A MITEL
PRODUCT
GUIDE

MiCollab Users and Services Provisioning

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) 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.

®,™ Trademark of Mitel Networks Corporation

Applications 1

This chapter contains the following sections:

1.1 Users and Services

1.1.1 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	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.
First Name	
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 **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.

1.1.2 Using the Interface

1.1.2.1 About the Users and Services Main Page

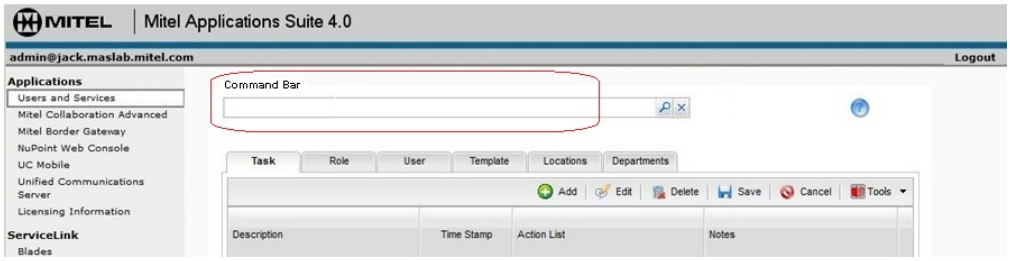
Overview

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.

1.1.2.2 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  . 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  , the search function displays any records that have the number 1001 in the following fields: First Name, Last Name, Number.

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  . The results are displayed in the main window.
4. Click  to clear the Task line.

1.1.2.3 Displaying Data

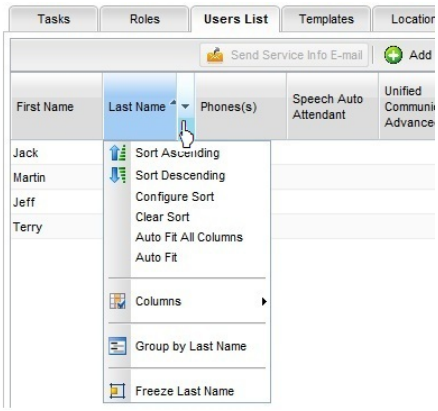
Sorting

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.



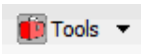
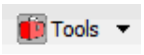
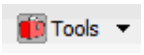
Viewing the Window Tabs

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.

1.1.2.4 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
	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	launch bulk user import or export tool
 Export	
 Report	save a report of the user data as an .dita file
 Print	print a report of the data in the current tab
	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

1.1.3 System Administrator

1.1.3.1 Getting Started

1.1.3.1.1 About the Users and Services Application

The Users and Services Provisioning application is a single, easy-to-use interface that allows you to add, edit, or delete users and their phone and application services on the MiCollab system. Flow Through Provisioning is supported for MiVoice Business platforms. This feature reduces the amount of user data administration.

The system automatically sends Service (Welcome) E-mails to new users that contain the user's communications settings, such as login ID, password, primary e-mail address, phone type and number, and service information. You can configure the Service E-mail with a default or custom greeting message. With the exception of the custom greeting, the information can be sent in two languages.

1.1.3.1.2 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.

1.1.3.1.3 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.

1.1.3.1.4 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	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.
First Name	
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 **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.

1.1.3.2 Manage Network Elements

- Add or Edit Network Elements on page 18
- MiVoice Business Network Element Field Descriptions on page 22
- MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400 Network Element Field Descriptions on page 31
- System Management Tool Access on page 34

1.1.3.2.1 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.

1.1.3.2.2 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

Field	Description	Values
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 bla nk. If this field is left blank, the MiV oice Business defaults this setting to Zone 1.
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
Use NuPoint UM IP Integration Licenses	If the Network Element will support the NuPoint UM application ports select this check box. After you click **Save,** the Network Element (ICP) is configured in the NuPoint UM application. 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.	

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 MiCol lab Client .	7-digit number maximum. (Default applied by MiCW is 7000).

Field	Description	Values
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 M iTAI application interface.)	7-digit number maximum. (Default applied by MiCW is 6400).
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).

1.1.3.2.3 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	Standard IP address notation of four sets of one to three digits separated by periods. For example, 192.168.0.1

Field	Description	Values
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
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, *, #)

Field	Description	Values
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, *, #)

1.1.3.2.4 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:
Acc ess to the MiVoice 5000 Manager (AM7450) and MiVoice MX-ONE management interfaces are not supported from the Network Element page.

1.1.3.3 Manage Licenses

• About UCC Licensing on page 36

- UCC License Bundle Definitions on page 39
- Manage UCC Licensing Bundles (MiVoice Business only) on page 41

1.1.3.3.1 About UCC Licensing

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, MiVoice Business user license, and 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.

Licenses can be assigned via Roles and Templates

Licensing is supported through the Mitel Licenses and Services Tool and the Mitel Software Assurance (SWA) program. The Mitel Licenses and Services Tool 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 ARID to provide you with access to licenses, software releases, and upgrades. In SLS License Server, the ServiceLink ID has the same function like the ARID in AMC.

The partner orders the parts (i.e. CPQ) and the licenses are applied in the partner's License Bank (AMC or SLS). For example, if the partner orders license for MiCollab, including UCC User Licenses, there will be PBX User licenses included in the bundle. Unlike AMC, the SLS provides vouchers based on the server type (MiCollab, PBX) and they are applied separately. Only after synchronization do the roles and templates get impacted by default. Also, existing roles and templates are left as is.

After MiCollab is installed, the system must be synchronized with the license server over the internet to obtain the latest UCC license bundle definitions. The UCC licensing bundles are comprised of a set of user platforms and application licenses that define the phone and application services that you can assign to an individual user. You can assign a UCC license directly to a user from the USP Phones tab. You can also assign UCC licenses using roles and templates.

Roles and templates define the phone and application services, including the licensed functionality, for different types of users. When you apply a role to a user using the Quick Add function, the role references a user template that can assign a UCC license bundle to the user. The system provides a set of default UCC user roles and templates.

Note:
For MiVoice Business platforms, templates are only applied during the creation of new users. If you apply a UCC 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 (see Manage UCC License Bundles).

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.

1.1.3.3.2 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.

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

Licenses included	UCC Licenses		
	Basic	Entry	Standard
MiVoice Business user l icense 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

Licenses included	UCC Licenses		
	Basic	Entry	Standard
Standard and Advanced UM license	No	Yes	Yes
MiCollab Desktop Client with Instant Messaging P resence	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 Prese nce	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 Clientweb lice nse (seeNote 1)	Yes (Basic features only)	Yes (Entry features only)	Yes
MiCollab Client softphone l icense (see Note 1)	No	No	Yes
MiCollab Client Mobile SIP for Softphone	No	No (See **Note 5**)	Yes (See **Note 6**)

Licenses included	UCC Licenses		
	Basic	Entry	Standard
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 as well as manage their Dynamic Status.

1.1.3.3.3 Manage UCC Licensing Bundles (MiVoice Business only)

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. Upgrades from "Basic to Standard" is supported for these platforms from their call manager administrator interface.

This topic covers the following tasks for MiVoice Business platforms only.:

- Assigning UCC Licensing Bundles
- Removing UCC Licensing Bundles
- Upgrading a UCC Licensed User to Next Bundle Level
- Downgrading a UCC Licensed User
- Swapping UCC Licensing Bundles between two users
- Configuring existing MiVoice Business UCC Basic Users on MiCollab
- Range programming MiCollab Client Profiles
- Identifying UCC license usage

Note:
Templates are only applied during the creation of new users. If you apply a UCC 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 UCC Licensing Bundles

You can assign UCC licensing bundles

- directly to an existing user entry from the "UCC Licensing" field in the User tab,
- by applying one of the default UCC licensing templates when you create a new user with Quick Add,
- by adding custom templates that specify a UCC licensing bundle (Basic, Entry, or Standard) and then using Quick Add to apply the template during the creation of new users.

Note:
If all the available UCC license bundles for a specific bundle type (Basic, Entry, or Standard) 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 Basic Bundle

To assign a user, who currently has no bundle, with a Basic bundle:

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 (for Enterprise) and click **Save**.
3. In the **Phones** tab, add a phone with Service Level set to Full.
4. In the **MiCollab Client** tab, set the Feature Profile to "UCC (Vx.0) Basic".

Assign Entry Bundle

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

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 (for 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 **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 "UCC (Vx.0) Entry".

6. Reach through to the MiVoice Business and configure the user in a Multi-device Group of type "Standard".

Assign Standard Bundle

To assign a user, who currently has no license, with a Standard bundle:

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 (for 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 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 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 "UCC (Vx.0) Standard".
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 "Standard".

Removing UCC Licensing Bundles

To remove a UCC licensing bundle from a user, set the UCC 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 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.

Entry to Standard

Basic to Standard

Basic to Entry

Upgrade from Entry 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 (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 Soft phone 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.

1.1.3.4 Define Locations

- Add or Edit Location Information on page 50

1.1.3.4.1 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 **Save**.

To delete a location namge

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

1.1.3.5 Define Departments

- Add, Edit or Delete Department Information on page 51

1.1.3.5.1 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).
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**.

1.1.3.6 Manage Roles and Templates

- About Roles and Templates on page 54
- Default Roles and Templates on page 55
- Guidelines for Using Templates on page 61
- Manage User Templates on page 62

- Enter Template Information on page 66
- Manage Roles on page 101
- Apply Roles on page 102
- Template Migration on page 102

1.1.3.6.1 About Roles and Templates

Overview

Use roles and templates to apply common configuration data across multiple user entries. This approach greatly reduces the amount of time that it takes to enter customer data. Roles define the task, position, or responsibilities for a type of user within the organization. Roles are associated with user templates that define the common phone and application service settings for the roles.

Identify types of users that have common phone and application service needs and then create user templates. Define the required services for the users in each template. Then, assign roles to the templates. You can apply the roles and the associated template data to user entries using any of the following methods:

- **Quick Add**: allows you to create a new user using a role. The assigned role automatically applies the associated template data to the user entry.
- **Bulk User Provisioning**: allows you to import a CSV or LDIF file of user entries and specify user roles for the entries. The roles reference templates that automatically apply common data during the import process. You also have the ability to auto-fill a selection of user entries in the bulk user provisioning tool with roles, directory entries, and e-mail addresses.
- **Provisioning with IDS**: When a directory server is integrated with MiCollab , you can map a directory service attribute to a MiCollab role. When a user is provisioned in the directory service and synchronized with the MiCollab database, the template data that is associated with the specified role is applied to user entry created on MiCollab .

Default roles and templates are provided with the system.

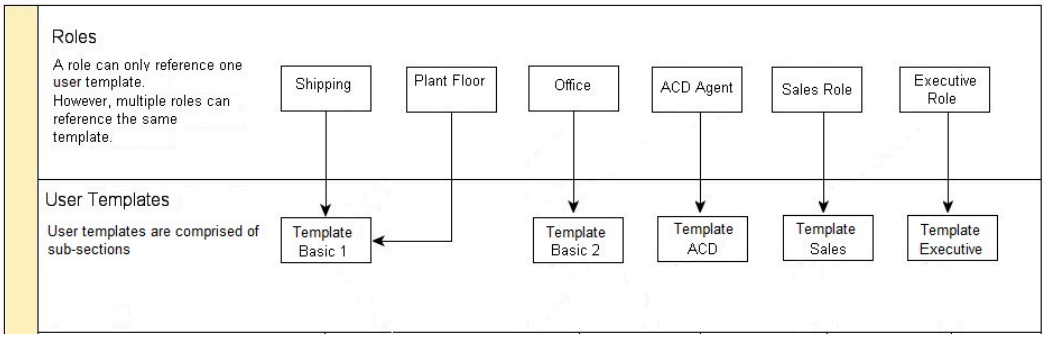
Relationship between Roles and Templates

A *role* can only reference one *user template*. However different roles can reference the same user template. A user template is comprised of sub-sections that define the user information, phone services, and application settings:

- User Template
- User Information
- Primary Phone
- Secondary Phone
- Other Phone

- Speech Auto Attendant
- MiCollab Client
- NuPoint Unified Messenger
- EMEM Voicemail Service
- MiCollab Audio, Web and Video Conferencing
- Vidyo

The following figure illustrates the relationship between roles and templates.



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

Default UCC Users and Services Template (Enterprise)	Template Contents	Functionality provided
	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
	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

Default UCC Users and Services Template (Enterprise)	Template Contents	Functionality provided
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

Default UCC Users and Services Template (Enterprise)	Template Contents	Functionality provided
	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
	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 a nd 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.
Teamwork Mode User ð	MiCollab Client Teamwork Mode User ð	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 ð	HotDesk SIP Softphone Userð	The template contains the user information and applies SIP softphone capability for hot desking users along with Teleworker service.

1.1.3.6.3 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:0
  - 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 userr'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.

1.1.3.6.4 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.

View

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

Add

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**.

Edit

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 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**.

1.1.3.6.5 Enter Template Information

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.

Field	Description	Values
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.
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.

Field	Description	Values
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.

Field	Description	Values
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.)
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.

Field	Description	Values
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

Field	Description	Values
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. • 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. • 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.	Not selected.

Field	Description	Values
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. • 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.	Not selected.

Field	Description	Values
Enable SIP Softphone for MiCollab for PC 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. The **Enable SIP Softphone for MiCollab for PC Client** setting is supported for MiCollab for PC Client only. **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-	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

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 modee.	
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.
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

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.
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.

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. • 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.	Default is unchecked.

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).
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.

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.

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	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
Room Type	Normal: Assign this setting to regul ar users. It allows a user to host p ersonal Vidyo meetings from a de sktop device or mobile device. Vidyo Mobile and VidyoDesktop users can 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 pr iority users. It allows them to conn ect from any VidyoMobile or Vidy oDesktop enabled device without a concurrent use license.	
	Panoramic: Assign this setting to me eting rooms that are equipped with multiple screens (up to nine high-res loution screens are supported).	

1.1.3.6.6 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.

1.1.3.6.7 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.

1.1.3.6.8 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 .

1.1.3.7 Provision Users and Services

1.1.3.7.1 Provisioning Methods

1.1.3.7.1.1 Flow Through Provisioning - Description

Flow Through Provisioning synchronizes updates made to the following data between the MiCollab and MiVoice Business system databases using System Data Synchronization (SDS).

- Network Elements
- Roles and Templates
- Users and Services Hosting
- Phone Services

For MiCollab sites with MiVoice Business servers, Flow Through Provisioning provides the following advantages:

- Allows you to perform user and service provisioning for a network of MiVoice Business servers from the MiCollab User and Services application. Although changes made to user and services data on a MiVoice Business system are distributed to the other

system databases in the network, including MiCollab , the recommended practice is to perform user and service provisioning from MiCollab .

- Provides a Reconcile wizard that synchronizes the user and services data of an existing MiVoice Business to a MiCollab database. After a software upgrade, this wizard also helps you reconcile any conflicting user entries, roles, and templates.
- Allows you to view and manage distribution errors and pending updates. 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.
- Provides single-sign on to the administration interfaces for the Mitel communications network. After you sign into the MiCollab server manager, you are granted Reach Through access to the MiVoice Business system administration tool and vice versa.
- Supports context sensitive Reach Through from the User and Services application to specific MiVoice Business programming forms. You can modify system settings by launching the system administration tool of the MiVoice Business system that hosts the user's phone. For example, you can reach-through to the Class of Service form and modify COS parameters. SDS then shares the COS updates to the other MiVoice Business systems in the network.

Note:
If Flow Through Provisioning is not configured, you can still configure user and phone services on MiCollab . However, you must also log into the MiVoice Business system and manually configure the phone services.

Note:
The Single Point Provisioning (SPP) functionality that was supported in MiCollab Release 6.0 SP2 and earlier is not supported in MiCollab Release 7.0. It used MiXML to apply MiCollab updates to the MiVoice Business systems. SPP has been replaced with Flow Through Provisioning in MiCollab Release 7.0.

Sharing Icon

The following icon is displayed in the Users and Services application interface beside data elements that are being shared via Flow Though Provisioning:

The following images show examples of the sharing icon:

.

1.1.3.7.1.2 About the Bulk User Provisioning Tool

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.

Element	Description	Notes
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.

Element	Description	Notes
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.	
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".

Element	Description	Notes
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.	
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.	

Element	Description	Notes
	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).

1.1.3.7.1.3 Provisioning with IDS

You can integrate the user database of a corporate directory service with the MiCollab database to minimize data entry and administration. The user data on the corporate directory server is synchronized with the MiCollab database using Lightweight Directory Access Protocol (LDAP). If single point provisioning is enabled, then MiCollab distributes the user data to the communication platforms. Synchronization occurs in one direction only—from the directory server to MiCollab .

On the directory server, you can assign an "employeeType" attribute to each user data record. The "employeeType" attribute maps to a "role" in the MiCollab database which corresponds to a MiCollab user template. The template applies additional personal data, application services, and telephony features 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. Refer to Integrated Directory Services for details.

1.1.3.7.1.4 Manual Provisioning

It is recommended that you use Quick Add to provision new users; however, you also can provision users and services directly from the **User** tab without applying role and template. From the **User** tab, you can

- add, edit, or delete users or services
- re-send Service Information E-mails to users
- add Hot Desk Users

If Flow Through Provisioning is enabled, then MiCollab distributes the user data to the MiVoice Business platforms.

To add or edit users or services manually:

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

2. On the **Users** tab, click **Add**, and add a new user

   or locate an existing user using search, select the user, and then click **Edit**.

Note:
You can also double click a user's last name to open the Edit window.

Note:
Add, **Quick Add**, **Edit**, or **Delete** option is not supported if MiCollab is integrated with MiVoice 5000 or MiVoice MX-ONE .

1. Click each of the tabs and modify the fields as required. Mandatory fields are identified with an asterisk (*). You must click **Save** to commit your changes before you switch to a new tab. Users may have configuration information stored on one or more of the following tabs:

   - User
   - Phones
   - MiCollab Speech Auto Attendant
   - Groups
   - NuPoint UM
   - MiCollab Client
   - Audio, Web and Video Conferencing
   - MBG (Teleworker)
   - Vidyo
2. Click **Save**.

1.1.3.7.2 Flow Through Provisioning

- Flow Through Provisioning - Description on page 103
- Flow Through Provisioning - Conditions and Limitations on page 116
- Flow Through Provisioning - Management Capabilities on page 121
- Flow Through Provisioning - Summary of Behaviors on page 122
- Flow Through Provisioning - Configuration on page 123
- Flow Through - Maintenance on page 123

- Flow Through Provisioning - Events and Alarms on page 128
- Reconcile Wizard on page 134
- Reach Through on page 152
- Manage Distribution Errors on page 167

1.1.3.7.2.1 Flow Through Provisioning - Description

Flow Through Provisioning synchronizes updates made to the following data between the MiCollab and MiVoice Business system databases using System Data Synchronization (SDS).

- Network Elements
- Roles and Templates
- Users and Services Hosting
- Phone Services

For MiCollab sites with MiVoice Business servers, Flow Through Provisioning provides the following advantages:

- Allows you to perform user and service provisioning for a network of MiVoice Business servers from the MiCollab User and Services application. Although changes made to user and services data on a MiVoice Business system are distributed to the other system databases in the network, including MiCollab , the recommended practice is to perform user and service provisioning from MiCollab .
- Provides a Reconcile wizard that synchronizes the user and services data of an existing MiVoice Business to a MiCollab database. After a software upgrade, this wizard also helps you reconcile any conflicting user entries, roles, and templates.
- Allows you to view and manage distribution errors and pending updates. 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.
- Provides single-sign on to the administration interfaces for the Mitel communications network. After you sign into the MiCollab server manager, you are granted Reach Through access to the MiVoice Business system administration tool and vice versa.
- Supports context sensitive Reach Through from the User and Services application to specific MiVoice Business programming forms. You can modify system settings by launching the system administration tool of the MiVoice Business system that hosts the user’s phone. For example, you can reach-through to the Class of Service form and modify COS parameters. SDS then shares the COS updates to the other MiVoice Business systems in the network.

