certificates** button.
5. Select **Trusted Root Certification Authorities** and click **Import**. The Certificate Import Wizard opens.
6. Click **Next**.
7. Click **Browse** and browse to the **mitelcert.cer** file and click **Open**.
8. Click **Next**.
9. Select **Place all Certificates in the following store**.
10. Click **Browse** and select **Trusted Root Certification Authorities**.
11. Click **OK**.
12. Click **Next**.
13. Click **Finish**.
14. Click **Yes**. An Import was successful dialog appears.
15. After the certificate is installed, restart Internet Explorer.

- In some circumstances, a user's Google Calendar may fall out of synchronization with MiCollab Audio, Web and Video Conferencing. For example, if the user creates a new Google- MiCollab Audio, Web and Video Conferencing conference and then quickly closes their Google Calendar or internet browser, MiCollab Audio, Web and Video Conferencing may fail to create a corresponding conference. Similarly, if the user creates a new Google- MiCollab Audio, Web and Video Conferencing conference while the MiCollab server is being rebooted, a corresponding conference will not be created in MiCollab Audio, Web and Video Conferencing . To correct an out-of-sync error, the user should delete the event in Google Calendar and then recreate it.

31.1.3 Configure OAuth 2.0 for Service Accounts

Use this procedure to configure a secure connection between Mitel applications such as NuPoint UM and Google Apps such as Google Calendar using the OAuth 2.0 protocol.

With this type of server-to-server interaction, the application has to prove its own identity but end users do not need to be involved.

Create an API Project and Client ID in Google

Note:

The following instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help:

1. Log In to the Google API Console:
   a. Open a web browser and navigate to https://code.google.com/apis/console.
   b. Enter the domain administrator **Email** and **password** to log in.
2. Create the Project:
   a. Click the **Create project** button.
   b. Enter the **Project name** (for example, "NuPoint Advanced UM") and click **Create**. Remain in the project.
3. Enable Google APIs for the project:
   a. Open the side menu and select **API Manager**.
   b. Select a Google API such as "Calendar API" and click **Enable API**.
   c. Repeat for all Google APIs you want to support. Remain in the project.
4. Create the Service Account with Client ID:
   a. Open the side menu and select **Permissions**.
   b. Under the **Service accounts** tab, select **Create service account**.
   c. Enter a **Name**, select **Furnish a new private key** and **JSON** as the file type, and then select **Enable Google Apps Domain-wide Delegation**. Set a **Product name** if prompted.
   d. Click **Create** and **Close**. The service account is created and the file containing the Private Key and Client ID is downloaded.

Note:
Store the file in a safe location. You will require it to establish your credentials to MSL.

e. For the service account you just created, click **View Client ID**.
f. Copy the Client ID and click **Cancel**. You will require the Client ID in the next procedure.

5. Manage API Client Access (API Scopes): Once a service account is created, you must enable the scope of access for your client ID.

a. Access the Google Admin console:

i. Open a web browser and navigate to admin.google.com.
ii. Enter the domain administrator **Email** and **password** to log in.

b. Click **Security**.
c. Click **Show more** and then click **Advanced settings**.
d. Under **Authentication**, click **Manage API Client access**.
e. On the Manage API client access panel:

i. Paste the client ID in the **Client Name** box.
ii. Enter the following in the **One or More API Scopes** box:

To support Gmail integration (for NuPoint Advanced UM), enter: https://mail.google.com/

iii. Click **Authorize**.

The client ID now has access to resources in the specified domains.

Upload Credentials to MSL

This procedure involves uploading your OAuth 2.0 credentials (service account Client ID and Private Key) from your computer to MSL. MiCollab employs these credentials to integrate with publicly available Google Apps.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Google Apps**.
3. Select the **Service Account** tab.
4. Under **Configuration**, choose the following files from your computer:

- Service Account ID (.json file)
- Private Key (.p12 file)

Note:
The **Private Key (.p12 file)** file is required only for earlier implementations.

5. Click **Upload Credentials**.
6. Confirm that the Client ID, Email address, and Private Key are correct by comparing them to the corresponding fields in the Google API project.

It is now possible to configure a secure connection to publicly-available Google Apps using the OAuth 2.0 protocol for the Service Account client ID.

Note:

- You can generate another private-public key pair and then upload the private key to the Service Account in MSL.
- OAauth 2.0 data is not included in system (MSL) backups. Accordingly, if you perform a backup and restore procedure, you must then re-enter the OAuth 2.0 data in order to restore the Google Apps integration.

31.1.4 Configure OAuth 2.0 for Installed Applications

Use this procedure to configure a secure connection between integrated applications such as MiCollab Client and Google Apps such as Google Contacts or Google Calendar using the OAuth 2.0 protocol.

