A MITEL
PRODUCT
GUIDE

MiCollab Client Administrator Console

Release 9.6
July 2022

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.

MiCollab Client Service 1

This chapter contains the following sections:

1.1 About Help and Versions

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

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

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

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

1.2 About MiCollab Client

MiCollab Client is an application that converges Mitel communication platform call control capabilities with Dynamic Status, presence, contact management, and collaboration to simplify and enhance real-time communications.

Note:
MiCollab Client functionality described in documentation refers to enterprise **as a single company entity**. In scenarios where multiple server domains are created, it is understood to be within a single company environment where multiple MiCollab Client Services or mixed PBX nodes are required to manage the solution.

Users can access MiCollab Client features from the following interfaces:

- MiCollab for PC Client
- MiCollab for Web Client
- MiCollab for Mobile Client
- MiCollab for MAC Client
- MiCollab for Microsoft Client

MiCollab Client user interfaces support several languages.

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English (US)
- English (UK)
- French (Canadian)
- French (European)
- German
- Italian
- Portuguese (European)
- Portuguese (Brazilian)
- Russian
- Spanish (European)
- Spanish (Latin American)
- Swedish
- Norwegian
- Finnish
- Danish

User documentation for MiCollab Client is available in the following languages:

- Dutch
- English (US)
- French (Canadian)

- French (European)
- Italian
- Portuguese (Brazilian)
- Portuguese (European)
- Spanish (Latin American)
- Spanish (European)
- Swedish
- Norwegian
- Finnish
- Danish
- German
- Chinese

MiCollab Client is integrated with other Mitel applications.

- **MiCollab Audio, Web and Video Conferencing (formerly known as Mitel collaboration Advanced)**: Access to MiCollab Audio, Web and Video Conferencing is integrated within MiCollab Client . When users are licensed for MiCollab Audio, Web and Video Conferencing , they can use collaboration features such as real-time audio and Web conferencing, annotation, chat, file transfer, and desktop sharing.
- **MiCollab Unified Messaging™ (UM)**: Provides access to NuPoint UM voice mail and FAX messages from the Desktop Client's Visual Voice Mail view. Voice mail messages can also be retrieved from the MiCollab Client Web/Mobile Portals, MiCollab Mobile Client for Android and MiCollab Mobile Client for iOS.
- **MiVoice Border Gateway**: Provides a secure communications path for remote MiCollab Client softphones and IP desk phones to the Unified Communications server. ***This product is supported for MiVoice Business communication systems only***.
- **Mitel Web Proxy v2.0**: Web Proxy provides a secure communications path from remote users to the MiCollab Web Clients. ***This product is supported for MiVoice Business communication systems only.***

See the Administrator Tasks topics for basic administrator and links to task-related instructions.

See the Administrator Interface topic for a description of the UI elements in the MiCollab Client Service Administrator pages.

Note:
For instructions on how to integrate the MiCollab Client database into the USP database using the MiCollab Client Integration Wizard, refer to the ***MiCollab Installation and Maintenance Guide***.

MiCollab Client Service Administration Page

This page includes the following sections:

- **Configuration**:

  Provides a button that links to the administration tabs and associated pages. Click **Configure MiCollab Client Service**to access.

  > **Note**:
  >
  > While configuring, the MiCollab Client Service must use an FQDN of 57 characters or less.

- **Status**:

  Provides the current status for the MiCollab Client Service , and the ability to start, stop, or refresh the server. For Server Status, the name of the server is displayed along with one of the following:

  - **Active**: The server is online and operational.
  - **Becoming Active**: The server is in the process of coming online.
  - **Idle**: The server is offline and not operational.

  To start, stop, or refresh the server:

  1. Select an action from the list box:
     - Start Mitel MiCollab Client Service
     - Stop Mitel MiCollab Client Service
     - Refresh Status
  2. Click **Perform Requested Action**.

- **Client Versions**:

  Under the MiCollab Client Service, the Client Versions section lists all the MiCollab Client software versions that are available on the server for the particular release.

  The administrator also has an option to enable/disable the feature to Upgrade PC Clients from Cloud. By default, this setting would remain enabled in the server, which means that all users will upgrade their clients from Cloud unless the administrator explicitly disables the option.

Note:

Even if the **Upgrade PC Clients from Cloud** option is selected, and there is a newer version of PC clients available on the server and not on Cloud, the end-users will receive a notification pop-up for upgrading their PC Clients. The end-users will not have any back-end information regarding the notifications that they receive, whether the upgrade is getting done from the Cloud or from the server.

Note:

The feature to Upgrade Clients from Cloud is only applicable for PC Clients.

The MiCollab Client software stored on this server may be upgraded or downgraded without requiring an upgrade of the MiCollab Client service.