Note:
If Flow Through Provisioning is not configured, you can still configure user and phone services on MiCollab . However, you must also log into the MiVoice Business system and manually configure the phone services.

Note:
The Single Point Provisioning (SPP) functionality that was supported in MiCollab Release 6.0 SP2 and earlier is not supported in MiCollab Release 7.0. It used MiXML to apply MiCollab updates to the MiVoice Business systems. SPP has been replaced with Flow Through Provisioning in MiCollab Release 7.0.

Sharing Icon

The following icon is displayed in the Users and Services application interface beside data elements that are being shared via Flow Though Provisioning:

The following images show examples of the sharing icon:

.

1.1.3.7.2.2 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.

1.1.3.7.2.3 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).

1.1.3.7.2.4 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.

1.1.3.7.2.5 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.

1.1.3.7.2.6 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**.

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.

1.1.3.7.2.7 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.

Event or Alarm Description	Severity	Details
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.

Event or Alarm Description	Severity	Details
User Sync Started or Completed f rom a MiVoice Business server	Indeterminate	This event indicates that a MiVoice Business server performed a 'Sync' t o synchronize data with the MiCollab server and that the synchronization is complete.
Device Data Synchronization Star ted or Completed	Indeterminate	This event indicates that the MiColl ab server performed a synchroniz ation of device data with all networ k elements. All of the phone service s hosted by all of the MiVoice Busin ess servers in the administration gr oup will have full service details liste d 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.

Event or Alarm Description	Severity	Details
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.
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.

Event or Alarm Description	Severity	Details
MiTAI Authentication Failed for <MiV B 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 <MiV B IP Address> - Username/Passwor d 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.

Event or Alarm Description	Severity	Details
Update Rejected	Minor	If the MiCollab server rejects an up date 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 i n the distribution error management tools of other network elements.
SDS Sharing could not be started	Minor	If an older MiVoice Business attempt s to start sharing with MiCollab , M iCollab reverts the sharing attempt and displays an event and red ba nner stating that the sharing could not be started.

1.1.3.7.2.8 Reconcile Wizard

1.1.3.7.2.8.1 Reconcile Wizard - Description

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.

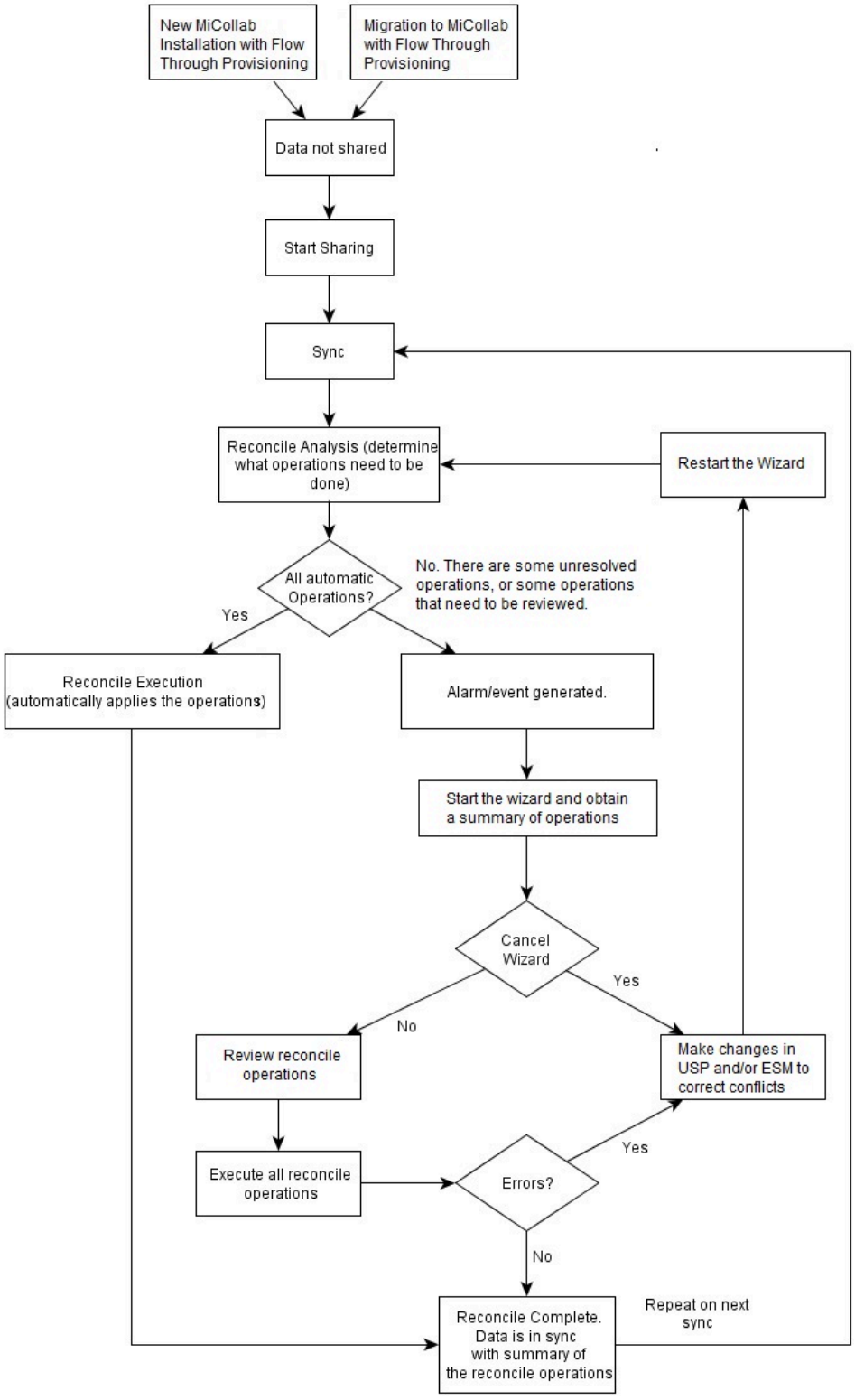
When you configure Flow Through Provisioning, you must add the MiCollab system as a network element to the MiVoice Business Network Element form, click the **Start Sharing** button to share and begin the synchronization process. At the start of the synchronization process, the system automatically runs 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:



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

1.1.3.7.2.8.2 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.

1.1.3.7.2.8.3 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
MiCollaband MiVoice Businessusers 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 Businessusers that are not paired with a MiCollab user are not automatically assigned MiCollab Clientservice.	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.

Status of entries	Reconcile Operation
Matching MiCollaband MiVoice Businessentries 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
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.

Status of entries	Reconcile Operation
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 direc tory number (DN) and the MiVoice Business user has a dditional DNs.	The wizard pairs the MiCollab and MiVoice Business u sers based on the matching DN. The merged user uses the MiCollab user information. The additional MiVoice Bu siness user DNs are also included with the merged user.
MiCollabuser 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 inform ation. 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 di rectory 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. Network elements that need to be reconciled with this n etwork element.	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 MiVo ice Business systems, and then start the Reconcile W izard again.
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 n ot shared across the network.

1.1.3.7.2.8.4 Using the Reconcile Wizard

- Reconcile Wizard - Welcome on page 141
- Reconcile Wizard - Analyze Reconcile Operations on page 142
- Reconcile Wizard - Non-Sharing Network Elements on page 143

- Reconcile Wizard - Sharing Network Elements on page 144
- Reconcile Wizard - MiCollab Phones to be Reviewed on page 145
- Reconcile Wizard - Execute Reconcile on page 146

1.1.3.7.2.8.4.1 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 wizard to sync hronize the databases and config ure Flow Through Provisioning. T he MiCollab USP database will not begin sharing data with the MiVoice Business databases 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 Summary report of the failed, unresolved, and successful opera tions.	
Backups	Make backups of MiCollab and MiVoice Business system databases before running this wizard. 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.

Warning:
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.

1.1.3.7.2.8.4.2 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

Field	Description
Operations Count	Number of operations identified (automatic operations, operations for review, and unresolved operations). Operation details are provided in a summary at the end of the wizard.
Progress Bar	Provides visual indication of the analysis process.

1.1.3.7.2.8.4.3 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.

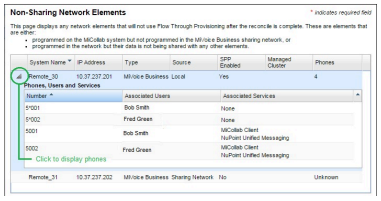
Note:
This page only appears if there are non-sharing network elements.

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

Parameter	Description
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. Th erefore, it is most likely that this element should be a dded 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 ena bled.
Managed Cluster	Name of the managed cluster
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 S ingle Point Provisioning, you are required to confirm that these elements do not need to share data with any oth er network elements after the reconcile operation is com plete. You must check the I wish to proceed box to enabl e the Next button.

1.1.3.7.2.8.4.4 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 MiVoice Business
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

1.1.3.7.2.8.4.5 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
Associated Services	Services (applications) assign to the phone

1.1.3.7.2.8.4.6 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.

1.1.3.7.2.8.5 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 MiCollabUser 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	MiCollabDepartment 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.
MiCollabusers 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.

Failed or Unresolved Operations	Description	Corrective Action
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.
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).

Failed or Unresolved Operations	Description	Corrective Action
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.
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.

1.1.3.7.2.8.6 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**.

1.1.3.7.2.8.7 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.

1.1.3.7.2.9 Reach Through

- Reach Through - Description on page 152
- Reach Through - Conditions on page 158
- Reach Through - Configuration on page 158
- Using Reach Through on page 166

1.1.3.7.2.9.1 Reach Through - Description

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
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

MiCollab User and Services Application page	MiVoice Business (MiVB) System Administration Tool form
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

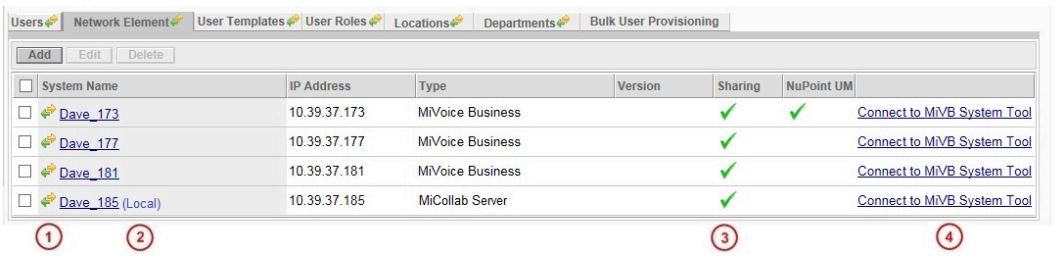


Figure 2: Edit User Page

Figure 3: Phone Details

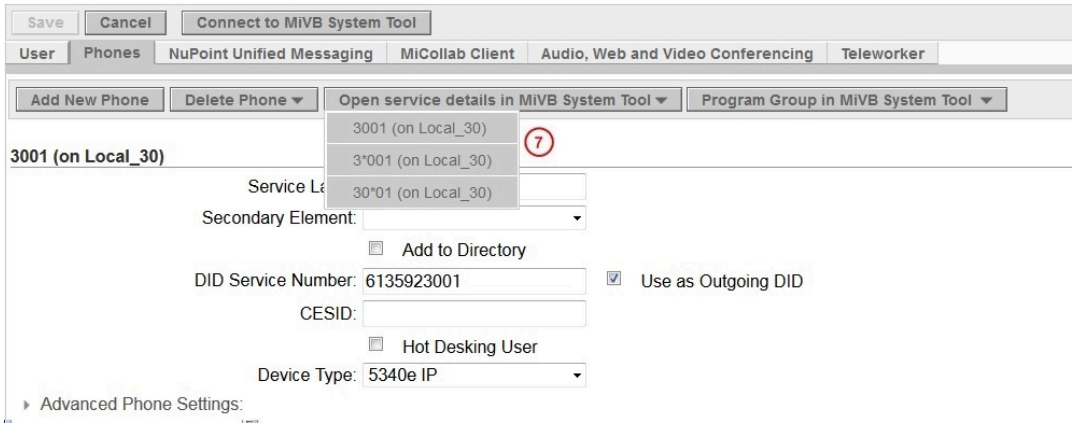


Figure 4: Group Details

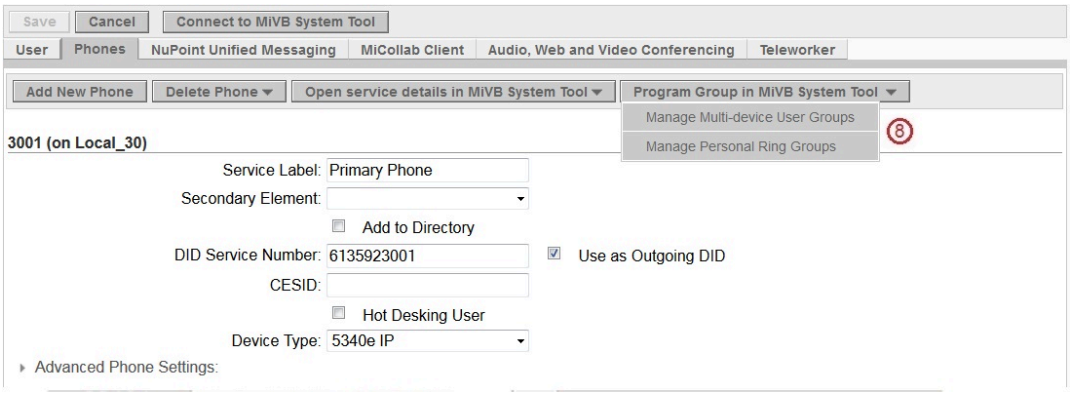


Table 1: Reach Through Support

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.

Item	USP Page	Description
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.

1.1.3.7.2.9.2 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 Internet Explorer (version 9.0 or later) or Mozilla Firefox (version 33 or later) 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 MiCollabto MiVoice Business , reach through will be blocked. Note that Internet Explorer is not supported in Compatibility Mode.
- 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 just add the subnet to the trusted network (that is, 10.46.26.1).

1.1.3.7.2.9.3 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".

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.

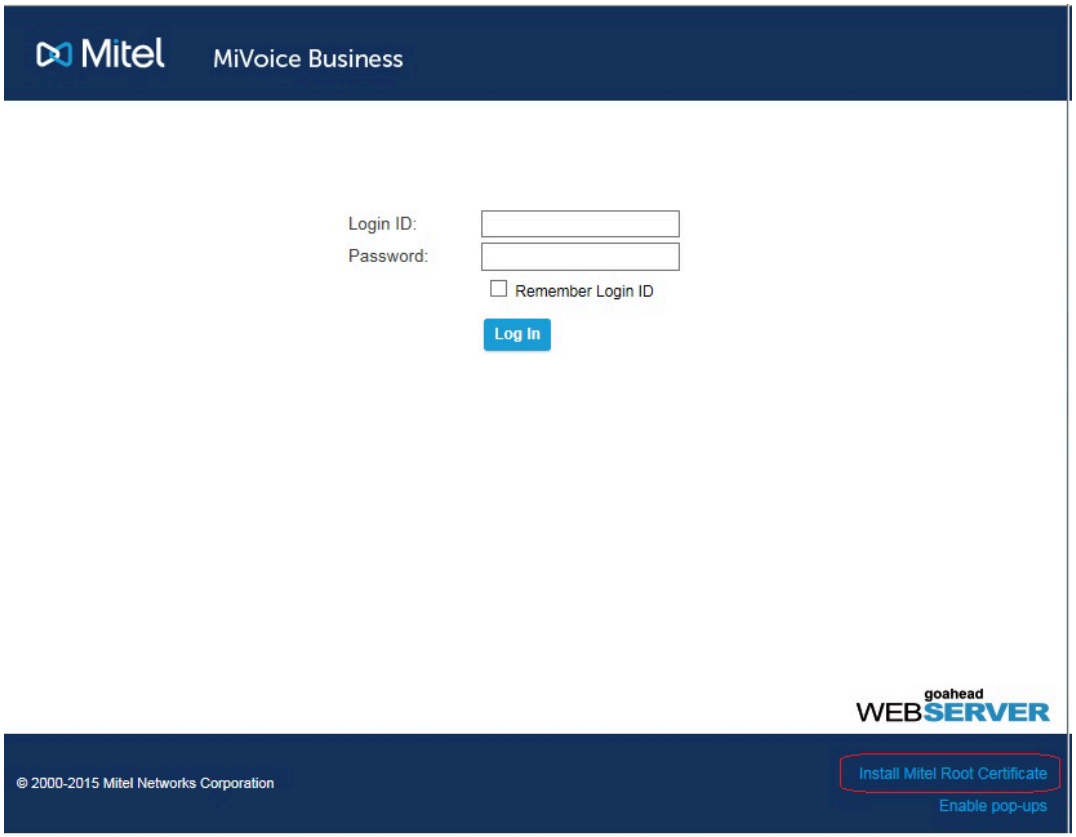
1. Launch the browser.
2. Navigate to the IP address of the MiVoice Business server.
3. Log into the System Adminstration Tool.
4. Navigate to Voice Network ⇒ Admin Groups
5. Click **Change**.
6. Select the admin group name.
7. Click **Save**.
8. Navigate to System Properties ⇒ System Administration ⇒ 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 Internet Explorer or 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 Internet Explorer or 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. The certificate is the same one for both Internet Explorer and Firefox.

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 Internet Explorer:

1. Launch Internet Explorer.
2. Select **Tools** and then click **Internet Options**.
3. Click the Content tab and then click the **Certificates** button.
4. Select **Trusted Root Certification Authorities** and click **Import**. The Certificate Import Wizard opens.
5. Click **Next**.
6. Click **Browse**.
7. Browse to the downloaded mitelcert.cer file and click **OK**.
8. Click **Next**.
9. Select **Place all Certificates** in the following store.
10. Click **Browse**.
11. Select **Trusted Root Certification Authorities**.
12. Click **OK**.
13. Click **Next**.
14. Click **Finished**.
15. Click **Yes**. An Import was successful dialog appears.

16. Click **OK**.

After the certificate is installed, exit Internet Explorer, 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.

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**.
12. 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.

Internet Explorer

1. Launch Internet Explorer.
2. Select **Tools** and then click **Internet Options**.
3. Click the **Security** tab.
4. Select the 'Local intranet' zone.
5. Click **Sites**.
6. Click **Advanced**.
7. Add the IP addresses for MiVoice Business servers to add them to the zone. Use *https://<IP address>*.
8. Click **Close**.
9. Click **OK**.
10. Click the **Privacy** tab.
11. Clear the **Turn on Pop-up Blocker** check box or add the IP addresses for the MiVoice Business servers to the list of websites to allow (under 'Settings').
12. Click **OK** to close the Internet Options dialog.