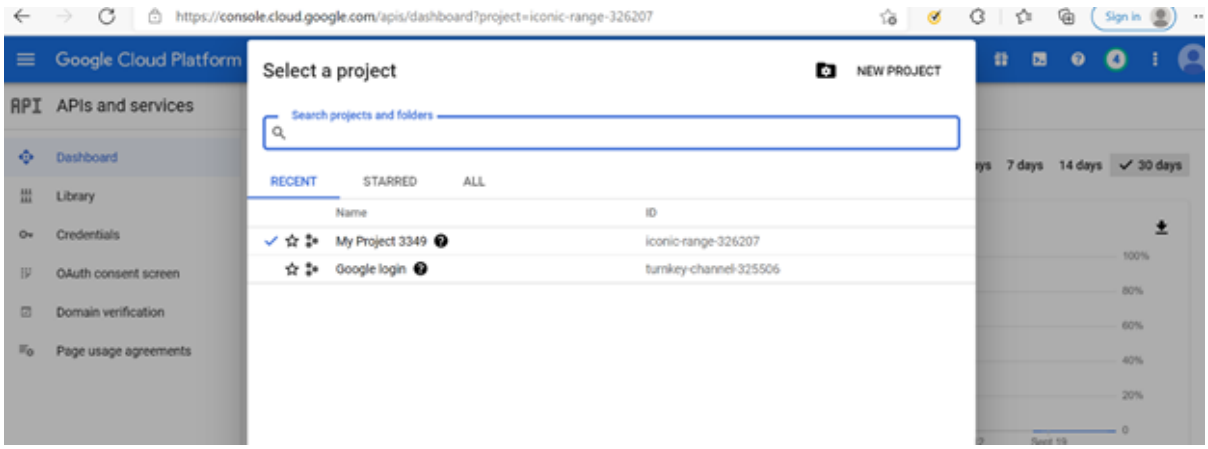
If OAuth 2.0 authorization is successful then Google will grant an access token to the application on the Mitel Standard Linux server. These tokens can be re-issued when they expire or if the project is changed in any way.

Create an API Project and Client ID in Google

1. Access the Google API console:

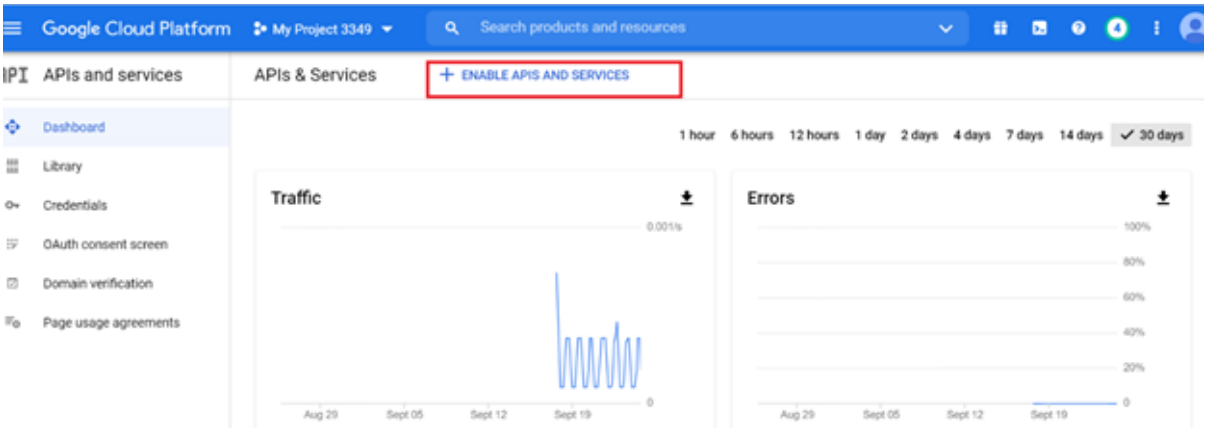
   a. Open a web browser and navigate to https://code.google.com/apis/console.
   b. Enter the domain administrator **Email** and **password** to log in.

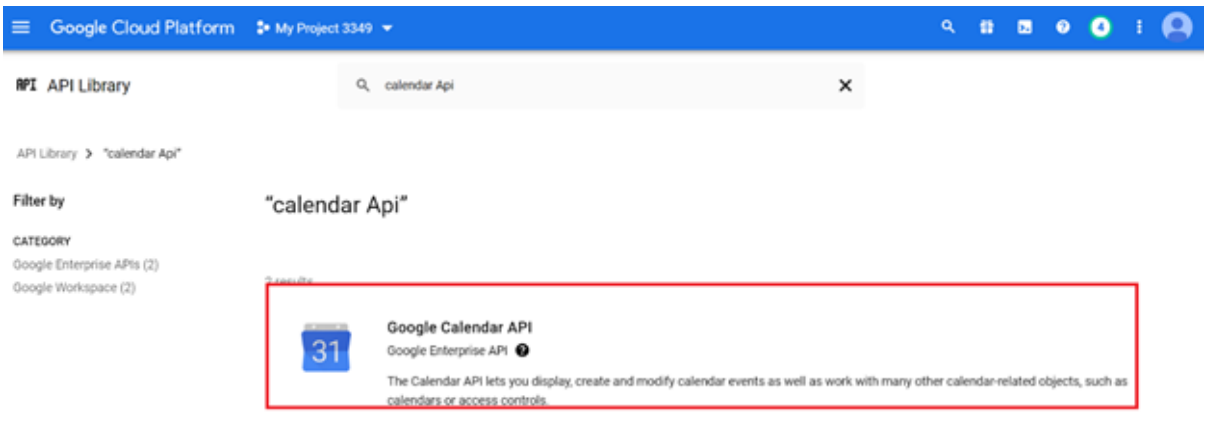
2. Create a new project and give it a name such as "NuPoint Advanced UM." Remain in the project.



3. Enable Google APIs for the project:

   a. Open the side menu and select **API Manager**.
   b. Select a Google API such as "Calendar API" and click **Enable API**.