To perform an upgrade or downgrade of a supported MiCollab Client:

1. Under **Applications**, click **MiCollab Client Service**.
2. In the New Client Package field, click the **Browse**button and navigate to the MiCollab Client package to be uploaded.
3. Click **Upload MiCollab Client**.
4. The list of installed MiCollab Client software will automatically be refreshed with the updated version information.

Note:
The MiCollab Client Service Administration page accepts only .rpm format when uploading MiCollab Client software.

- **Diagnostics**:

The Diagnostics section of the page provides access to diagnostics tools. Click **Perform Server Diagnostics**to access diagnostics tools.

Note:
Do not use the MiCollab Client Service Diagnostic tools unless you are instructed to do so by Mitel technical support personnel.

- **Import Data**:

  Allows you to import MiCollab Client Service data from an already backed-up file. If you have a backup file generated on a MiCollab Client Service, use this form to restore the data.

  Note:
  MSL configuration information (network information, hostname, and so on) contained in the backup file will be ignored.

  Importing data using this option will overwrite all MiCollab Client Service configuration information and reinitialize the MiCollab Client Service database to the values stored in the specified backup file.

  To import the data file:

  1. Under **Import Data File**, click **Browse**.
  2. Navigate to the backed-up form file, select the file and click **Open**.
  3. Click **Import MiCollab Client Service Data**.

- **Reinitialize System**:

  Selecting the Reinitialize MiCollab Client Service Configuration, reinitializes the configuration of the MiCollab Client Service.

  Note:
  Selecting this option will remove all MiCollab Client Service configuration information and reinitialize the MiCollab Client Service database.

  To reinitialize MiCollab Client Service configuration:

  1. Click **Reinitialize MiCollab Client Service Configuration**.
  2. Click **OK**.

- **RC4 Setting**:

  Rivest Cipher 4 (RC4) is a stream cipher that protects confidential data messages sent to and from secure URLs. However, RC4 has multiple vulnerabilities and the Payment Card Industry Data Security Standard (PCI DSS) recommendation is to disable it.

  For MiCollab 8.1 or later, by default, RC4 is disabled. For earlier releases, RC4 is enabled by default and the administrator must disable it to be compliant with Payment Card Industry Date Security Standard (PCI DSS). Enabling or disabling this option may impact presence and ongoing chats, so change this setting outside of business hours. To change the setting:

  1. Clear the box to disable or check the box to enable.
  2. Click **Save RC4 Setting**.

  Note:
  If MBG is acting as a gateway for connections from a MiCollab server, there may be a requirement to enable RC4.

- **MiVB (MiXML/MiTai) Security Setting**:

  Enable **MiVB (MiXML/MiTai) Security Setting**to support public and corporate certificate for MiXML and MiTai connections towards MiVoice Business .

  Before enabling security setting, make sure prerequisites are met and take note of limitations.

  Prerequisites:

  - MiVB version is 8.0 or higher.
  - Public certificate or corporate certificate **signed by same authority**is installed on both MiVB and MiCollab Server.
  - MiVB FQDN or IP address must be included in subject or subject alternate name in the certificate.

Note:
If prerequisites are not met, PBX synchronization and MiTai connection will fail.

Limitations:

- Wild card domain names are supported in common name only.
- Self signed certificate is not supported.

By default, MiVB (MiXML/MiTai) setting is disabled. To enable the setting:

1. Check **Enable MiXML MiTai Security Setting**checkbox.
2. Click **Save MiXML MiTai Security Setting**.

Note:
In public certificate, IP address is not supported. If public certificate is used, administrator must program MiVBs with MiVB FQDN in MiCollab.

Note:
For MiVB 8.0 release, web server certificate signed by same authority needs to be installed.

Note:
For MiVB 9.0 release, web server certificate and device certificate, signed by same authority needs to be installed.

- **Federation Service Setting**:

  Click **Enable Federation Service Setting** to enable the federation service in MiCollab Client Service.

  Note:
  Enabling or disabling the federation service will restart MiCollab Client Service.

  By default, the Federation Service Setting is disabled. To enable the setting:

  1. Check **Enable Federation Service Setting** checkbox.
  2. Click **Save Federation Service Setting**.
  3. Click **OK** on the prompt to restart MiCollab Client Service.

- **MiTAI UTF-8 Support**:

  Enable MiTAI UTF-8 Support to get UTF-8 characters in CDRs (name fields) from MiVB. Before enabling this setting, make sure all MiVBs connected to this server are running on version 9.0 or later.

  By default, MiTAI UTF-8 support setting is disabled. To enable the setting:

  1. Check MiTAI UTF-8 Support checkbox.
  2. Click Save MiTAI UTF-8 Setting.
  3. Click OK on the prompt to restart PBX Proxy. PBX Proxy will automatically restart in the background.