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

Internet Explorer

1. Launch Internet Explorer.
2. Select **Tools** and then click **Internet Options**.
3. Click the **Content** tab and then click **Certificates**.
4. Select **Trusted Root Certification Authorities** and click **Import**. The Certificate Import Wizard opens.
5. Click **Next**.
6. Click **Browse**.
7. Browse to the extracted certificate (.crt) file and click **OK**.
8. Click **Next**.
9. Select **Place all Certificates in the following store**.
10. Click **Browse**.
11. Select **Trusted Root Certification Authorities**.
12. Click **Ok**.

13. Click **Next**.
14. Click **Finished**.
15. Click **Yes**. An Import was successful dialog appears.
16. Click **Ok**.

After the certificate is installed, exit Internet Explorer, and then restart it. You can now log in to MiCollab and not receive the security certificate warnings.

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

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**.
8. 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.

1.1.3.7.2.9.4 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.

1.1.3.7.2.10 Manage Distribution Errors

- About SDS Distribution Errors on page 167
- Resolving Distribution Errors on page 169
- Exporting Error Data on page 172
- Viewing Data Distribution Alarms on page 172

1.1.3.7.2.10.1 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.
Action ID	A unique number sequence that identifies the transac tion 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 upd ate retry.
Action	Specifies the configuration action type (for example: ad d, modify, or delete).
MiVB Form Name	Identifies the name of the MiVoice Business form from which the data distribution originated.

Parameter	Description
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.
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 E rror screen displays the total number of error listed.

1.1.3.7.2.10.2 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.

1.1.3.7.2.10.3 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).

1.1.3.7.2.10.4 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

1.1.3.7.3 Bulk User Provisioning

- About the Bulk User Provisioning Tool on page 105
- Bulk Import from File on page 181
- Auto Fill Selection on page 189
- Add User Entries on page 192
- Correcting Errors on page 193
- Importing contacts using Bulk User Provisioning on page 194

1.1.3.7.3.1 About the Bulk User Provisioning Tool

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.

Element	Description	Notes
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.
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

Element	Description	Notes
	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**.

Element	Description	Notes
Timestamp (Managed Detained Mode only)	Shows the date and time of when the entry entered the detained queue.	
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".

Element	Description	Notes
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.	
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.	

Element	Description	Notes
	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).

1.1.3.7.3.2 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.

Column Header	Mandatory or Optional	Format	Notes
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.
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.

Column Header	Mandatory or Optional	Format	Notes
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.

Column Header	Mandatory or Optional	Format	Notes
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	
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.

1.1.3.7.3.3 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.

1.1.3.7.3.4 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.

1.1.3.7.3.5 Correcting Errors

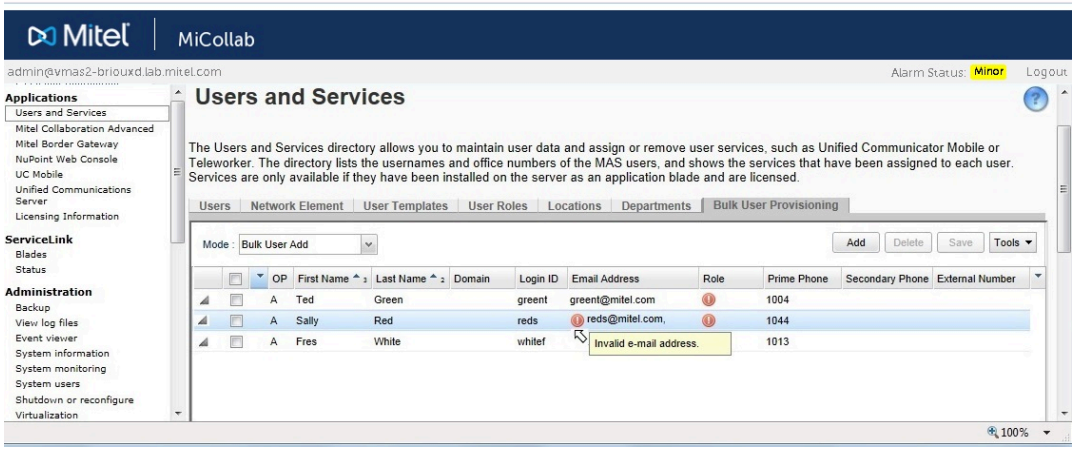
If errors occur during a bulk data import, they are listed in the Bulk Provisioning Tool screen and indicated by icons:

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

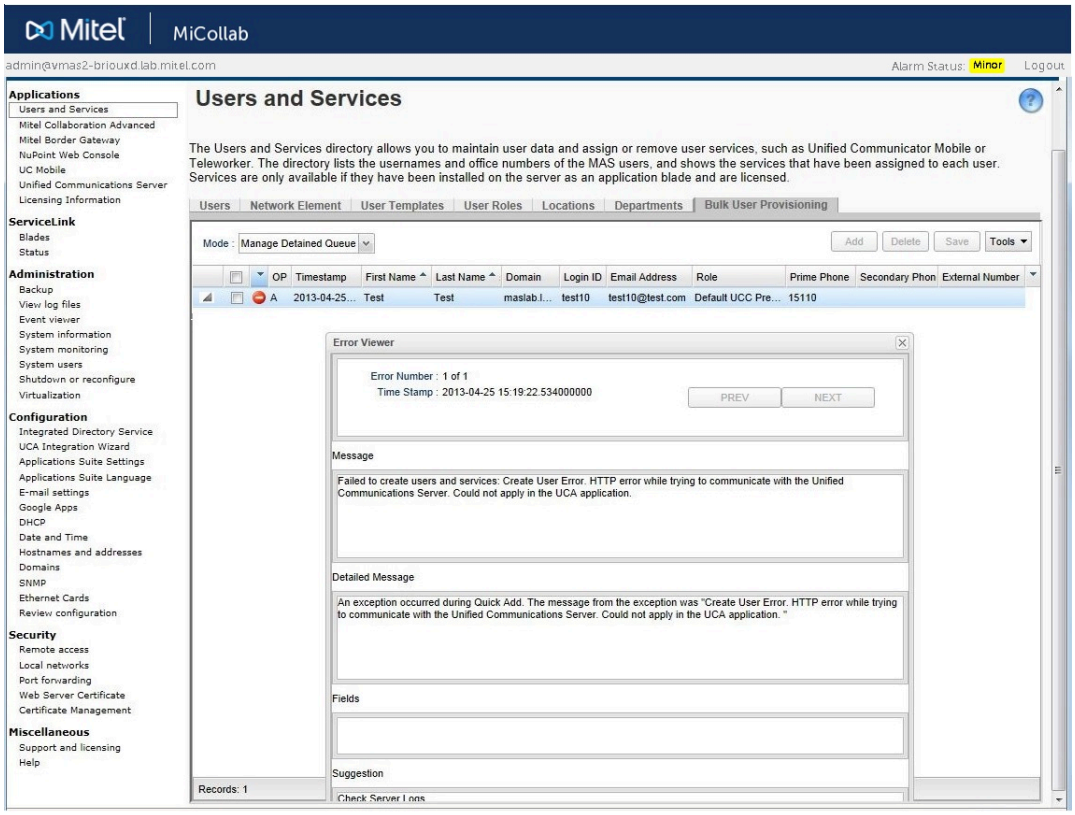
indicates a data import failure. To display the error, click the icon for details. The error report provides the corrective action. If multiple errors exist against the update, click **Next**.

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



1.1.3.7.3.6 Importing contacts using Bulk User Provisioning

You can use Bulk User Provisioning to import contacts via the following methods:

- Active Directory
- CSV file
- Manually added using the **Add** button

Note:
When a contact is created through BUP (using Manual Add), the Primary Phone, DID Number, External Number, and SIP Password fields are disabled, and the user cannot interact with these fields.

Conditions:

- The contacts imported via BUP are read-only for the users, that is, the contacts cannot be edited or deleted. Only the administrator can recreate the deleted contacts via BUP (Manual Add, CSV Import) and AD IDS Connection

- The contacts cannot be converted to a user.

1.1.3.7.4 User Information

- View User Directory on page 1
- Enter User Information on page 198
- Quick Add on page 211
- Delete Users on page 212
- Send Service E-mail on page 213
- Send CloudLink Welcome Email on page 213

1.1.3.7.4.1 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	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.
First Name	

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 **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.

1.1.3.7.4.2 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 " Firstname" of the " Lastname, Firstname" entry in the Name field of the MiVoice Business Telephone Directory Assignment form.

Field	Description	Values
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 " Lastname" of the " Lastname, Firstname" entry in the Name field of the MiVoice Business Telephone Directory Assignment form.
Display Name	Displays the " Lastname, Firstname" for 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	Select the UCC License 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.	Select one of the following: ********** • None ********** ********** • Default UCC Basic User for Enterprise • Default UCC Entry User for Enterprise • Default UCC Standard User for Enterprise • Default UCC Premium User for Enterprise ********** ********** Default is None.
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: • Change the email in the USP to the one set in MiCollab Client Service. It will change the email in USP. • Again change the email in USP to the original email. It will change the email in both USP and MiCollab Client Service.	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
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	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	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 \ & * + / = ? { } | < > ( ) ; : , [ ] " ‘ • 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. The UPN specifications are as follows: • The userPrincipalName (UPN) attribute must be in the internet-style sign-in format where the user name followed by the @ symbol and

Field	Description	Values
		• 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!).

Field	Description	Values
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. **Note**: For 5505 SIP phone, the

Field	Description	Values
Confirm Passcode	Re-enter the passcode to confirm (not necessary if generated randomly).	

1.1.3.7.4.3 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.
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**.

1.1.3.7.4.4 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 .

1.1.3.7.4.5 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**.

1.1.3.7.4.6 Send CloudLink Welcome Email

In certain cases where the user misses the CloudLink Welcome Email, the administrator can resend the welcome email to the users from the MiCollab USP using the option **Send CL Welcome Email**.

1.1.3.7.5 Services

- Enter Phone Information on page 214
- Enter Speech Auto Attendant Information on page 239
- Configure Groups on page 241
- Enter NuPoint UM Information on page 247
- Enter MiCollab Client Information on page 254

1.1.3.7.5.1 Enter Phone Information

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.

Field	Description	Values
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

Field	Description	Values
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. • 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. • 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.	Not checked.

Field	Description	Values
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. • 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.	Not checked.

Field	Description	Values
Enable SIP Softphone for MiCollab for PC 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. The **Enable SIP Softphone for MiCollab for PC Client** setting is supported for MiCollab for PC Client only. **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,

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.

Field	Description	Values
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-	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.	
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 #.

1.1.3.7.5.2 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.

1.1.3.7.5.3 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		

Field	Description	Default Values
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

Field	Description	Default Values
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

Field	Description	Default Values
	Click to delete a phone from the group. You can only delete non-prime phones.	Not applicable

1.1.3.7.5.4 Enter NuPoint UM Information

The **NuPoint Unified Messa ging** 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.	

Field	Description	Values
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.
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.

Field	Description	Values
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.
Message Waiting #1	Select the type of message waiting notification from the list.	Default is None.
Message Waiting #2		

Field	Description	Values
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.

Field	Description	Values
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 through the NuPoint UM web console. 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 UM Web Console*, or the user can define them through their *MiCollab End*	Default is unchecked. **Note**: The following configuration conditions apply: • The NuPoint UM Feature COS assigned to the mailbox must have the Standard UM feature enabled. • A Standard UM license is required for each mailbox that requires Standard 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, 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 .

Field	Description	Values
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. 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 UM 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 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*	Default is unchecked. **Note**: The following configuration conditions apply: • The NuPoint 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. Note that before you can clear the box, you must first delete the Unified Messaging email addresses from the user's mailbox: 1. Under **Applications**, click **NuPoint Web Console**. 2. Click **Mailboxes**

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.

1.1.3.7.5.5 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 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

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 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.

1.1.3.7.5.6 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.

1.1.3.7.5.7 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.

Field	Description	Values
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.

1.1.3.7.5.8 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

Field	Description	Default
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
	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.	

Field	Description	Default
	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).	

1.1.3.7.5.9 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.

1.1.3.7.5.10 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.

1.1.3.7.5.11 MiTeam Classic

1.1.3.7.5.11.1 About 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.

1.1.3.7.5.11.2 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.

1.1.3.7.5.11.3 MiTeam Classic Configuration

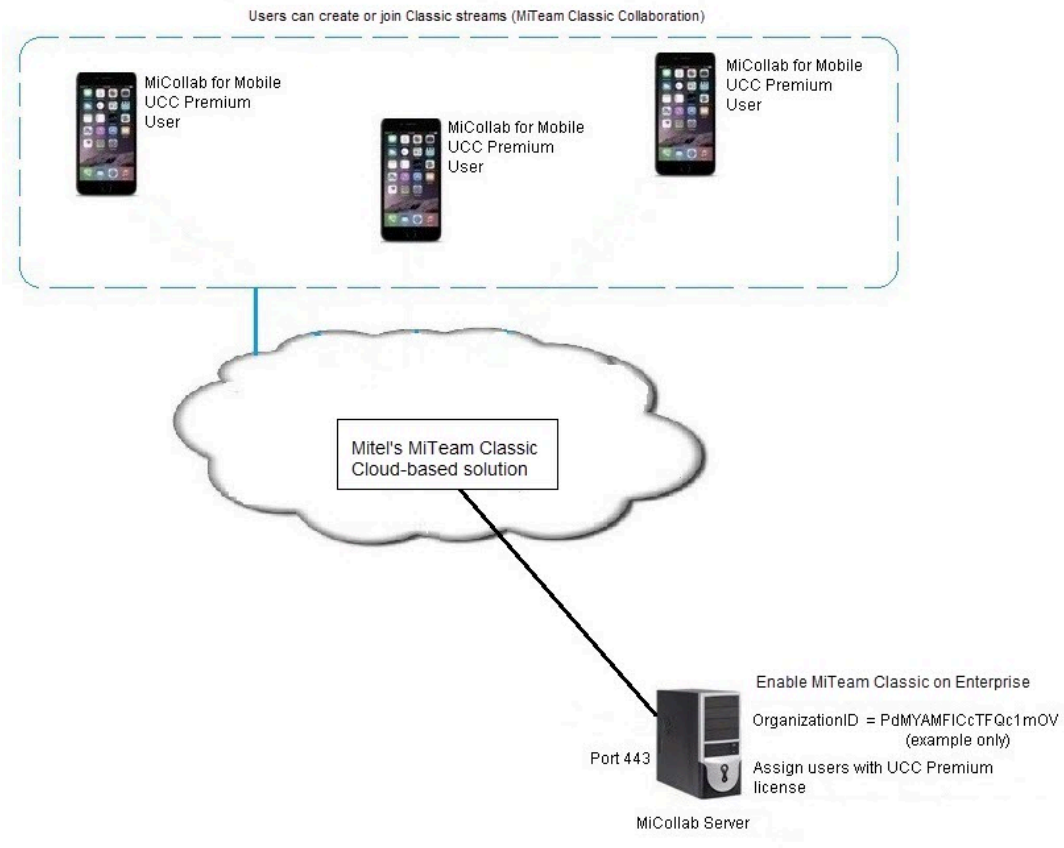
MiTeam Classic is supported in the following deployments

- 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:

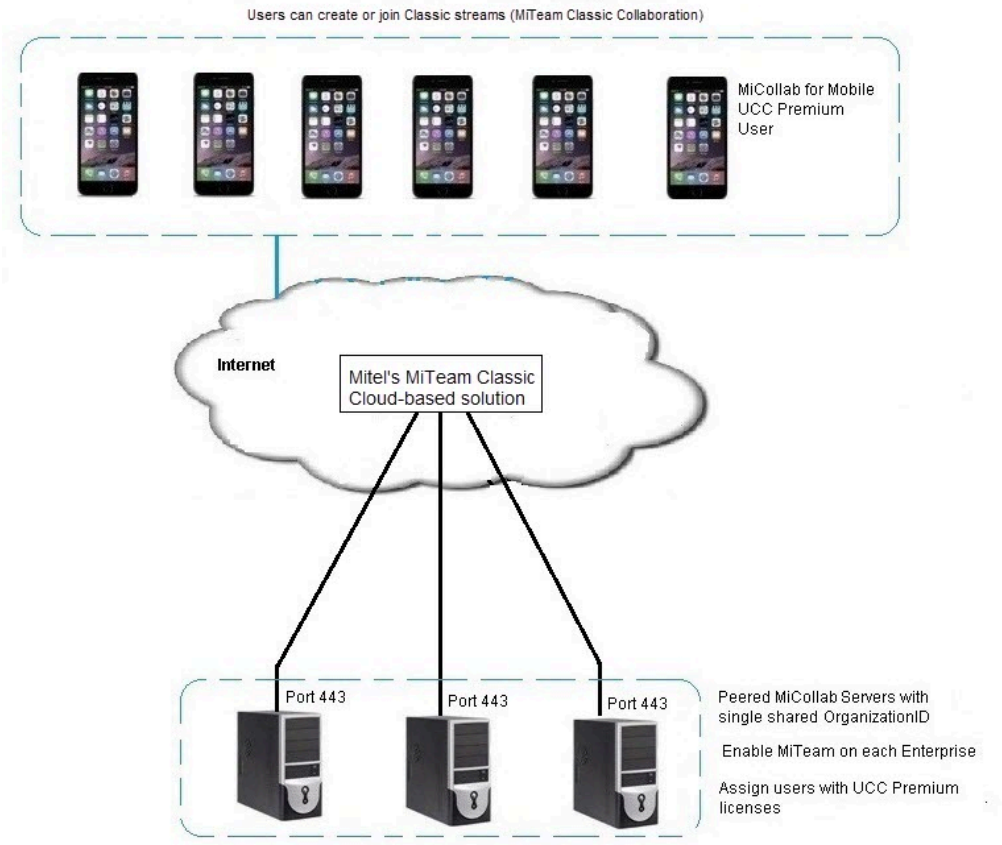
- assign MiVoice Business users with license bundles that provide UCC Premium licenses
- assign MiVoice 5000, MiVoice MX-ONE, or MiVoice 400 users with Roles that provide UCC Premium licenses.

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.

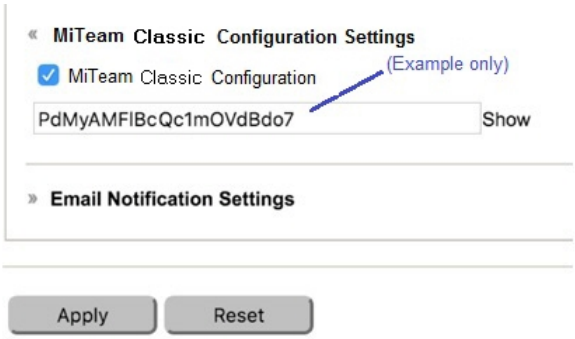
Resolving Conflicting OrganizationIDs

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.

1.1.3.7.5.11.4 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.

1.1.3.7.5.12 MiTeam Meetings

- About MiTeam Meetings on page 281
- Provision MiTeam Meetings on page 282

1.1.3.7.5.12.1 About 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.

1.1.3.7.5.12.2 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.

1.1.3.7.5.13 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**.

1.1.3.7.5.14 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.

1.1.3.7.5.15 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.

When you delete this service in MiCollab :	You also change these settings in the MiVoice Business :
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

1.1.3.7.5.16 Reports

- Generate User Summary or MiTeam Classic Status Report on page 293
- Generate Report of MiCollab Client Accounts on page 295

1.1.3.7.5.16.1 Generate User Summary or MiTeam Classic Status Report

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.