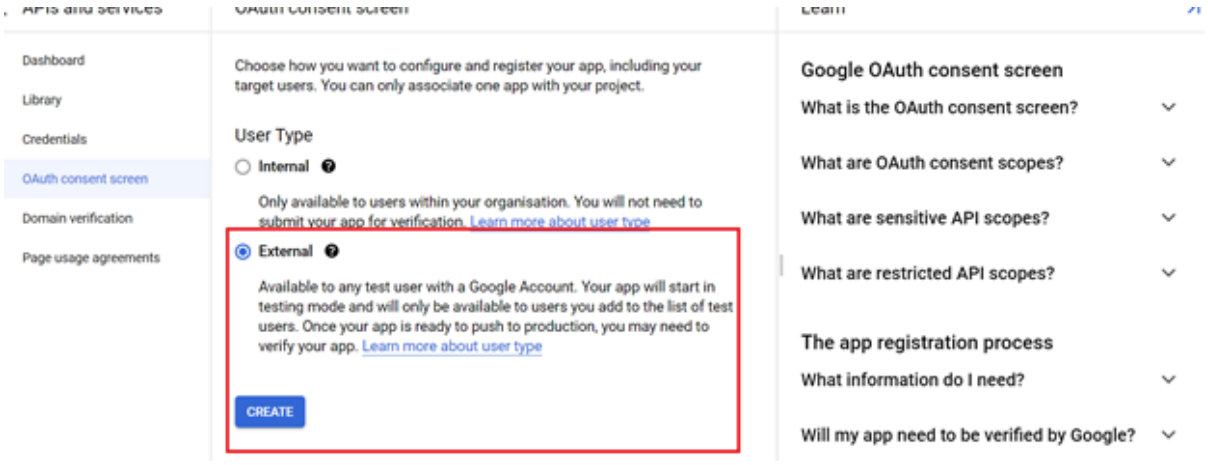
   c. Repeat for all Google APIs you want to support.

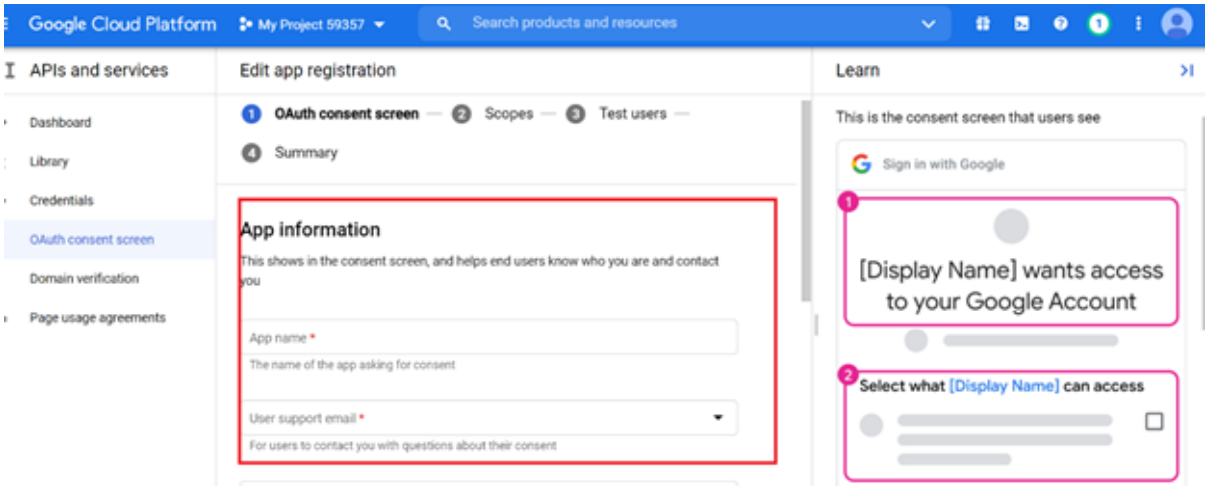
Note:

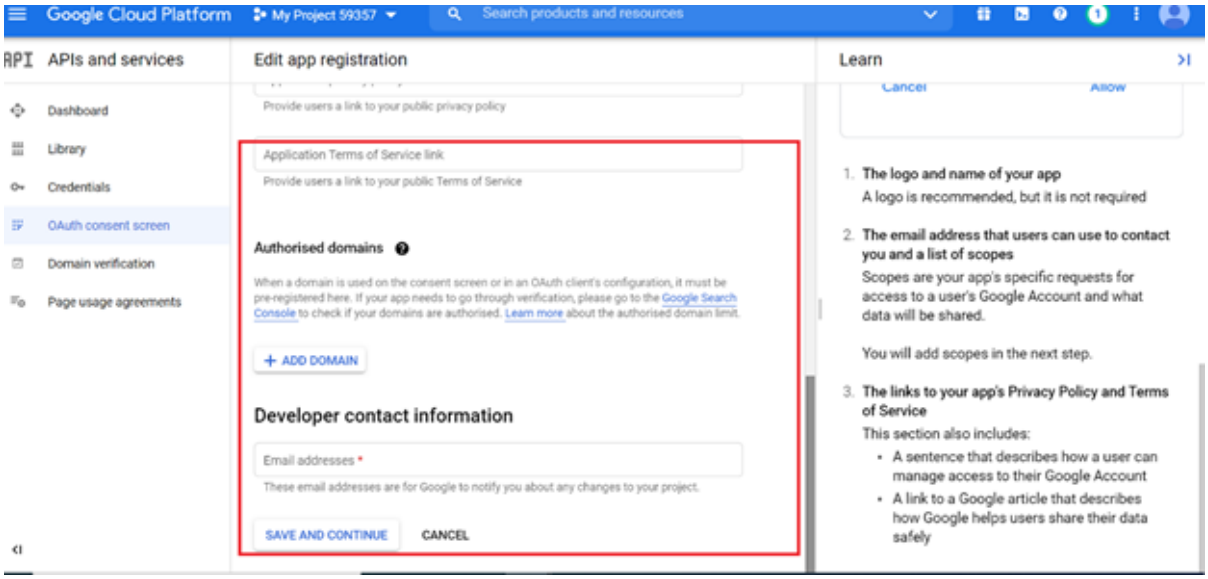
The preceding instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help: https://developers.google.com/workspace/guides/create-project.