1.1.3.7.5.16.2 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

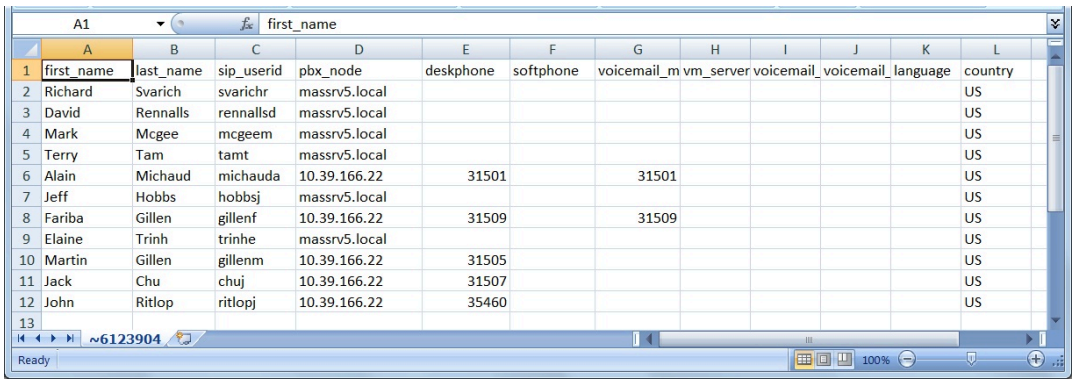
To generate this report:

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.



	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												

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
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

1.1.3.7.6 Deployment

- Deploy Mobile Client for Mobile on page 297
- Deploy Mobile Client for EHDU on page 298
- Deploy MiCollab MAC or PC Client (without Softphone) on page 299

1.1.3.7.6.1 Deploy Mobile Client for Mobile

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.

1.1.3.7.6.2 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.

1.1.3.7.6.3 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.

1.1.3.7.7 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.

1.1.3.8 Troubleshoot

- Correcting Errors on page 193
- Managing Detained and Failed IDS Operations on page 305
- Unable to Delete a User's Extension on page 307
- Unable to Add Phone After Deletion on page 307
- Pop-up Error in Chrome on page 307

1.1.3.8.1 Correcting Errors

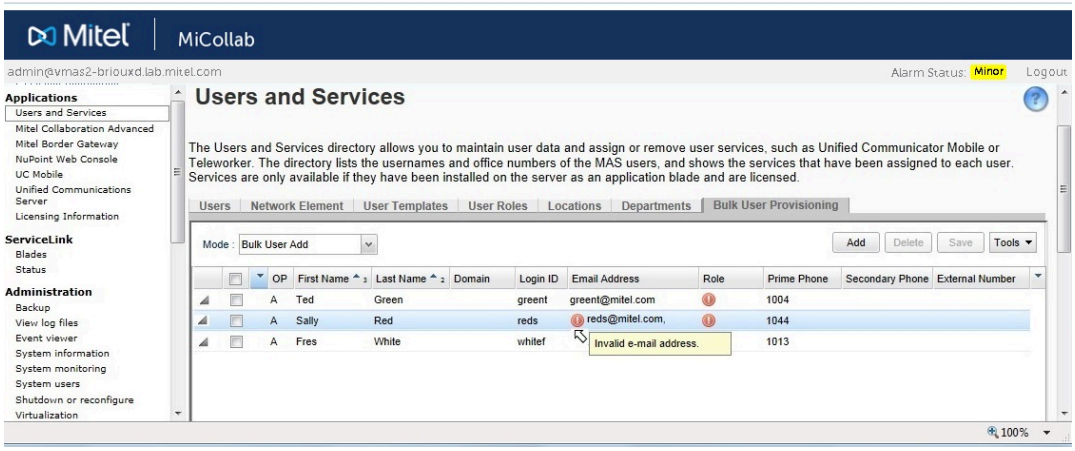
If errors occur during a bulk data import, they are listed in the Bulk Provisioning Tool screen and indicated by icons:

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

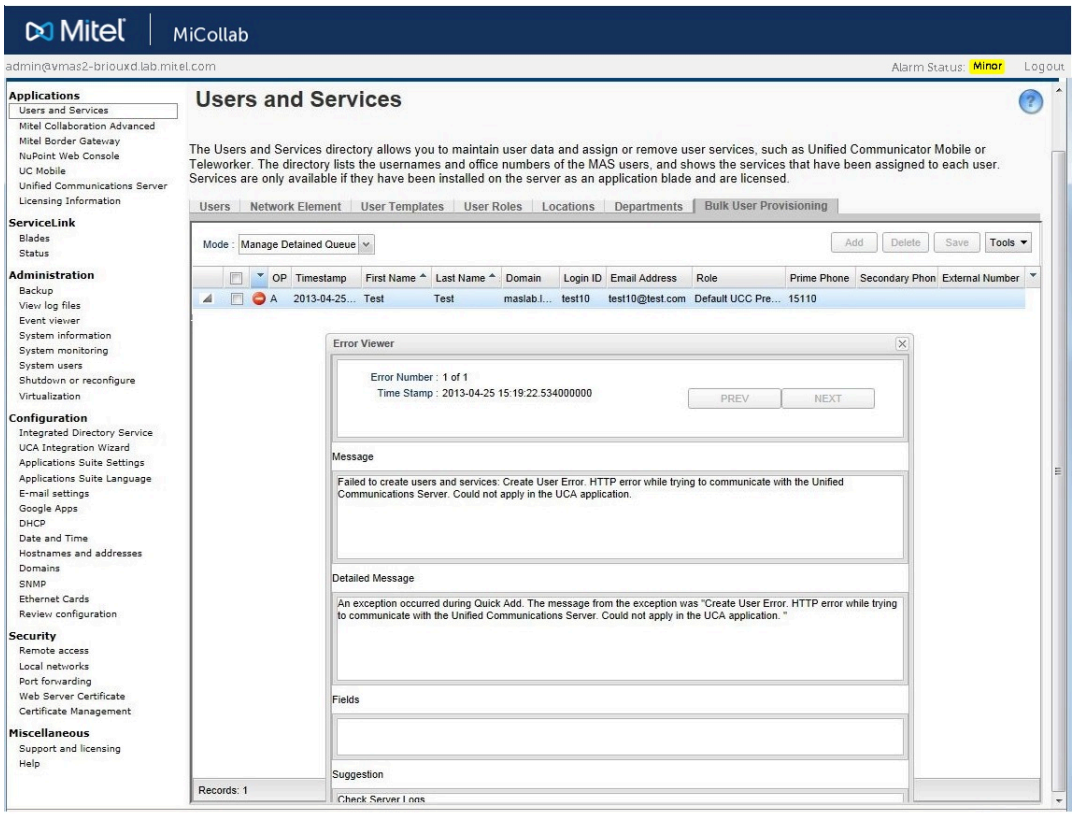
indicates a data import failure. To display the error, click the icon for details. The error report provides the corrective action. If multiple errors exist against the update, click **Next**.

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



1.1.3.8.2 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.

1.1.3.8.3 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.

1.1.3.8.4 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).

1.1.3.8.5 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.

1.2 View Licensing Information

The MiCollab administrator portal opens at the **Licensing Information** page, which displays details about user licensing for your applications.

Unified Communications and Collaboration (UCC) Bundles

This table lists the installed UCC Licensing bundles.

Column	Description
Bundle	Lists the type of UCC licensed bundle; for example, UCC Entry Level for Enterprise (V4.).Note that you can generate a report that identifies the UCC licensing bundl e assigned to each user.
User Licenses	Displays the maximum number of licensed bundles that you can assign.
Currently used	Displays the number of UCC bundles that you have ass igned or attempted to assign. When this total is greater than the number of Licenses, it is displayed in red to indi cate over provisioning. If required, you can purchase ex tra license bundles from your Authorized Reseller.

Note:
This table just shows the tally of the of the available licenses. To determine the licensing part numbers that are being used use to achieve the current level of licensing, you must access the Application Management Center and view the licenses that are assigned to the ULM.

Application User Totals

This table lists the installed applications and the user licensing information for each application. The totals in this table include the user licenses in the available UCC License Bundles plus any "al la carte" licenses that you may have purchased.

Column	Description
Application	Lists the installed applications.
User Licenses	Displays the maximum number of licensed users that y ou can assign to each application or service.
Currently Used	Displays the number of licenses that you have assigned or attempted to assign. When this total is greater than the User Licenses, it is displayed in red to indicate over provisioning (also see Voice Mailbox Over Provisioning). If required, you can purchase extra licenses or uplifts from your Authorized Reseller. **Note**: SIP phones appear in the Teleworker license count regardless of whether they are registered to the ICP.

Effect of Adding or Removing UCC Licenses

When you add or remove a UCC Licensing bundle, the system updates the UCC Licensing totals. The Application User Totals are also updated to reflect the change.

If you add/delete . . .	The following application user licenses (in use) increase/decrease by one . . .
UCC Basic License	• UCC Basic (includes MiVoice Business user license)
UCC Entry License	• UCC Entry • Multi-device user license • NuPoint UM mailbox, Standard UM, and Advanced UM • MiTeam Meetings license

If you add/delete . . .	The following application user licenses (in use) increase/decrease by one . . .
UCC Standard License	• UCC Standard • Multi-device user license • NuPoint UM mailbox, Standard UM, and Advanced UM license • One Teleworker license • MiCollab Client deskphone, web client, and softphone or mobile client • Vidyo client license • MiCollab Audio, Web and Video Conferencing license • MiTeam Meetings license
Premium UCC License	• UCC Premium • Multi-device user license • NuPoint UM mailbox, Standard UM, and Advanced UM license • MiCollab Audio, Web and Video Conferencing license • Three Teleworker licenses • MiCollab Client deskphone, web client, softphone, and mobile client • Vidyo client license • MiTeam Classic license • MiTeam Meetings license
NuPoint UM mailbox (when "al la carte" NuPoint licenses are available)	• NuPoint UM mailbox
NuPoint UM mailbox (when "al la carte" NuPoint licenses are not available but UCC license bundles are)	• UCC Entry (or Standard, or Premium depending on availability) • NuPoint mailbox

Voice Mailbox Over Provisioning

You are allowed to restore a database to a destination system even though the database may contain more voice mailboxes that the system licensing can support. Over provisioning of voice mailboxes is allowed in order to give you time to purchase additional licenses. If the system is in an over provisioned state:

- A warning message appears in the Users and Services application that indicates that you need to purchase additional NuPoint UM user licenses.
- You cannot add new voice mailboxes if the current mailbox count has reached the system NuPoint UM user licensed limit or if the system is in an over provisioned state. You will also be unable to add mailboxes from the NuPoint UM telephone user interface.
- You cannot log into the NuPoint UM web console.
- You cannot log into the MiCollab Audio, Web and Video Conferencing administration application.
- You can log into the NuPoint UM Telephone User Interface (TUI), but you will be unable to access the administrative options.

To return the NuPoint UM application to its normal state, purchase additional licenses or delete the extra mailboxes. You must reduce the number of mailboxes to be equal to, or lower than, the number of available licenses.

Configuration 2

This chapter contains the following sections:

2.1 Integrated Directory Services

2.1.1 Description

2.1.1.1 About Integrated Directory Services

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 .

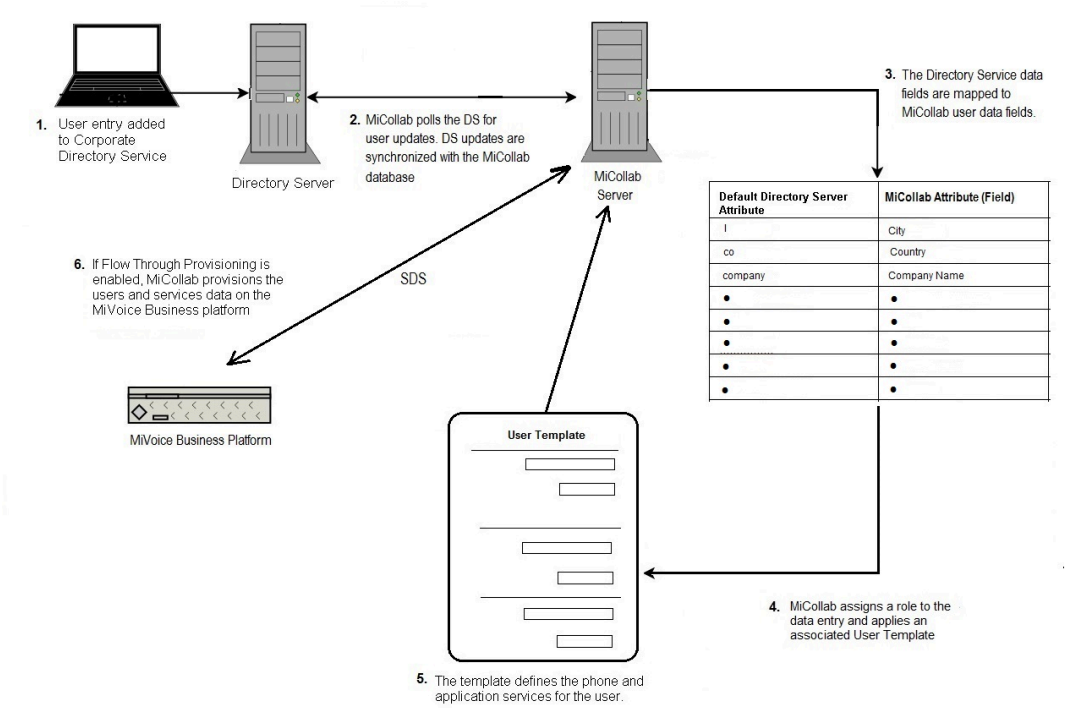


Figure 1: Directory Service Data Synchronization with MiCollab

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

You can configure the integrations described above with Active Directory 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). See Configure Active Directory Authentication for details.

2.1.1.2 Supported IDS Configurations

IDS is supported for the following configurations:

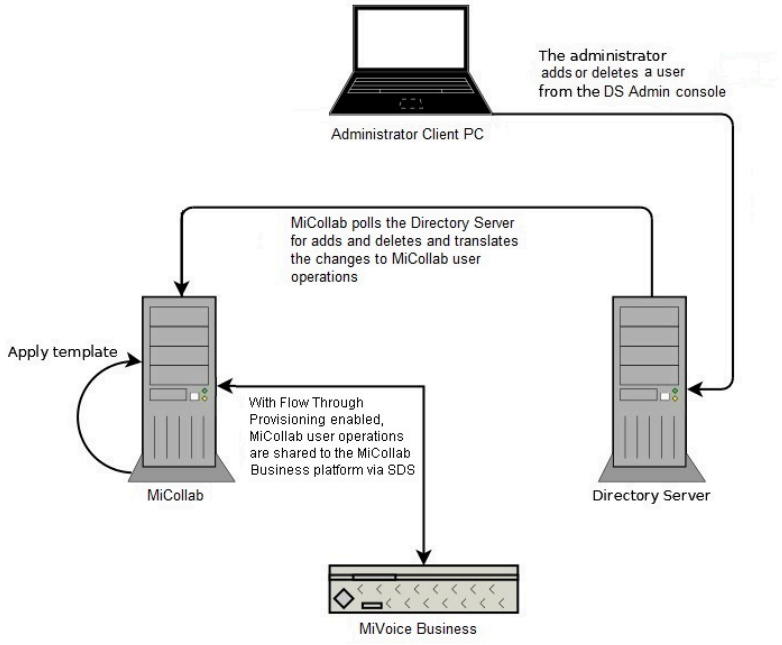
- MiCollab and MiVoice Business (s) with Flow Through Provisioning
- MiCollab and MiVoice Business (s) without Flow Through Provisioning
- MiCollab and MiVoice Office 250 or Non-Mitel PBX
- Multiple MiCollab Servers and a single MiVoice Business
- Single MiCollab Server and a single MiVoice 5000
- Single 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.



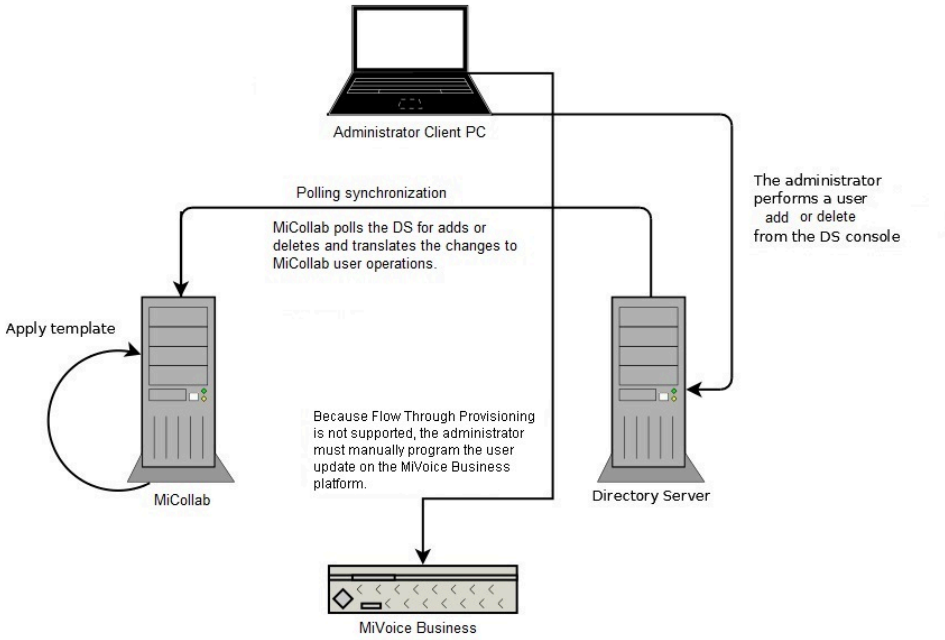
MiCollab and MiVoice Business (s) with Flow Through Provisioning

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.

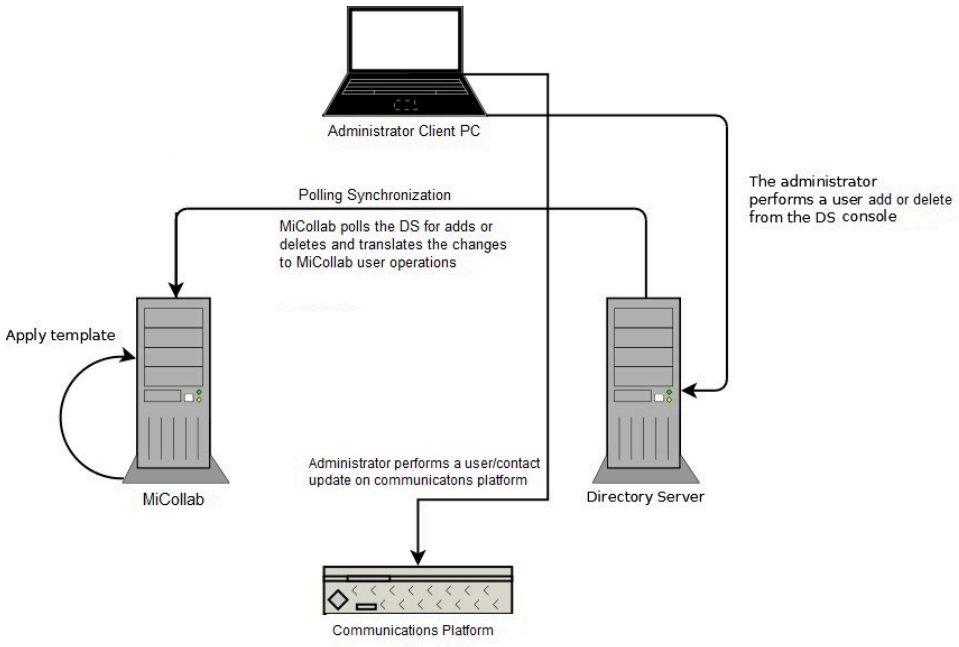


MiCollab and MiVoice Business (s) without Single Point Provisioning

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.



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.

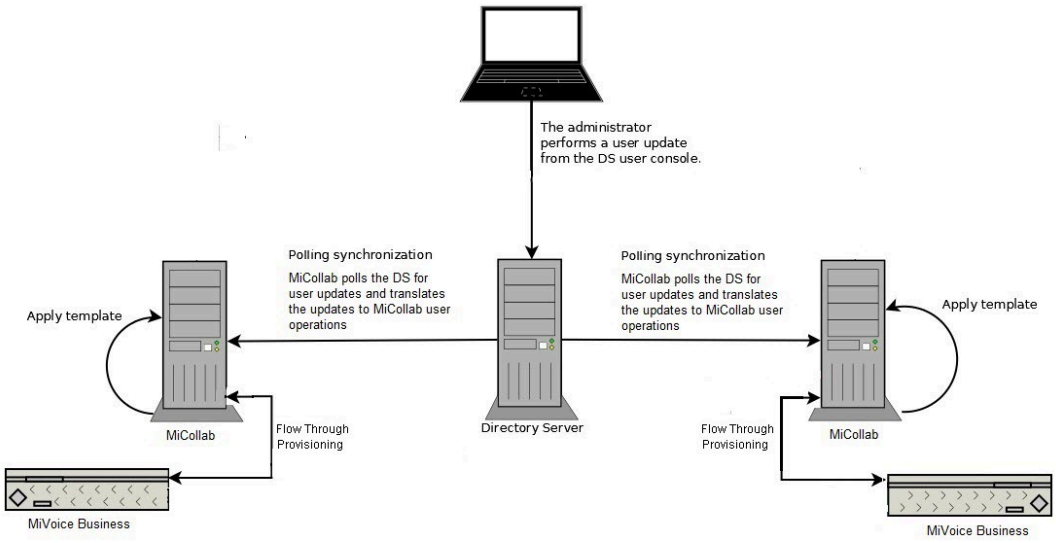


Figure 4: Multiple MiCollab Servers and Multiple MiVoice Businesses

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.

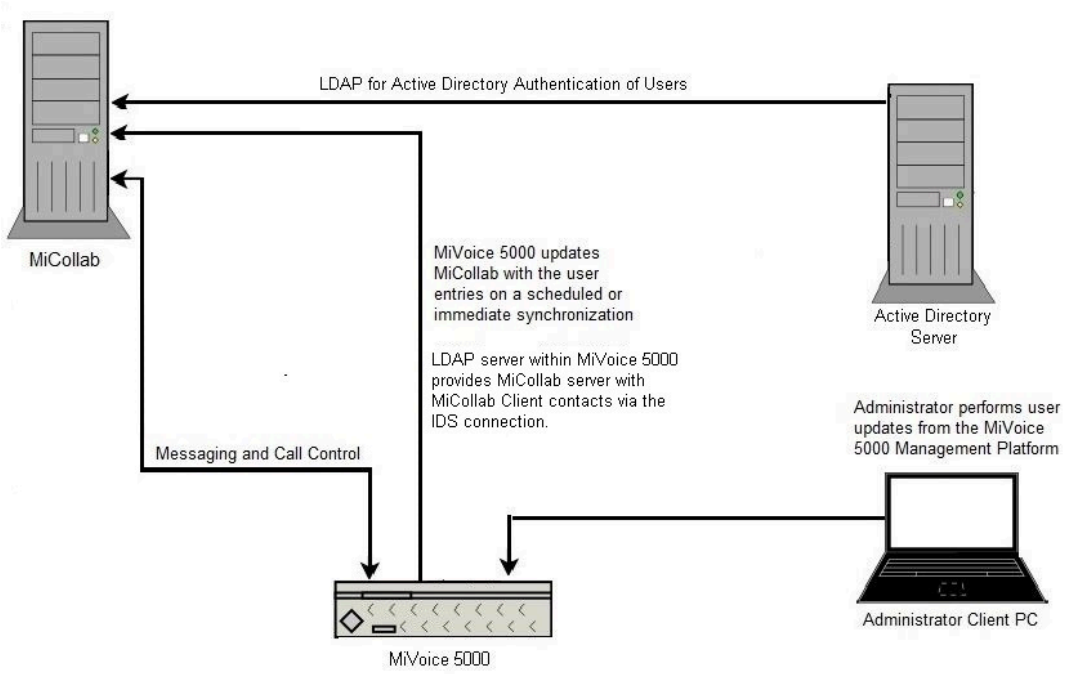


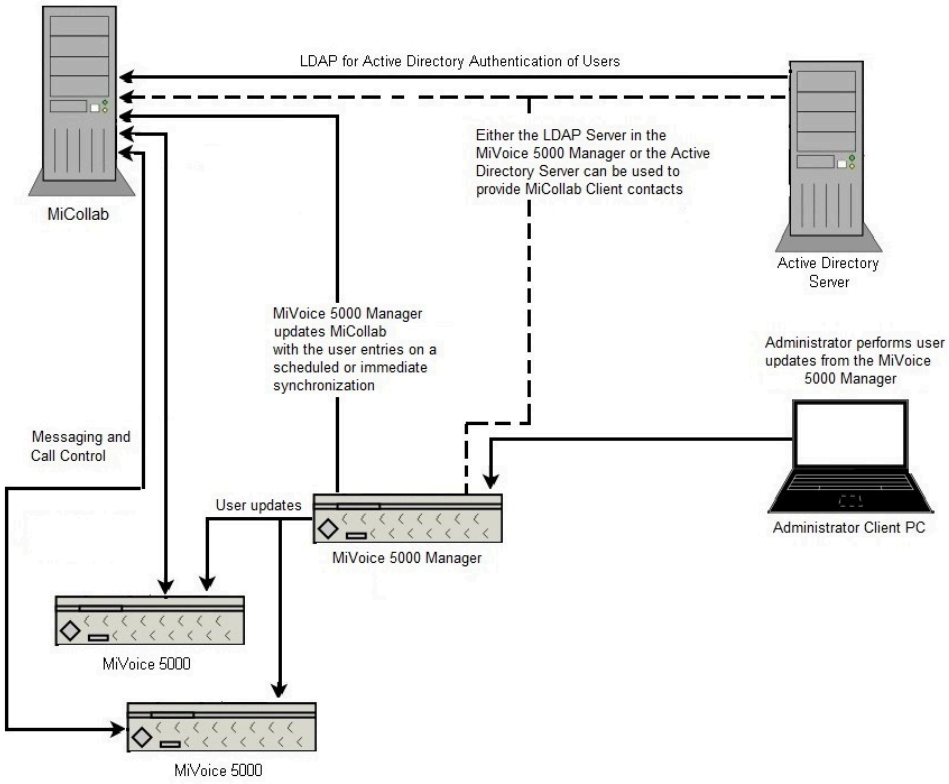
Figure 5: Single MiCollab Server and a Single MiVoice 5000

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.



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.

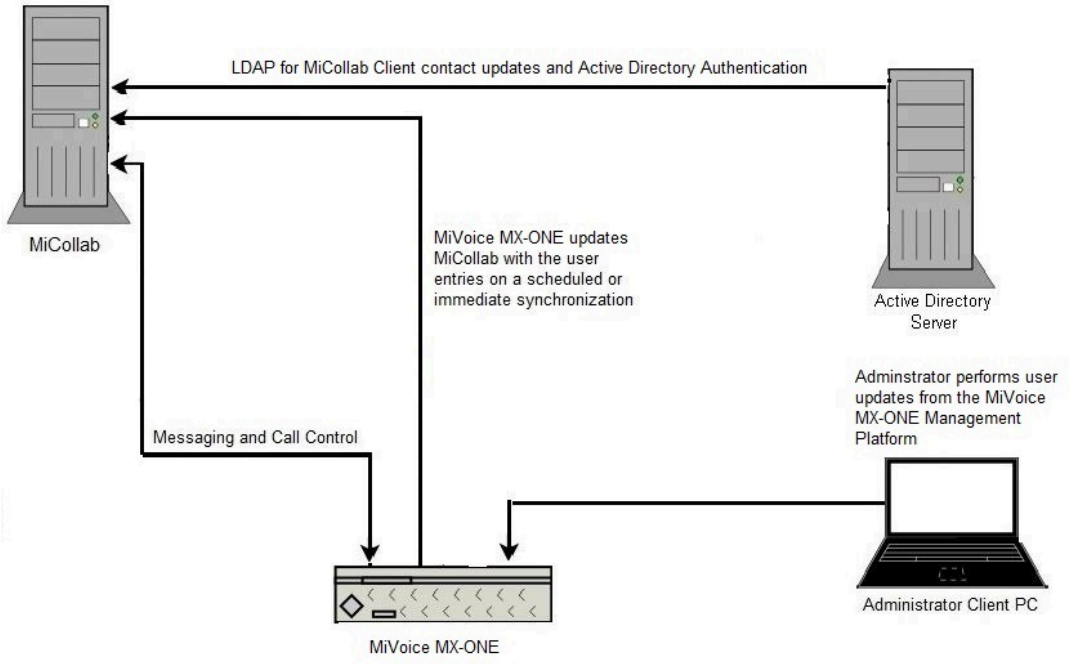


Figure 7: Single MiCollab Server and a Single MiVoice MX-ONE

2.1.2 Conditions and Limitations

- Guidelines and Limitations on page 321

2.1.2.1 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 2019, 2106, 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 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.

2.1.3 Programming

- Configure MiCollab or MiVoice Business Express System with IDS on page 325
- Configure MiCollab IDS for MiVoice MX-ONE on page 330
- Configure MiCollab IDS for MiVoice 5000 on page 332
- Configure Active Directory Authentication on page 335
- IDS Connections on page 339
- Attribute Mappings on page 364
- Disable IDS on MiCollab on page 384

2.1.3.1 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.

2.1.3.2 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.

2.1.3.3 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.

2.1.3.4 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).

2.1.3.5 IDS Connections

- Manage IDS Connections on page 339
- IDS Connection for MiVB Users and Contacts from Active Directory on page 357
- IDS Connection for MiVoice 5000 Contacts from Active Directory on page 358
- IDS Connection for MiVoice 5000 with contacts synchronized from a MiVoice 5000 Directory Service on page 360
- IDS Connection for MiVoice MX-ONE Contacts on page 361
- IDS Connection for Mitel MetaDirectory on page 362
- IDS Connection for Mitel InAttend on page 363

2.1.3.5.1 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	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

Secondary directory server	Enter the FQDN or IPv4 addressof 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 (schedu led) synchronization with the direct ory server. The 'Enable synchron ization' check box should not be che cked 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
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 mul tiple ADs) irrespective of whether t he users have USNChanged attribu te 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
Distinguished name (Directory Server Username)	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.	Blank
LDAP port	Enter the LDAP port number on th e directory server. The default valu e 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

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. Secure (LDAPS) is	TLS

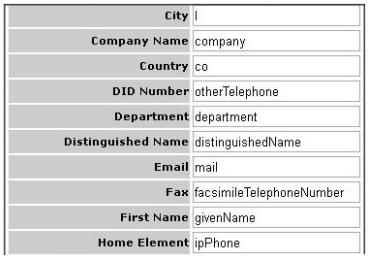
Default query string	Enter the default query string used for filtering LDAP searches. **Note**: The Active Directory default setting processes all user accounts and contact records. The MiVoice 5000 default setting processes all internal and external contact records.	Active Directory defaults to |(ObjectClass=user) (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
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. 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
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
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.

2.1.3.5.2 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:

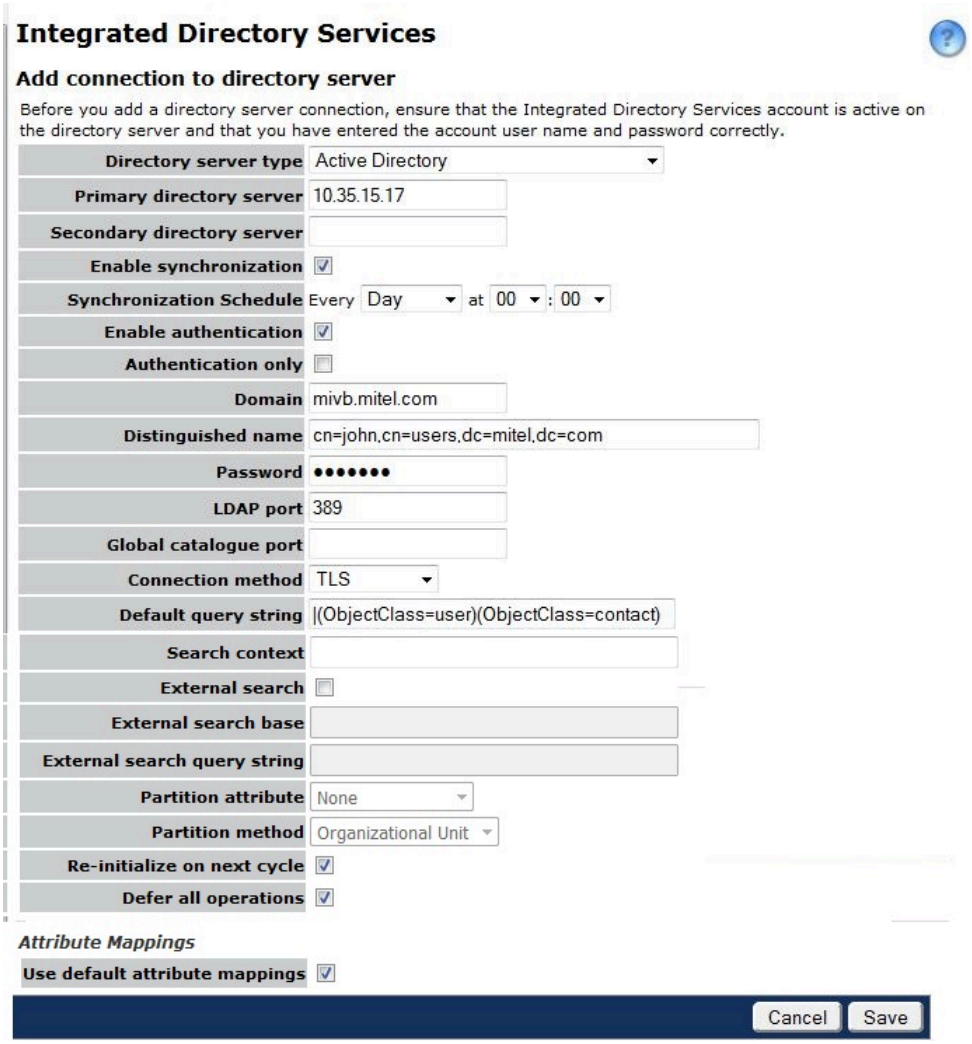


Figure 1: IDS Connection for MiVB Users and Contacts from Active Directory

2.1.3.5.3 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:

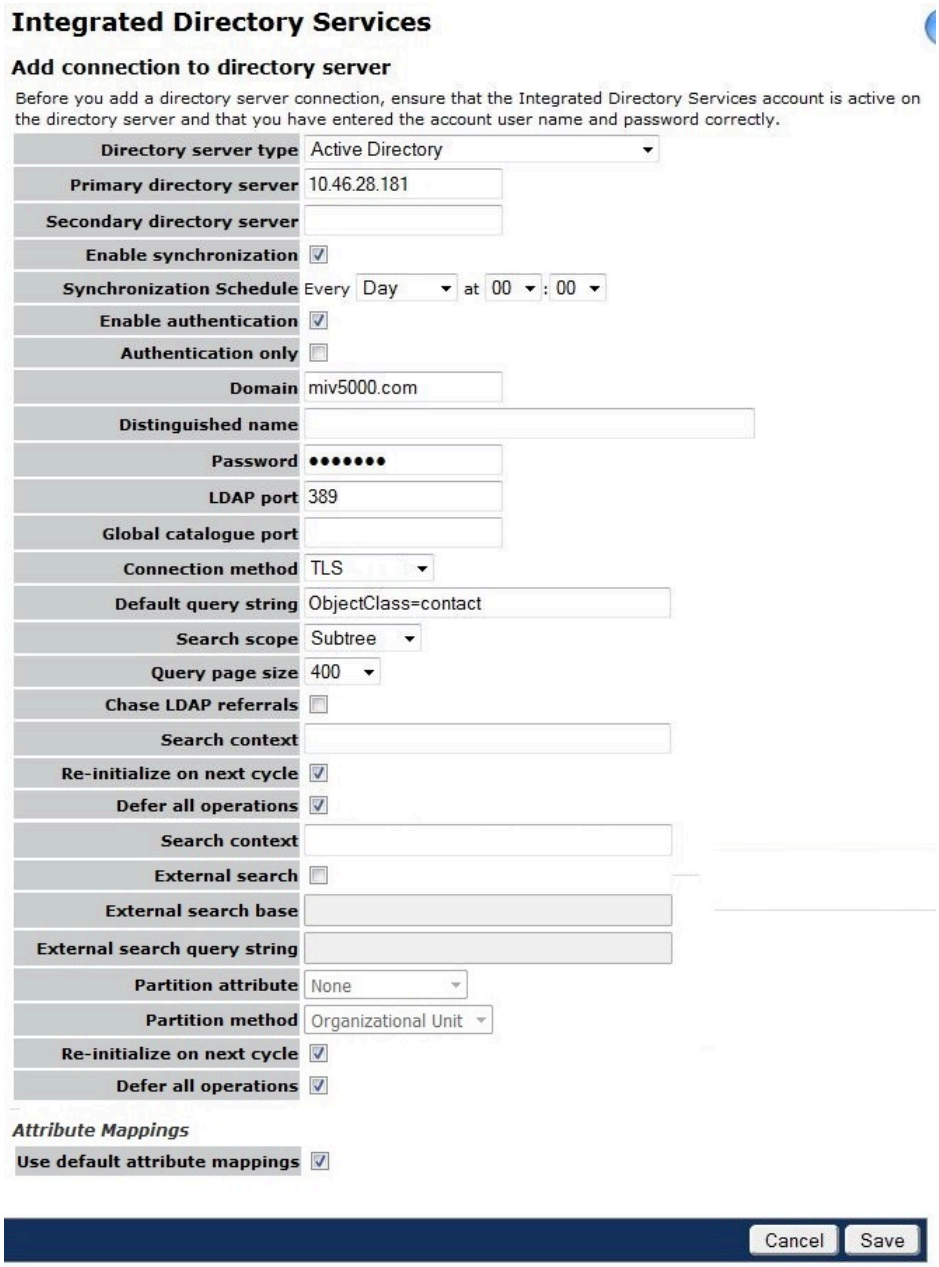
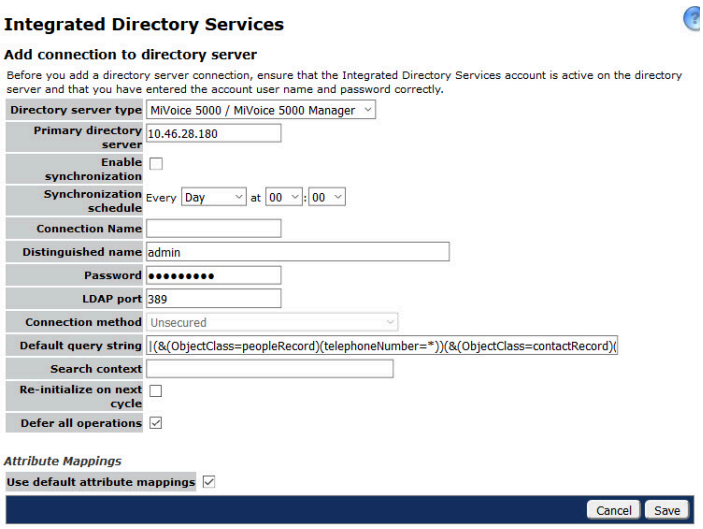