4. Configure the OAuth 2.0 consent screen.

   To configure the OAuth consent screen, please follow the following link: https://developers.google.com/workspace/guides/create-credentials#configure_the_oauth_consent_screen.



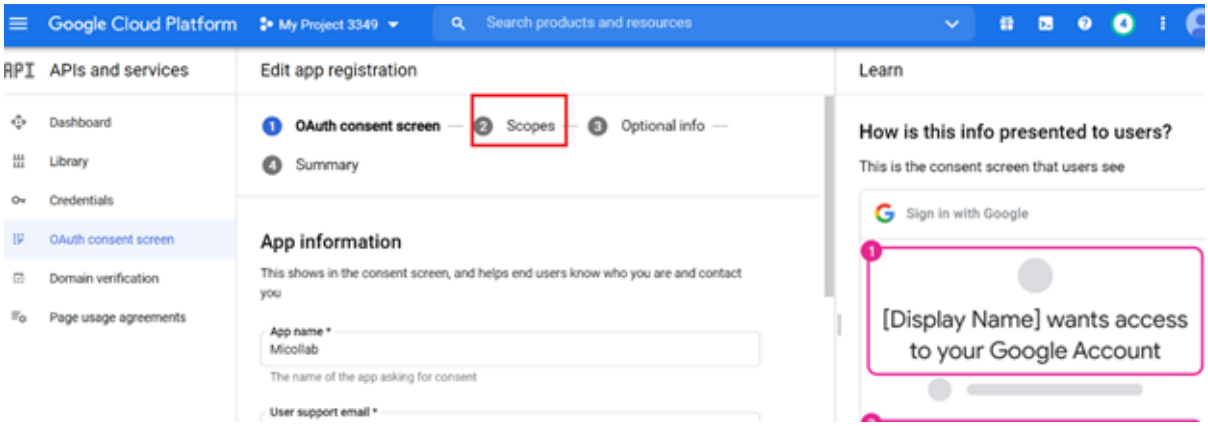


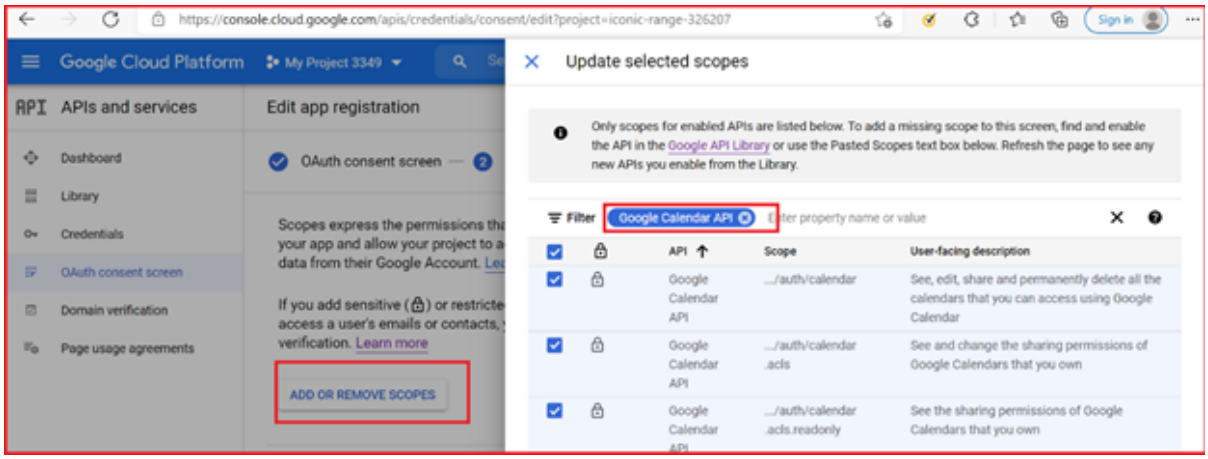


Note:

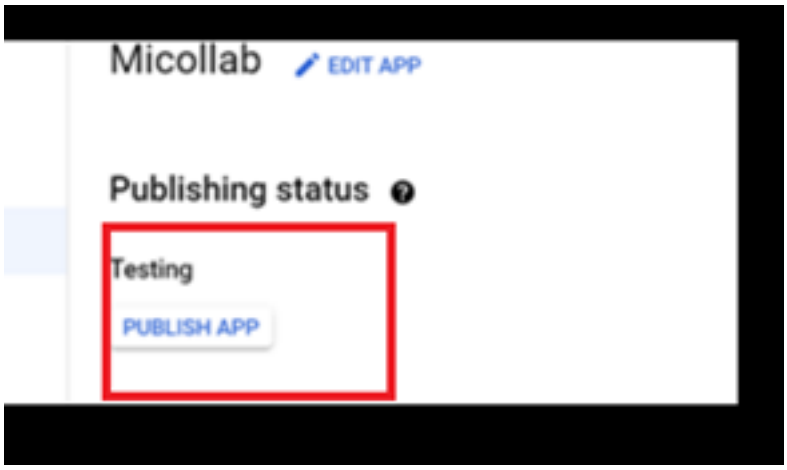
Following scopes are required for Google Calendar API:

- /auth/calendar.readonly
- /auth/calendar.events.readonly

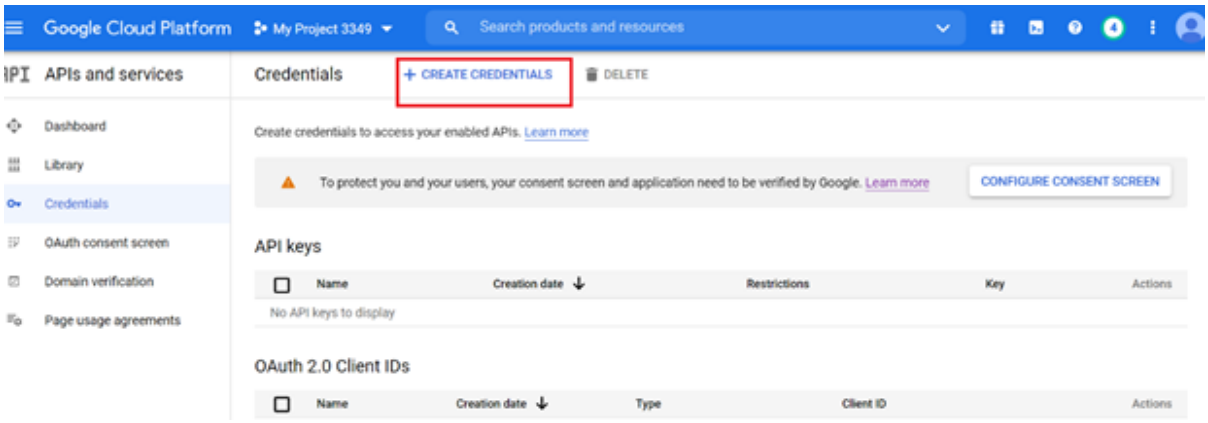


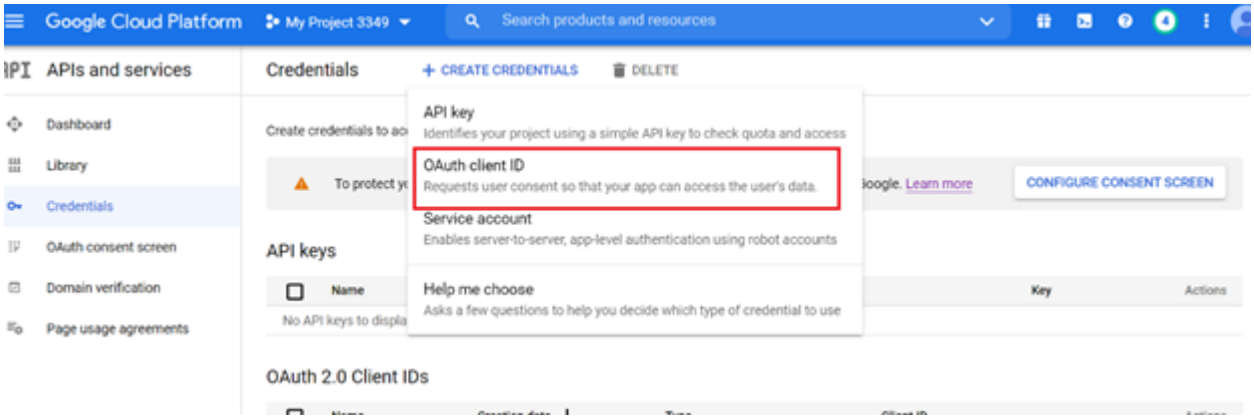


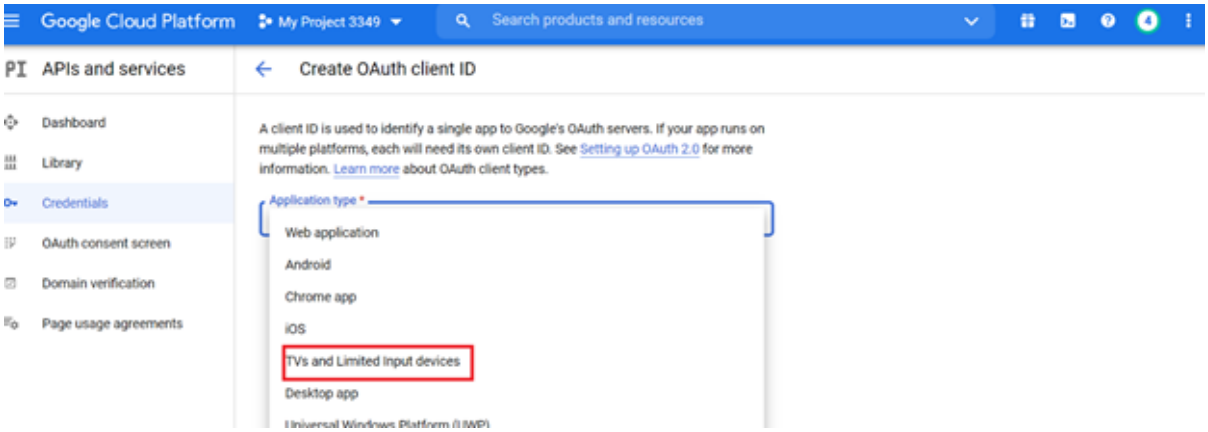
5. Publish the application.