Figure 1: IDS Connection for MiVoice 5000 with Contacts from Active Directory

2.1.3.5.4 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:



2.1.3.5.5 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:

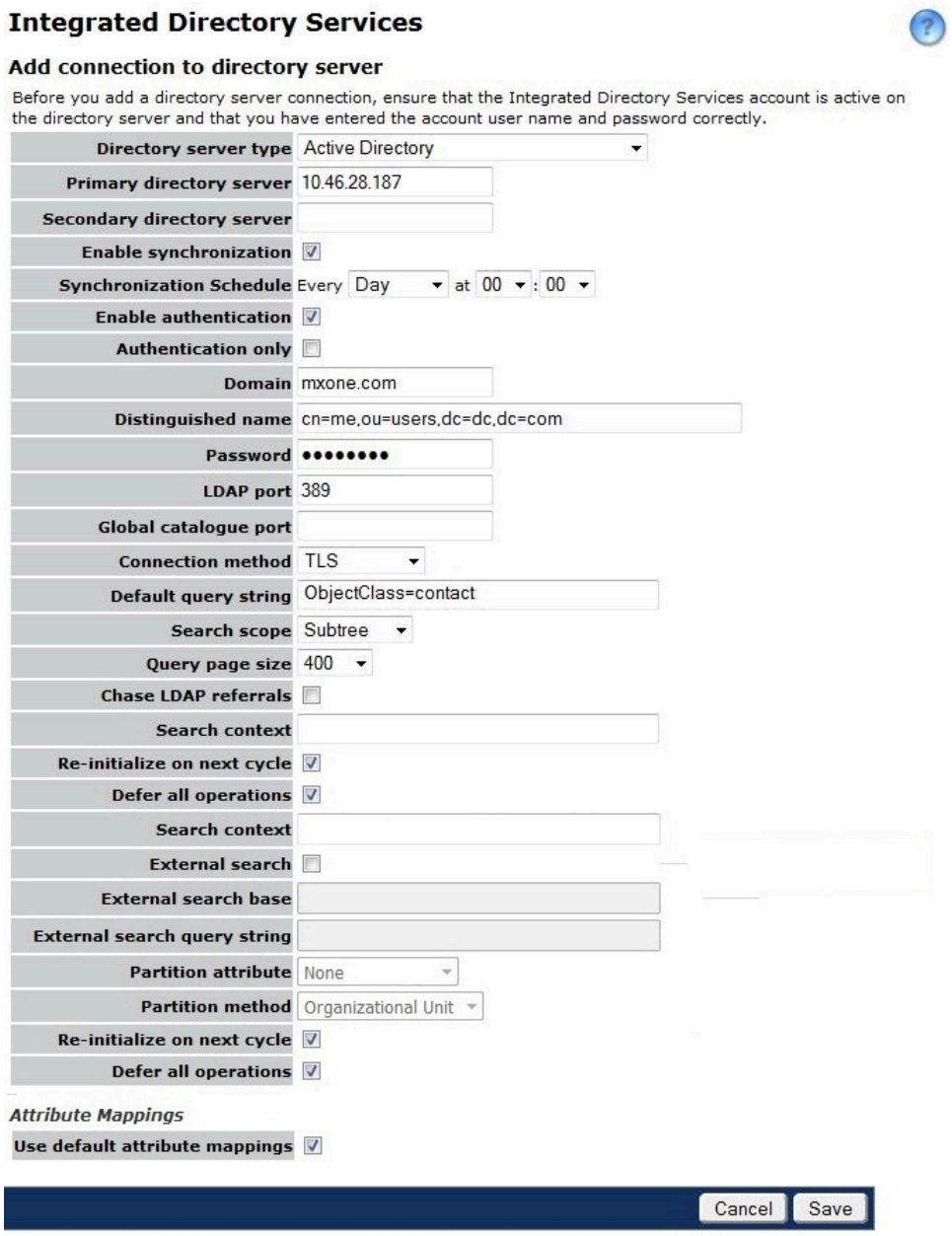


Figure 1: IDS Connection for MiVoice MX-ONE with Contacts from Active Directory

2.1.3.5.6 IDS Connection for Mitel MetaDirectory

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>	

2.1.3.5.7 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>	

2.1.3.6 Attribute Mappings

- Set Default IDS Attribute Mappings on page 364
- Set Custom IDS Attribute Mappings on page 382
- Attribute Mappings for Mitel MetaDirectory on page 383
- Attribute Mappings for Mitel InAttend (BluStar) on page 383

2.1.3.6.1 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.

- Conditions on page 365
- Attribute Mapping Descriptions on page 367

2.1.3.6.1.1 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.

2.1.3.6.1.2 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	name
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	facsimileTelephoneNumb

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	ipPhone	ipPhone	ipPhone	(unmapped)

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

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	physicalDeliveryOfficeNa

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

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
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)					

2.1.3.6.2 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

2.1.3.6.3 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	

2.1.3.6.4 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	

2.1.3.7 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.

2.1.4 External (Off-board) Directory Access

2.1.4.1 Configure Access to External (Off-board) Directory

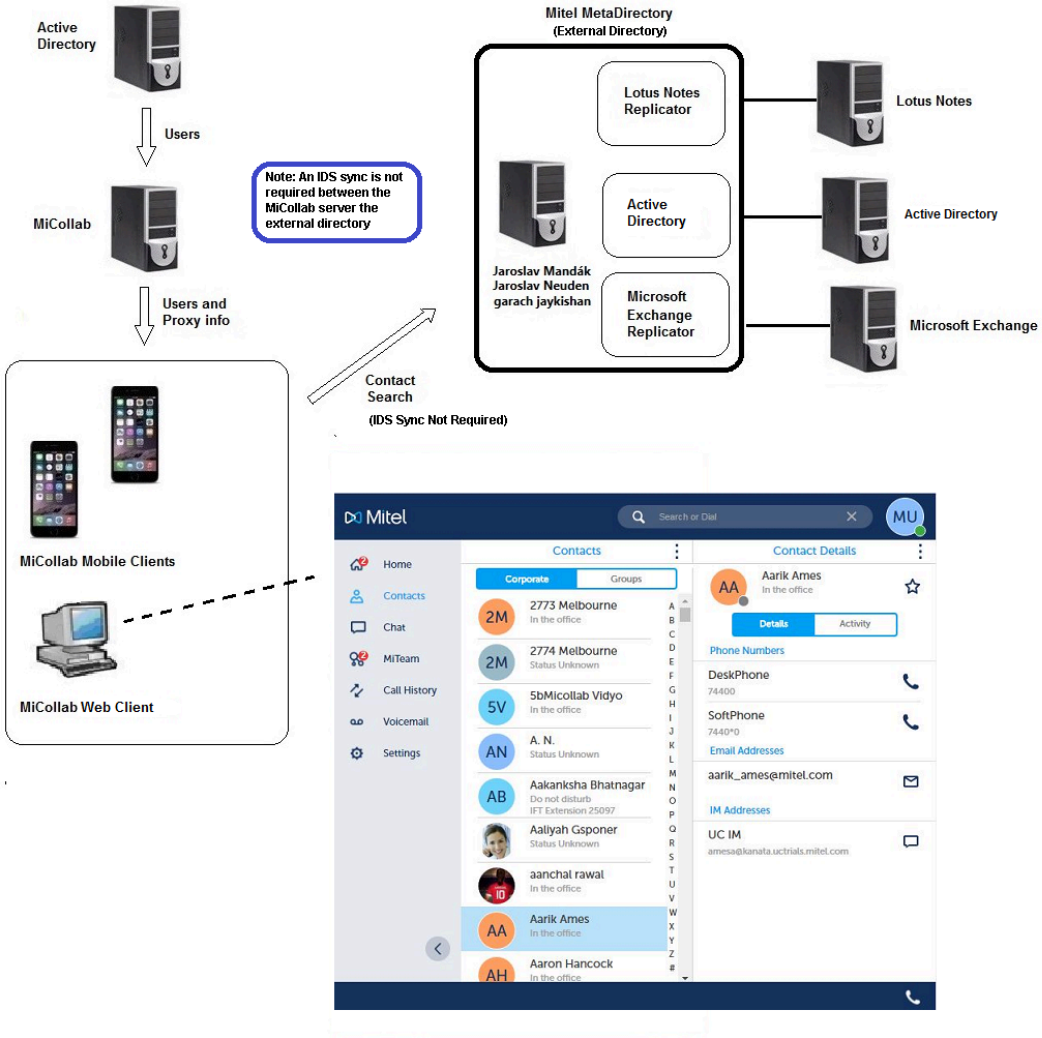
You can configure the MiCollab Client Service with access to a large, external off-board LDAP directory, such as Mitel MetaDirectory. MiCollab Client users can then search for corporate contacts from a very large number of entries.

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>	

Field	Mitel MetaDirectory Setting	Mitel InAttend Setting	Notes
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
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>	

Field	Mitel MetaDirectory Setting	Mitel InAttend Setting	Notes
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	

MiCollab Field	Mitel MetaDirectory mapping	InAttend mapping	Notes
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
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.

MiCollab Field	Mitel MetaDirectory mapping	InAttend mapping	Notes
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.

2.1.4.2 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".

2.1.5 Migrations

- Migrate MiCollab with MiVoice Business IDS to MiCollab IDS on page 395
- Migrate MiCollab with MiCollab Audio, Web and Video Conferencing IDS to MiCollab IDS on page 399
- Migrate MiCollab with MiCollab Client IDS to MiCollab IDS on page 403

2.1.5.1 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

MiVoice Business IDS Connection Settings	MiCollab IDS Connection Parameters
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
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.

2.1.5.2 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 ConferencingLDAP Configuration Settings" that you recorded in the table above into the MiCollabIDS 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.

2.1.5.3 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
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		
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.

2.1.6 Synchronizing IDS Data

- IDS Synchronization Overview on page 408
- Scheduling IDS Synchronizations on page 408

2.1.6.1 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.

2.1.6.2 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**.

2.1.7 Managing Entries

- Add, Edit and Delete Entries using IDS on page 410
- Non-Corporate Contacts on page 412
- Teamwork Mode Users on page 416
- Partitioning the External (Off-board) Directory on page 393
- Add External Numbers on page 269

2.1.7.1 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.

2.1.7.2 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.

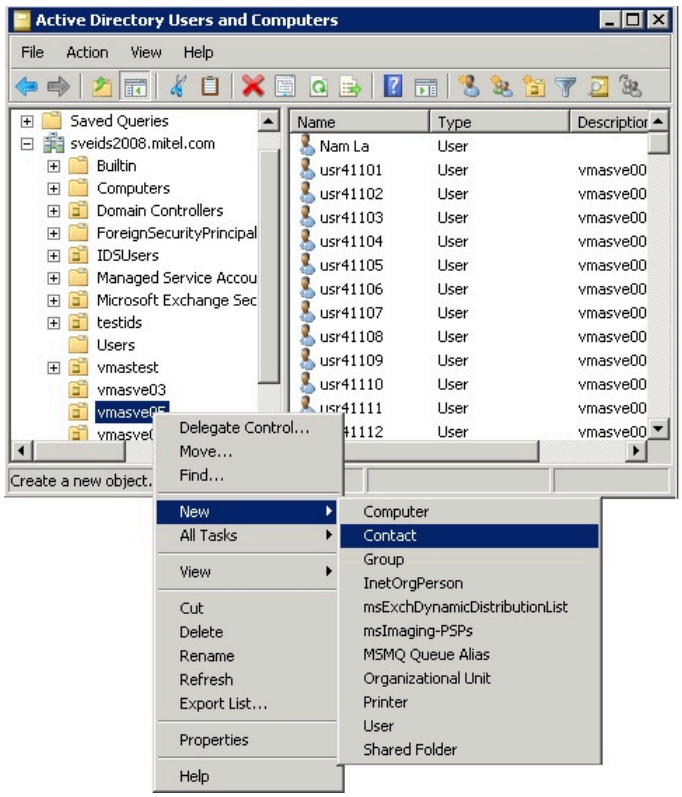
Define the Non-Corporate Contacts on Active Directory

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**.

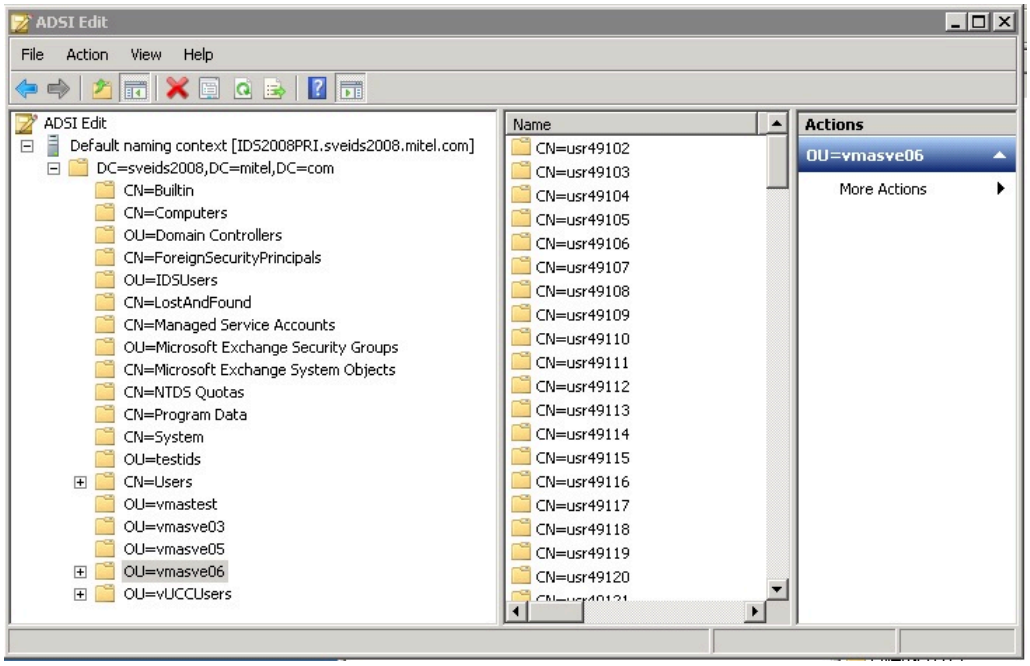


5. Complete the Contact fields. When the databases are synchronized, MiCollab IDS adds the directory entry as a non-corporate contact.

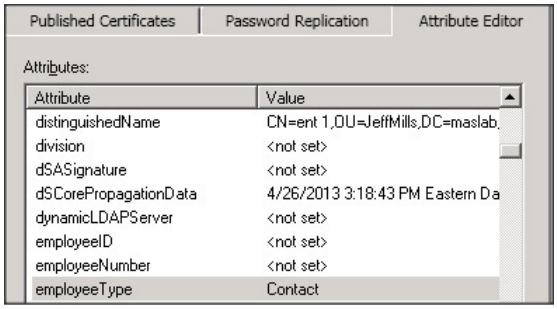
Change an Existing Active Directory Entry to a Non-Corporate Contact

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 fie ld 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 directori es as user entries; Directory servic e 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 directori es as user entries.
Contacts only	(ObjectClass=contact)	Directory service entries with objec t Class set to "contact" are added t o the MiCollab Client directory as n on-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.

2.1.7.3 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.

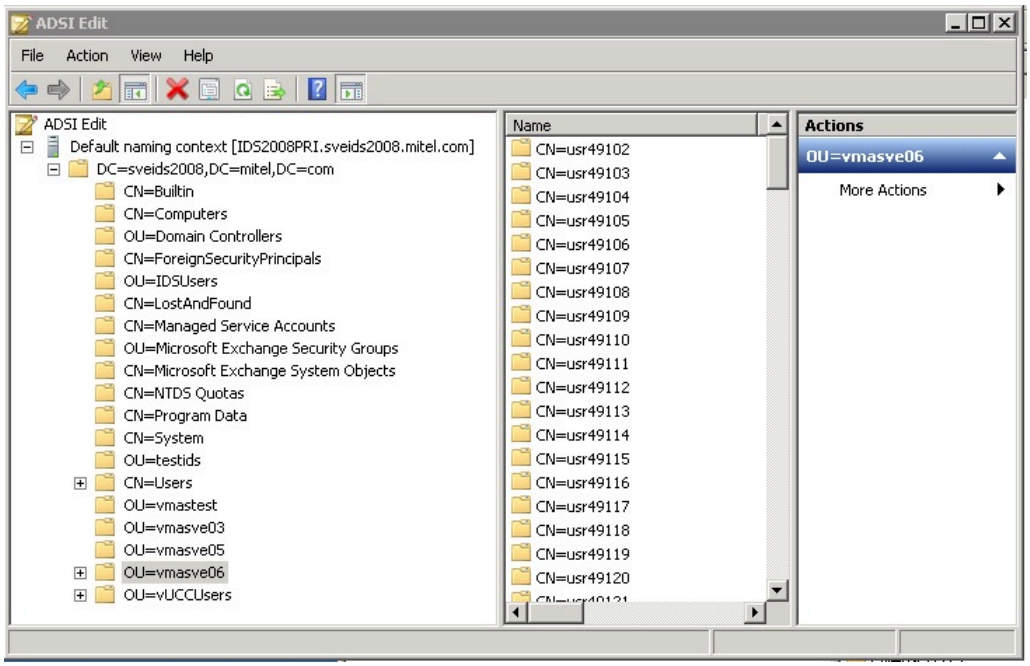
Conditions

- 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

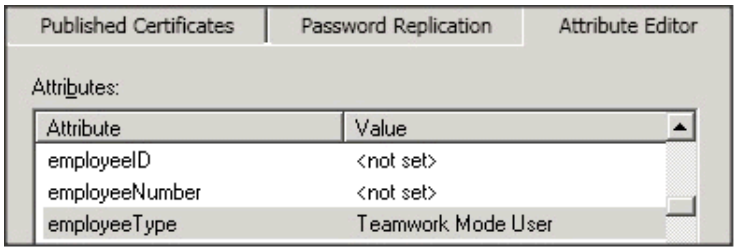
To designate an Active Directory user as a Teamwork Mode user:

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

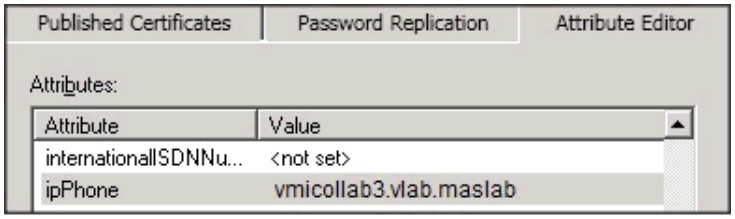
system database in Teamwork Mode. This is the recommended method of designating an Active Directory entry as a Teamwork Mode user.



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.



2.1.7.4 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".

2.1.7.5 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.

2.1.8 Managing IDS Data

2.1.8.1 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.

2.1.8.2 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.

2.1.8.3 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

2.1.8.4 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))

2.1.9 Troubleshooting IDS

- Managing Detained and Failed IDS Operations on page 305
- IDS Synchronization Error Handling on page 426
- Troubleshooting LDAP Authentication on page 427

2.1.9.1 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.

2.1.9.2 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

2.1.9.3 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.

Error	Possible Cause	Corrective Action
	SSL/TLS not enabled on directory server.	Ensure SSL/TLS is enabled on the directory server.
	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

2.2 MiCollab Client Integration Wizard

2.2.1 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 configured, MiTeam is not automatically enabled for them. You must manually enable MiTeam from the MiCollab Client tab of the User and Services application.

2.2.2 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.

2.2.3 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 Authentication error	Verify that the MiCollab Client Service is compatible with MiVoice Business.	
Soap client context setup error	Internal MiCollab Client Service error.	Restart the MiCollab Client Service .
Soap login failed Soap login rejected	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.
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		
Server returned failure	View the EPM logs to determine error code.	Corrective action based on the error code.
Version request failed Version fetch failed	The MiCollab Client Service is not compatible with MiVoice Business version.	Upgrade MiVoice Business and the MiCollab Client Service to compatible versions.
DSM internal error	MiCollab Client Service internal error.	Capture the MiCollab Client Service dsm.log and contact support.

Error	Details	Corrective Action
# instances: Subscriber creation failed: There are currently no licenses for the feature <FEATURE NAME> in the <ENTERPRISE NAME>	You don't have enough feature licenses on the MAS system to support the number of users that are being imported from the MiVoice Business s. The # of instances indicates the number of required feature licenses.	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.

2.3 MiCollab Settings

2.3.1 Configure MiCollab Settings

This form allows you to

- 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.

2.3.2 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
   - 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
   - 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.

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.

2.3.3 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**.

2.3.4 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.

2.3.5 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.

2.3.6 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.

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.

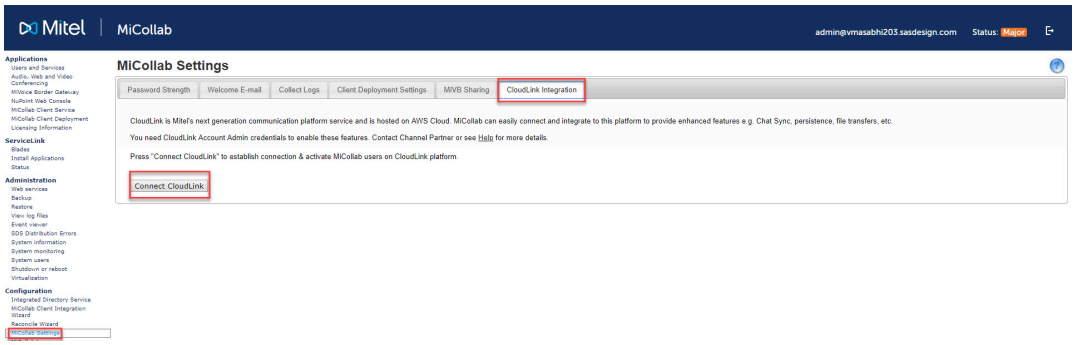
1. In the MiCollab Administrator portal, under **Configuration** click **MiCollab Settings.**

   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.

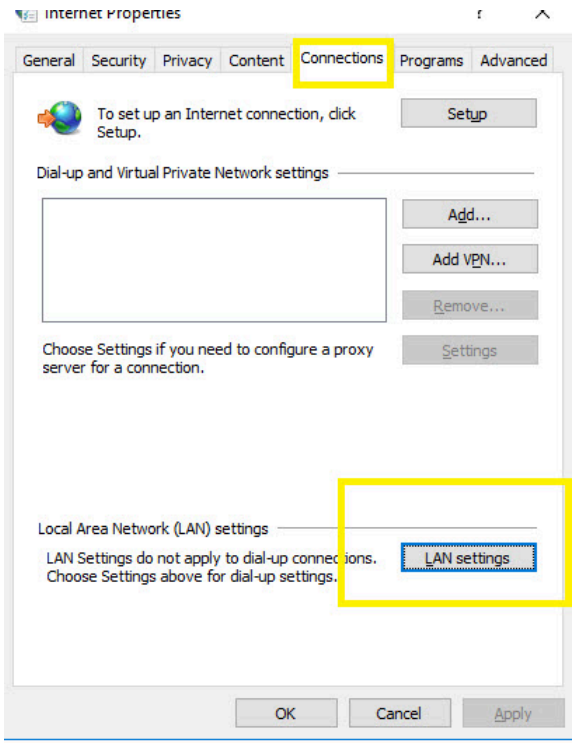
> **Note**:
> For CloudLink chat, at network firewall level, the following firewall related exceptions must be considered. The network firewall must allow access to CloudLink URLs on mitel.io (https on port 443). These URLs *(*.mitel.io/**) should be reachable from MiCollab Server, PCs, which are used for opening the MiCollab Admin Portal and the PCs and mobile phones where MiCollab Client is running.

Proxy Exception List

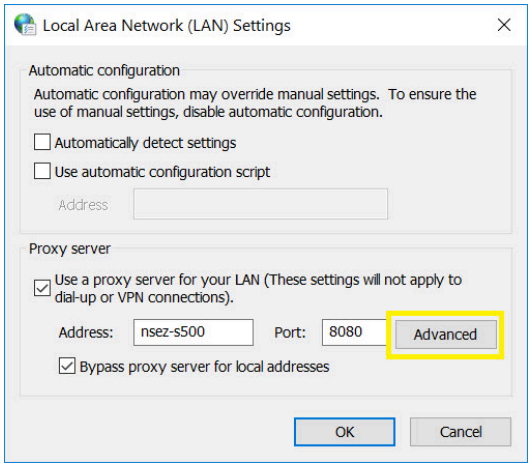
If your organization uses a web proxy, you may need to add the CloudLink server address to your proxy exceptions list. To add the server to your proxy exceptions list:

1. From Control panel, select **Internet Options**.

2. Under **Connections** tab, select LAN settings.

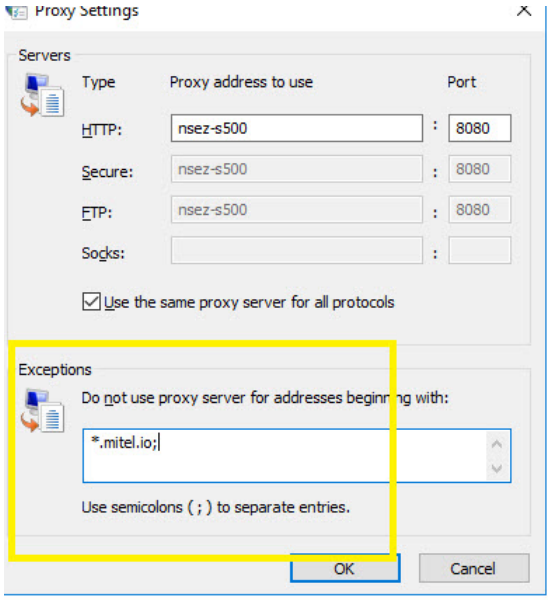


3. Enable the **Use a proxy server for your LAN** setting.
4. Enter the proxy address and the Port number and enable the **Bypass proxy server for local addresses** setting.



5. Click **Advanced**.

6. Add **.mitel.io* in the Proxy Exceptions list box.



7. Click **OK**.

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 CloudLink Accounts Console.

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 **CloudLink Accounts Console**.

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.

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.

Failure reason/ Error in CSV Report	Possible correction step to admin
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.
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.

Failure reason/ Error in CSV Report	Possible correction step to admin
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 CloudLink Accounts Console.
CloudLink Error - 409,User Already Exists	Check whether the user exist in CloudLink Accounts Console.

2.4 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.

2.5 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)
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.	

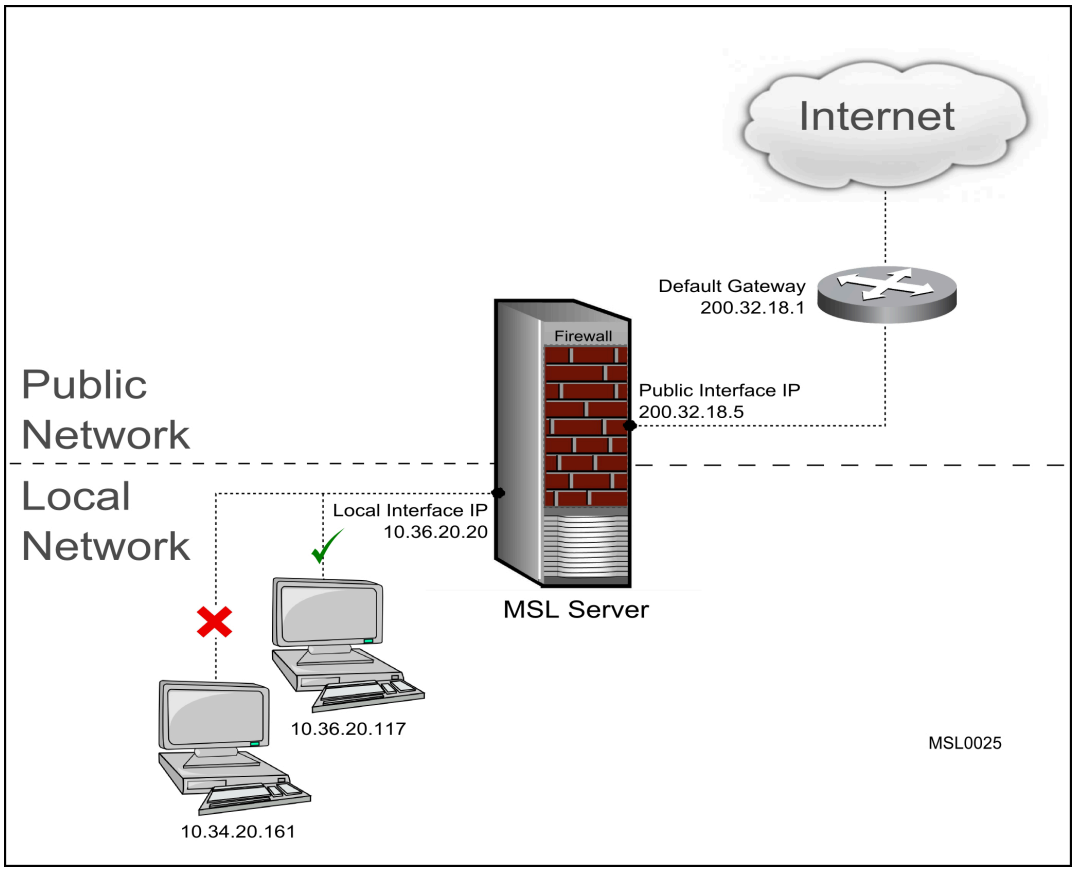
2.6 Configure Networks

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

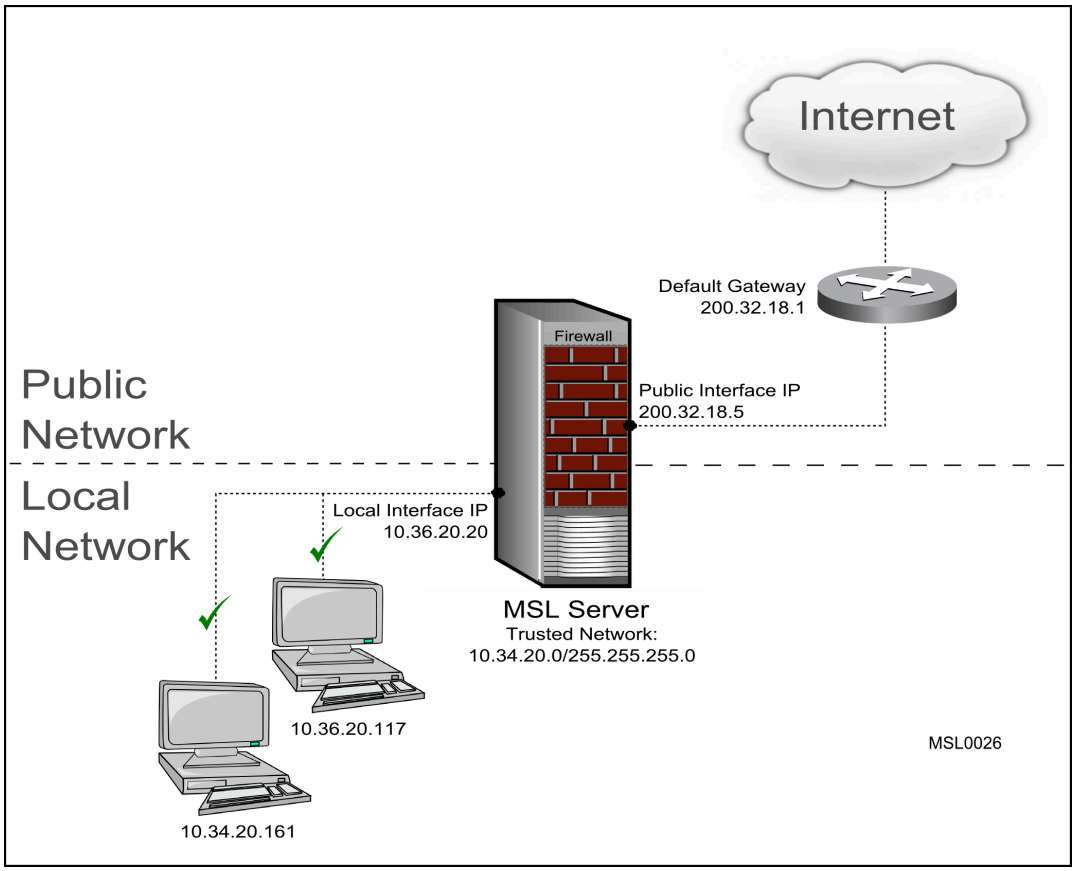
In the example illustrated below, the LAN interface of the MSL server has an IP address of 10.36.20.20. Accordingly, the server will accept traffic *only* from the 10.36.20.x network while blocking traffic from all other subnets on the LAN.



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 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 left 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:

- Enable Secure Shell for trusted and remote management networks.
- Add trusted network for the MPA with **Network** as 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**.

2.7 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.

2.8 Cloud Service Provider

2.8.1 Google

2.8.1.1 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.

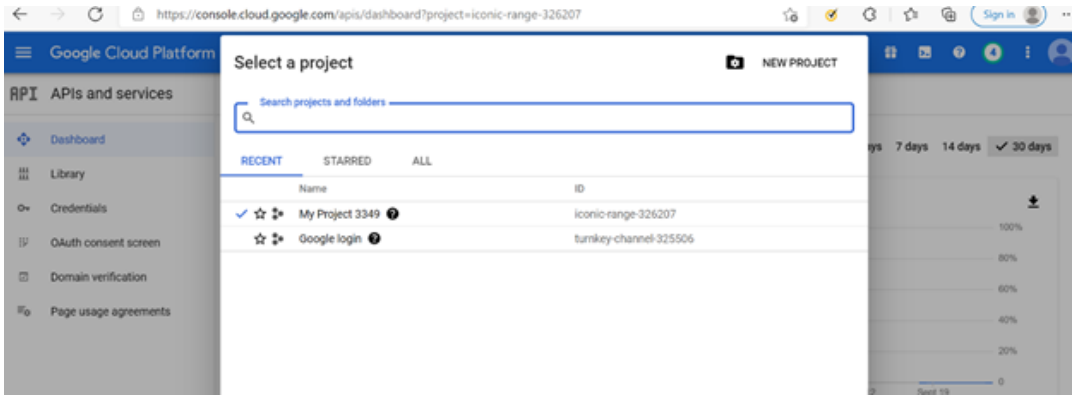
2.8.1.2 Configure OAuth 2.0 for Installed Applications

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.

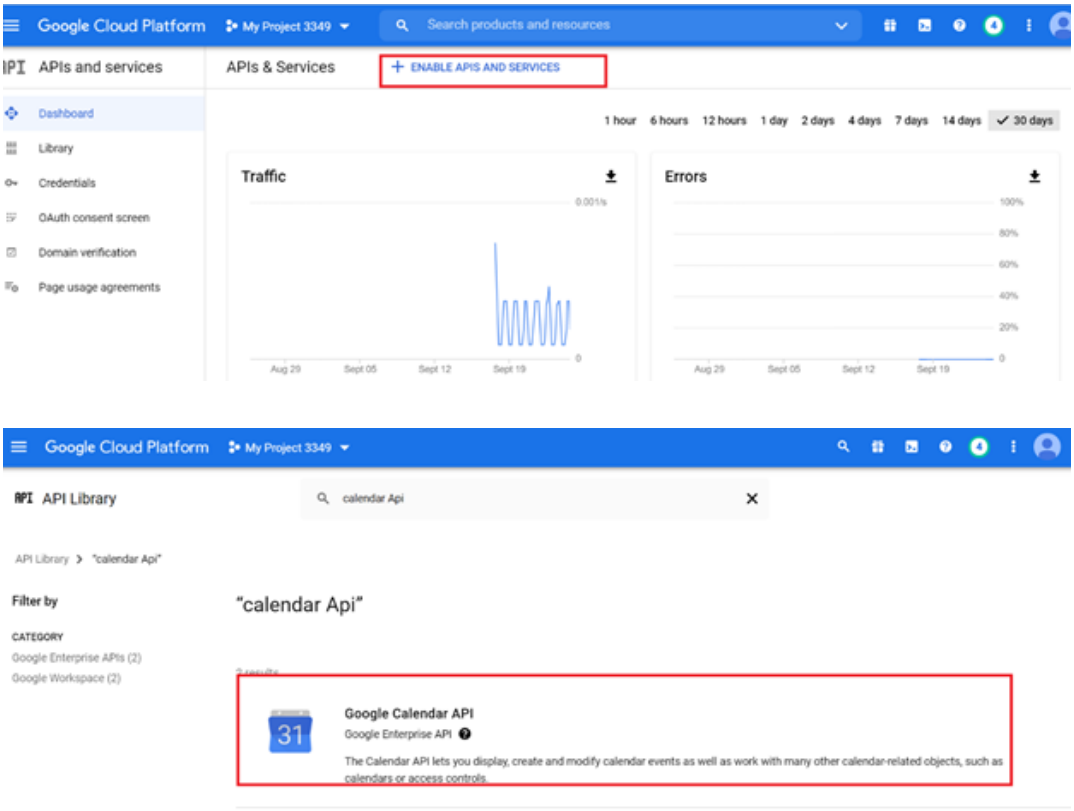
Create an API Project and Client ID in Google

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**.



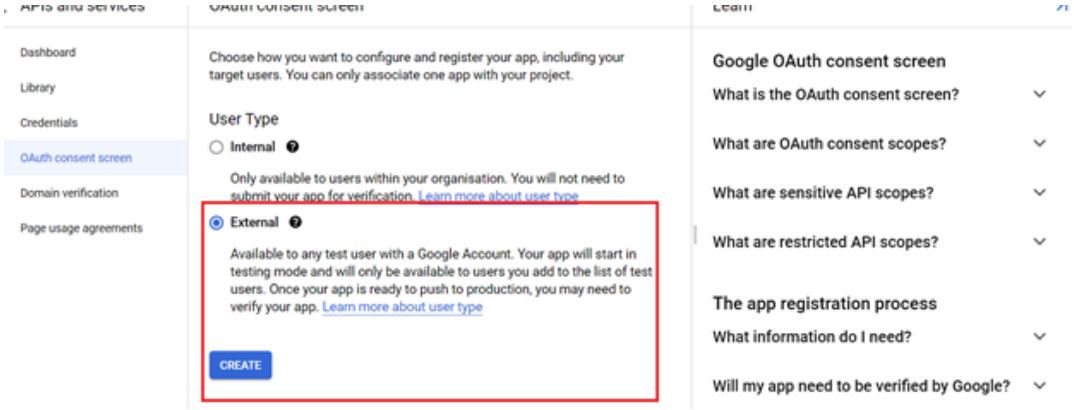
   c. Repeat for all Google APIs you want to support.