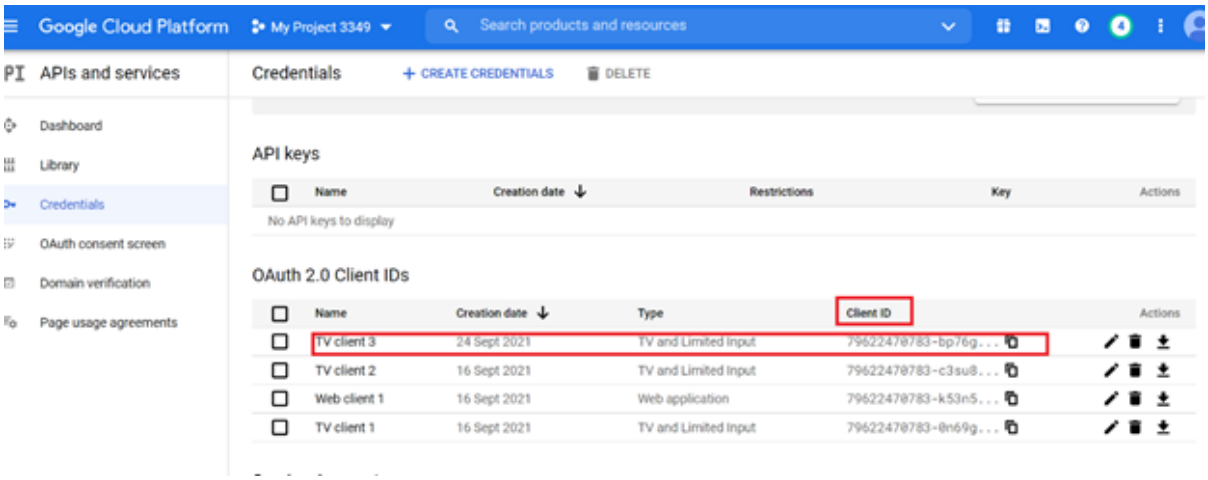


6. Create the OAuth 2.0 Client ID and Secret for the project:









To create the OAuth 2.0 Client ID and Secret, please follow the following link: https://developers.google.com/workspace/guides/create-credentials#create_a_oauth_client_id_credential

Note:

For the Google Calendar API, please select Application type as TVs and Limited Input devices.

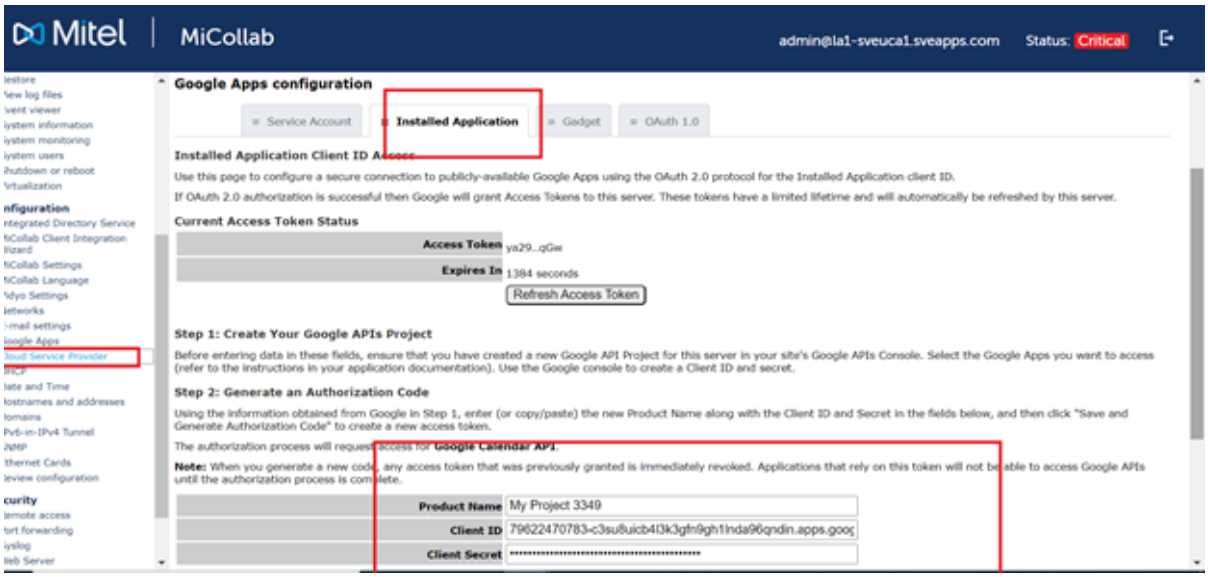
Google provides a **Client ID** and **Client secret**. Record them and the **Product name** for use in the next procedure.

Generate an Authorization Code in MSL

This procedure involves copying your OAuth 2.0 credentials (client ID and matching secret) from the Google APIs console to MSL, which generates an authorization code and then grants an access token. The application on the MSL server employs the access token to integrate with Google services.

1. Log in to the MSL Server Manager as "admin".

2. In the navigation tree, under **Configuration**, click **Google Apps**.

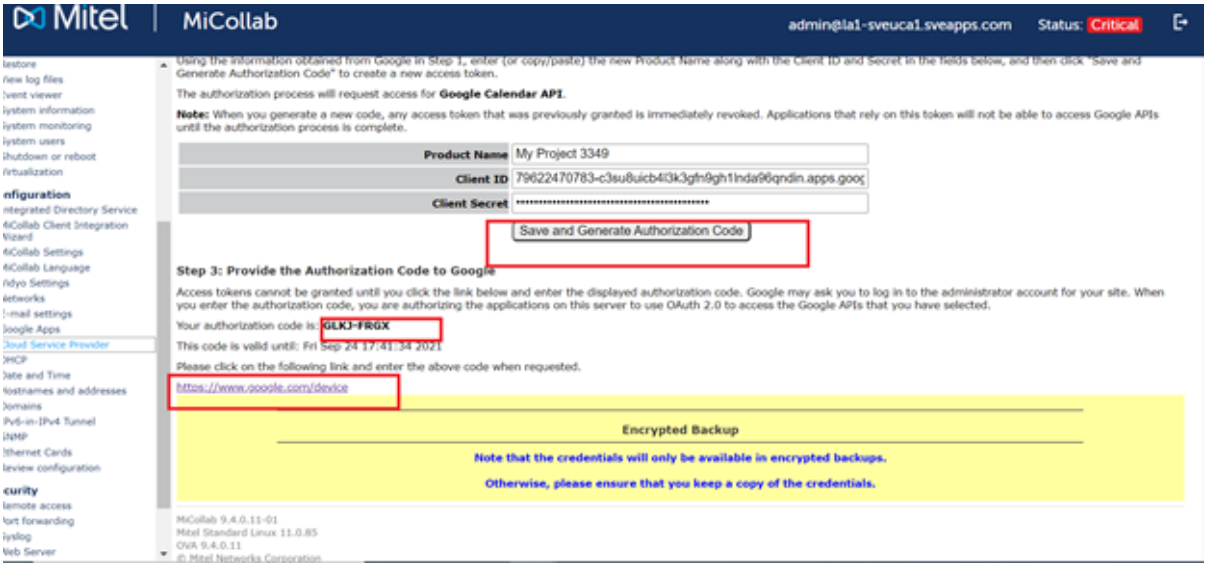


3. Select the **Installed Applications** tab.
4. Under **Step 2**, copy and paste the following from the Google APIs console:

   - Product Name
   - Client ID
   - Client secret

5. Click **Save and Generate Authorization Code**. The authorization code is generated and displayed. Remain on the Installed Applications tab in the MSL Server Manager.
6. Under **Step 3**, do the following:

   a. Copy the authorization code.
   b. Click the link provided to access the Google API console.



Allow Access Permission in Google

1. After clicking the link to access the Google API console, log in to your account.
2. Submit the authorization code to allow access in Google.

Google grants the access token, which enables MSL to access services in the API project. Note that after the access token is generated, the panel displays its current status (access token ID and expiry time in seconds).

Note:

- The access token is valid only for the set of operations and resources described in the token request. For example, if an access token is issued for the Google Calendar API, it will not grant access to the Google GMail API.
- If you regenerate the client ID and secret, you must then regenerate the authorization code in MSL.
- If an access token expires or you wish to change the list of supported services, you can repeat the procedures to Create an API Project and Generate an Authorization Code.
- OAauth 2.0 data is not included in system (MSL) backups. Accordingly, if you perform a backup and restore procedure, you must then re-enter the OAuth 2.0 data in order to restore the Google Apps integration.

31.1.5 About Google Apps Integration

When Mitel Standard Linux applications such as NuPoint UM and MiCollab Client require access to user-generated data that is stored in Google Gmail or Google Calendar, they must meet Google's authentication requirements. Google grants access only when the following conditions are met:

- the application provides its authentication information, and
- the user consents to allow the application to view the account information

All applications that access Google must be registered through the Google APIs Console and must configure access using the Open Standard for Authentication 2.0 (OAuth 2.0) protocol.

OAuth 2.0 is a relatively simple protocol. To begin, you register your application with Google in order to creates a client ID. Then your client application requests an access token from the Google Authorization Server, extracts a token from the response, and sends the token to the Google API that you want to access.

When you create a client ID, you must specify the type of application it is for. For integration with Mitel applications, two options are available:

- Installed Application - Select this option if the application is to be installed on a mobile device, tablet or computer. The registration process results in a client ID and a client secret, which you embed in the source code of the application. MiCollab Client requires this configuration.

- Service Accounts - Select this option if the application employs server-to-server interactions, such as those between a web application and Google Cloud Storage. MiCollab Audio, Web and Video Conferencing and NuPoint Unified Messaging require this configuration.

Note:
Support for OAuth 1.0 was deprecated with MSL Release 10.1. If you are currently using OAuth 1.0 and upgrade to the latest MSL software, you should reprogram API access for your application using an OAuth 2.0 Service Account. After you have done this, the OAuth 1.0 tab will be removed from the server manager interface. For new software installations, only OAuth 2.0 is available.

31.2 Microsoft

31.2.1 Configure Microsoft Identity

The OAuth 2.0 protocol is the authentication and authorization method used with the Application identity to access the API permission(s) granted by the tenant administrator.

To configure the Microsoft Identity on MSL, and administer access to the Microsoft resources using the Application identity created in your tenant directory, perform the following on the Microsoft Entra portal:

1. Register an application, see Microsoft help.
2. Obtain the unique Application ID and Tenant ID assigned by Microsoft Entra ID.