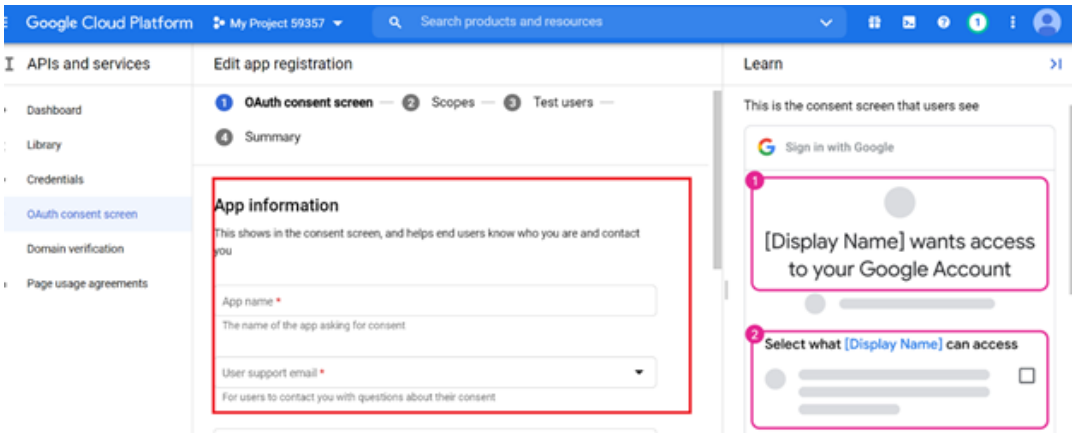
Note:

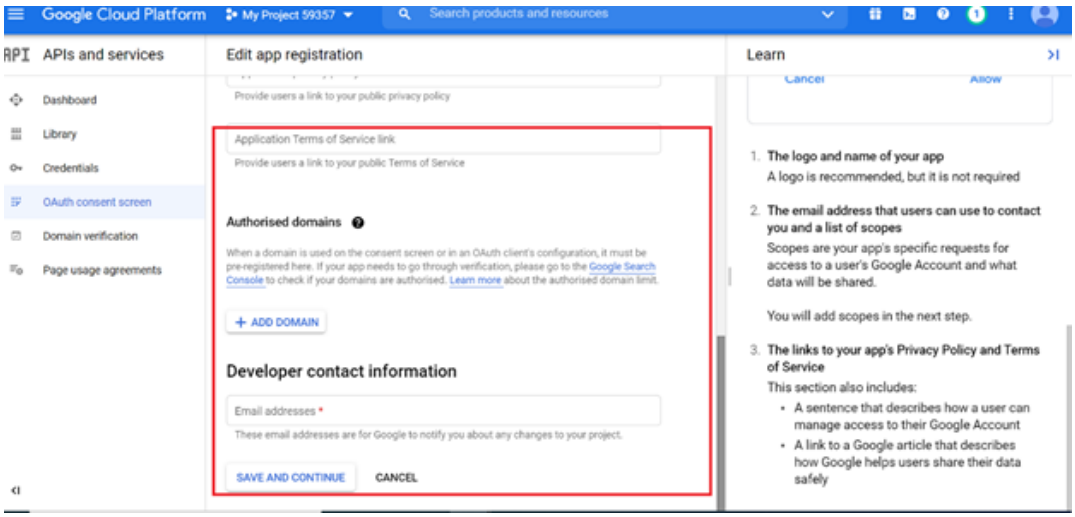
The preceding instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help: https://developers.google.com/workspace/guides/create-project.

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.



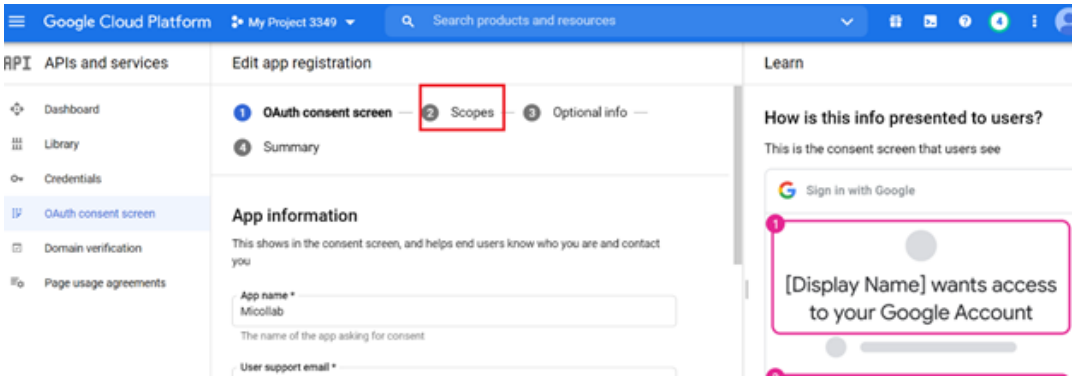


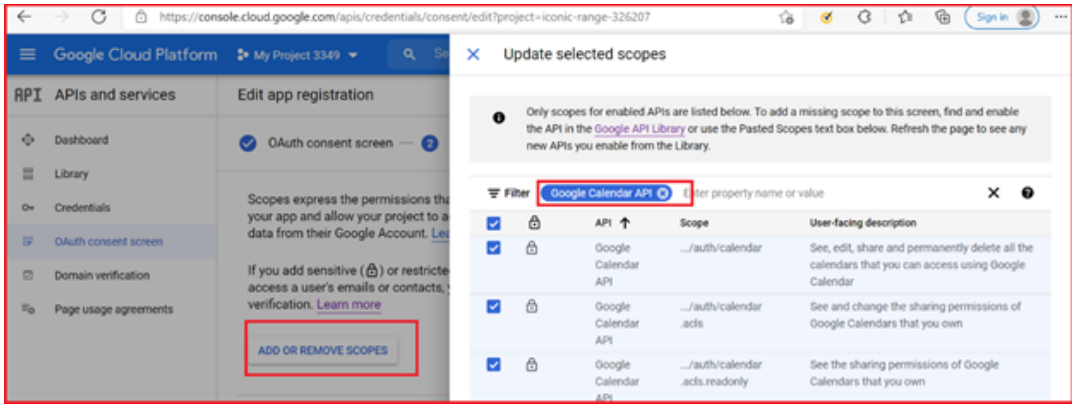


Note:

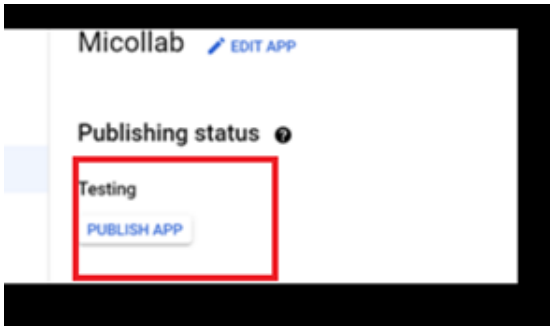
Following scopes are required for Google Calendar API:

- /auth/calendar.readonly
- /auth/calendar.events.readonly

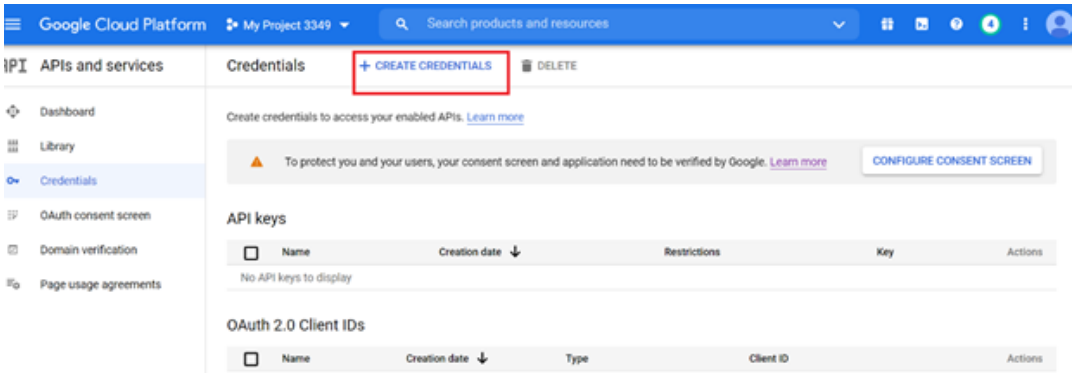


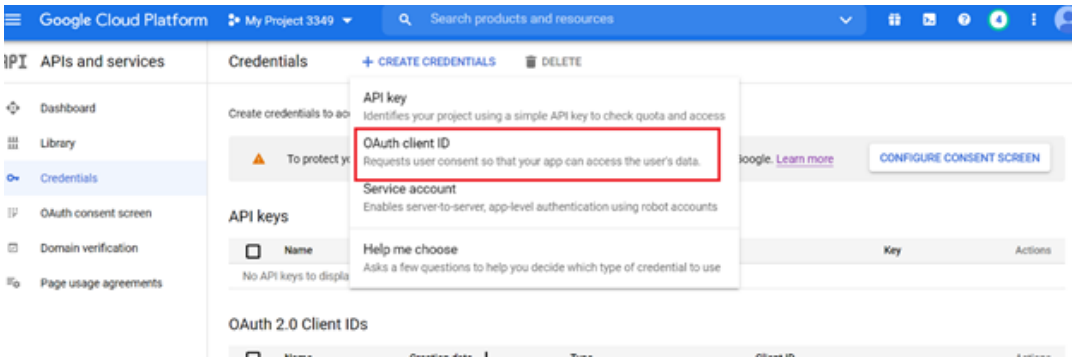


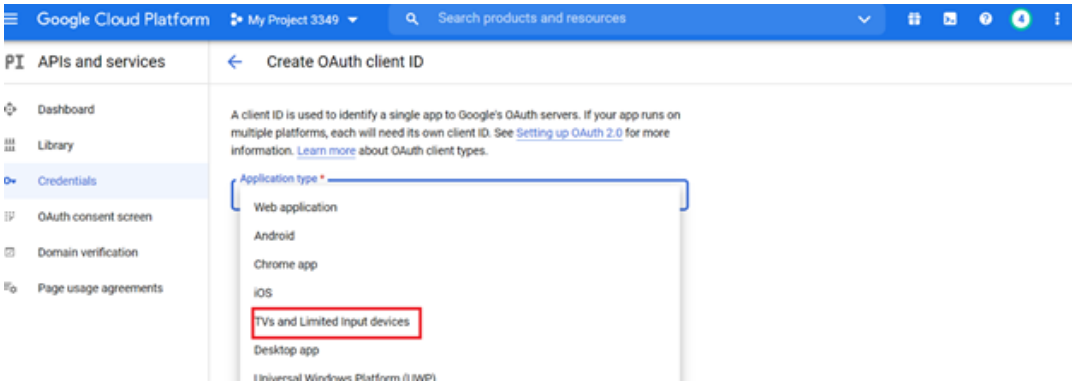
5. Publish the application.

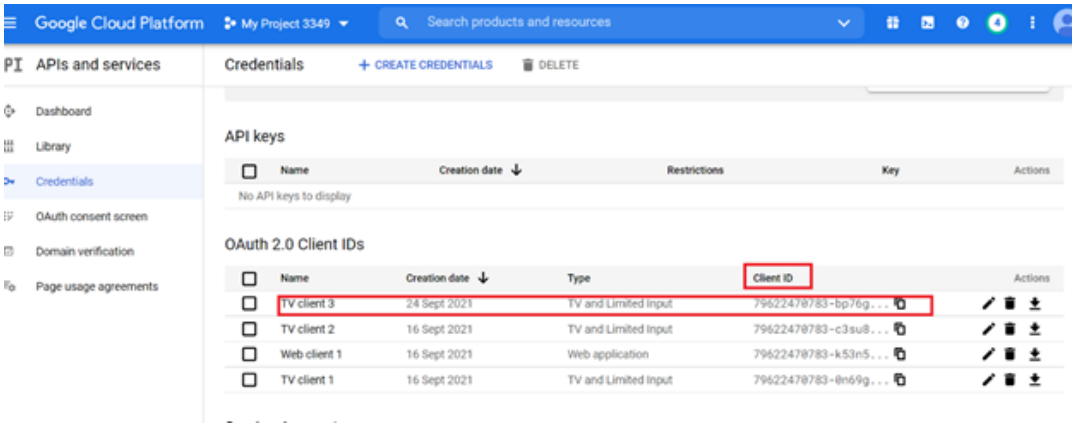


6. Create the OAuth 2.0 Client ID and Secret for the project:









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:

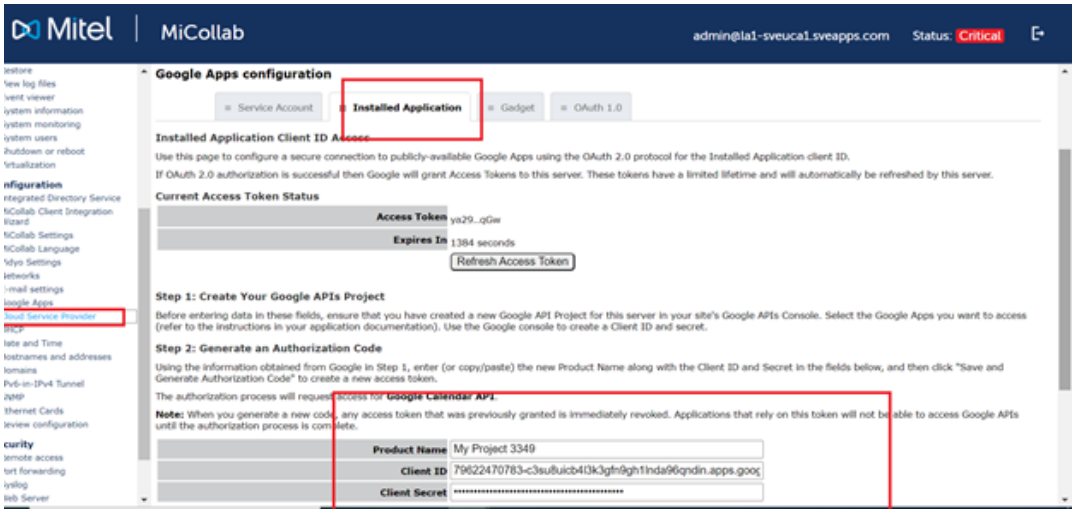
For the Google Calendar API, please select Application type as TVs and Limited Input devices.

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.

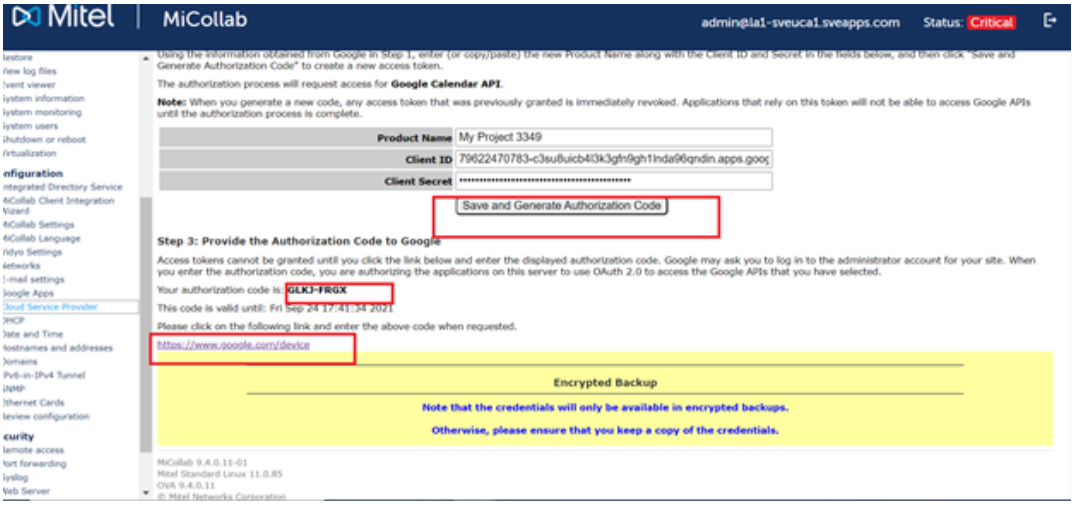
1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Google Apps**.



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.

2.8.1.3 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.

2.8.1.4 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 470

   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 synchronizatio with MiCollab Audio, Web and Video Conferencing . For example, if the user

2.8.1.5 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**.

2.8.2 Microsoft

- Configure Microsoft Identity on page 478

2.8.2.1 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 Azure portal:

1. Register an application, see Microsoft help.
2. Obtain the unique Application ID and Tenant ID assigned by Azure Active Directory.

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 Azure Active Directory. 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 Azure Active Directory. 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.

2.9 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.

2.10 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**.

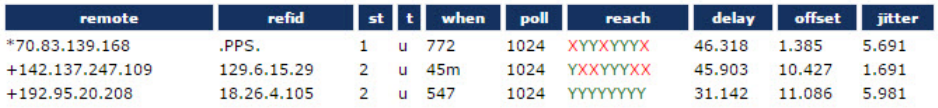
Note:

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).



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:	
	*	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.

Command output	Meaning	
	-	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.
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.

Command output	Meaning	
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.
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.

2.11 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.
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**.

2.12 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**.

2.13 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.

2.14 Configure SNMP Support

SNMP, or 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 c ommunity 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.
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.

Field	Description
One minute CPU threshold	If you have CPU monitoring enabled, you must cho ose a threshold value for the one minute load average, above which this server will flag the error at the previo usly mentioned OID. The value must be a positive rea l number with no more than two decimal places of pre cision.
Five minute CPU threshold	If you have CPU monitoring enabled, you must cho ose a threshold value for the five minute load average, above which this server will flag the error at the previ ously mentioned OID. The value must be a positive re al number with no more than two decimal places of pr ecision.
Fifteen minute CPU threshold	If you have CPU monitoring enabled, you must cho ose a threshold value for the fifteen minute load av erage, above which this server will flag the error at th e previously mentioned OID. The value must be a posi tive real number with no more than two decimal places of precision.
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 d aemon, enter the hostname or IP address of the host designated to receive these trap messages. If this is le ft blank, traps will not be sent. To send traps to more than one host, enter the hostnames and/or IP address es 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 b e used.
SNMPv3 Trap username	Enter the SNMPv3 trap user name to use when send ing trap messages. If you leave this field blank, SNMP traps will be sent using SNMP v2c.

Field	Description
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.

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)

Field	Description
Authentication Password	If you selected an Authentication Type (MD5 or SHA1) , you must enter an authentication password (also kn own as “authentication passphrase”) at least eight c haracters long.
Privacy Protocol	Select the Privacy Protocol that matches SNMP manager/agent configuration: • DES • None (no encryption)
Privacy Password	If you selected a Privacy Protocol (DES), you must e nter 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 autom atically.

2.15 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.

Setting	Description
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.

2.16 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

Miscellaneous 3

This chapter contains the following sections:

3.1 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. 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 n**ew 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