Note:

The customer's firewall settings should allow access to the following Microsoft resources:

- outlook.office365.com
- login.microsoftonline.com
- graph.microsoft.com

Perform the following steps under **Cloud Service Provider** to complete the authorization related configuration at MSL:

1. Log in to MSL Server Manager as administrator.
2. Under **Configuration**, click **Cloud Service Provider** > **Microsoft**.

3. Complete the Configuration form:

- **Tenant directory**

  a. Tenant Name (Optional): Enter a descriptive name for the tenant directory. This field is optional.
  b. Tenant ID: Enter Directory (tenant) ID from the Microsoft Entra ID. This field is mandatory.

- **Application Identity**

  a. Application Name (Optional): Enter the descriptive name for the application created during application registration. This field is optional.
  b. Application ID: Enter the Application (client) ID from the Microsoft Entra ID. This field is mandatory.
  c. Application Secret: Enter the client secret obtained from the application Certificates & Secrets page. This field is mandatory.

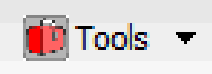
> **Note**:
>
> - Certificate-based authentication is not supported at this time.
> - Once the secret is copied, it cannot be retrieved again; if the secret is lost, another one needs to be created.
> - The admin can revoke the secret by deleting it, in which case a new secret is required.

4. Click **Save.**

> **Note**:
> After a backup restore, the Application Secret will remain intact in the MiCollab if server is restored from an Encrypted backup in the Enterprise. In Google Cloud Platform (GCP), the Application secret will be restored after a backup/restore.

Glossary 32

The following table lists Call Director terms used in this Help system:

Term	Definition
Action	Any of the twelve programmable functions (Over-Ride, Sch edule, Message, Menu, etc.) that determine how a call is handled.
Alias	Another instance of an action in a call flow. Each instance inherits the properties of the original action and is identified by an underline as follows:  To create a call flow with multiple instances of an action, each with different properties, assign the actions unique names.
Alternate Transfer	Sends a call to an external telephone number. Also used for paging and sending text messages.
Answer Supervision	A signal sent by the telephone system when it is connect ing a call to indicate that the called party has answered. S upervised transfers require answer supervision; blind transf ers do not.
Attendant Transfer	Sends a call to the extension designated as the attendant by the System Administrator.
Blind Transfer	Dials the destination and then releases the call regardless whether the destination is busy or not answering.
Call Flow	The series of actions programmed by the call flow owner, which controls how a call is handled.
Call Flow Owner	Can be either an extension user or the System Administra tor. Extension users program personal call flows, which are associated with their own voice mailbox. The Administrat or programs the corporate or line group call flows, and can also add, modify and delete personal call flows.
Call Flow Tree	The graphic representation of the call flow hierarchy.
Call Transfers	(Action) The four types of call transfers that you can add to a call flow to route an incoming call: Blind Transfer, Supervi sed Transfer, Screened Transfer, and Alternate Transfer
Caller ID	(Action) Handles incoming calls certain ways, depending on the caller ID. For example, a call flow owner may configure the Caller ID action to send his manager's calls to his voice mailbox, and send his calls from home to his cell phone.

Term	Definition
Dial-by-Name	(Action) Sends the incoming call to the NuPoint Unified Messaging Dial-by-Name application, which allows callers to key in the name of the party they wish to reach.
Gathered Digits	The collection of digits that are dialed to make a call to the desired phone or mailbox.
Greeting	See Message.
Interflow	Interflow allows calls to be transferred from one call flow directly into another call flow. You use the Transfer and Voicemail actions to transfer a call to another call flow (outgoing interflow), and you use the Override action to determine the call flow for a call that comes in from another call flow (incoming interflow).
Internal/External	(Action) For handling calls based on whether their origin is internal or external.
Line Group Call Flow	Call flow for handling calls to the company's main telephone number(s). Available for programming by the Administrator only.
Menu	(Action) List of recorded voice prompts to which a caller would listen for call-directing instructions. For example, "If you know the extension of the person you wish to reach, press 1. To speak to the sales desk, press 2. To speak to an attendant, press 0." The caller must then press the desired key, or hang up.
Message	(Action) A recording played for a caller. Includes greetings and menu prompts. The call flow owner records the message using their phone.
Multi-key	A Menu option that allows callers to enter multiple digits (for example, extension numbers or voice mailbox numbers).
Override	(Action) Alters the normal call flow for temporary situations such as vacation absences or unexpected office closures. Overrides can be turned on and off from any touch-tone telephone and from Call Director.
Personal Call Flow	Call flow administered by the end user. Personal call flows are associated with the end user's voice mailbox. Administrators can add, delete or modify personal call flows.
Properties	The parameters, such as the destination for a call transfer, that are specific to an action.
Screened Transfer	Similar to a Supervised Transfer, except that the caller's name is first recorded and then played back to the called person. The called person has the option to accept or reject the call.
Supervised Transfer	A transfer that requires the called party to answer; otherwise, the caller is reconnected for further processing.
Result	Outcome of an action. Some actions have multiple results—for example, a Supervised Transfer has Busy, No Answer, or Invalid as its result.
Schedule	(Action) Consists of time slots that define work hours and off hours; therefore, if a user sets their work hours, then a call flow will be treated differently after work hours. In addition, Schedule includes an optional set of holiday hours.

Term	Definition
Mailbox	(Action) Sends the incoming call to a voice mailbox prog rammed by the caller flow owner or obtained from the caller.
Template	A call flow with pre-defined properties and results for all the actions.

Mitel
Powering connections
mitel.com

Copyright 2024, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.