  Note:
  If the configured MiVB version is not available or lower than 9.0, administrator cannot enable the MiTAI UTF-8 Support setting.

Note:
If the MiTAI UTF-8 support setting is enabled and the administrator provisions MiVB (lower than MiVB 9.0), the server will raise a critical alarm during next PBX sync. The administrator must disable this setting or upgrade MiVB version to 9.0 or later. After the configuration is updated, clear the alarm from the event log.

1.3 What's New in MiCollab Client

For a list of new functionality, see MiCollab What's New Guide in the Mitel Customer Documentation site, the Document Center.

Note:
For additional details about end-user MiCollab Client new features and enhancements, refer to the ***online Help*** for the specific interface or the ***Mitel MiCollab Client Administrator Guide*** available on the Mitel Document Center Web site.

1.4 Requirements

This topic provides basic requirements for the MiCollab Client product. For additional details, refer to the ***Mitel MiCollab Client Administrator Guide*** available on the Mitel Document Center Web site.

Server Requirements

The MiCollab Client Service resides as either a stand-alone application on a Mitel Standard Linux (MSL)-approved hardware platform or an integrated application in the MiCollab. There are three options for the MiCollab Client Service component:

- Purchase an approved MSL hardware platform, download, install, and configure the required MSL operating system and MiCollab Client Service blade on site.
- Purchase the MiCollab Server Appliance, which includes the pre-installed MSL operating system and MiCollab Client Service software blade on an approved hardware platform. This option requires minimal on-site configuration. Note that for MiCollab Client 5.0, the MiCollab Client Service Appliance is no longer available for purchase. You can upgrade to MiCollab Client 5.0 with the MiCollab Client

Service Appliance in place, but be aware that support for the MiCollab Client Service Appliance is nearing end-of-life.

- Purchase and install the Virtual MiCollab Client software package to run on a VMware-approved hardware platform.

The information below lists the server requirements:

Component	Requirement	Version
Hardware Platform	An approved Mitel Standard Linux (MSL) hardware platform.	
Operating System	Mitel Standard Linux (MSL)	Latest released version
Virtualization	VMWare® ESXi™ VMWare vSphere™	Refer to the Virtual Deployment Solutions Guide
Software Blade	MiCollab Client Service	Latest version

Note:
Virtualization: For information about installing and configuring VMware ESXi on the hardware platform, refer to the VMware documentation supplied with the product.

Communication Platforms Requirements

To use MiCollab Client , users must be configured with a desk phone, softphone, or both on one of the following Mitel communication platforms and versions:

- MiVoice Business v4.2 or later (5.0 SP2 is required for SIP softphone)
- MiVoice Office 250 v3.2 or later (5.1 is required for SIP softphone)
- MiVoice Office 400 v4.2 SP2 or later
- MiVoice 5000 v6.1 SP2 or later
- MiVoice MX-ONE v6.1 SP1 or later
- MiVoice 400 v4.1 or later

When deployed in a MiCollab environment, MiCollab Client can be integrated with MiVoice 5000 6.1 SP2 or later and MiVoice MX-ONE Release 6.0 SP2 or later. Refer to the ***MiCollab Installation Guide*** for more information.

MiCollab Client Requirements

MiCollab Client Desktop Client

MiVoice for Skype for Business

MiCollab Client Web Portal

MiCollab for Mobile for Android

MiCollab Audio, Web and Video Conferencing Collaboration Product

MiCollab UC-Client

The MiCollab Client Desktop Client provides the full suite of MiCollab Client features. To install and use the MiCollab Client Desktop Client, users must have a computer that meets the documented computer requirements .

Component	Requirement	Version
Central Processing Unit (CPU)	Dual Core, 1.6 GHz minimum	
Hard Disk Space	100 MB free hard disk space	
Random Access Memory (RAM)	2 GB minimum (4 GB or more recommended)	
Network Interface Card (NIC)	10/100/1000 Mbps full duplex required (100 Mbps full duplex recommended)	
Sound Card	Full Duplex	
Digital Media Player	Windows Media® Player	6 or later
Operating system (OS)	Microsoft Windows 7	Professional/ Enterprise/ Ultimate 32 or 64-bit
	Microsoft Windows 8, 8.1	Desktop mode only 32 or 64-bit

Component	Requirement	Version
	Microsoft Windows 10 and 11	32 or 64-bit
Microsoft Office Application(s)	Office 365	
Thin Clients	Citrix XenApp 7.13, 7.14, or 7.18 VMware View – 4.6, 5.0 (5.0 onwards supports MiCollab Client Softphone), 5.1, 5.5, or 6.5	
Remote Desktop Services (formerly Windows Terminal Services)	v6.1 (Installed as part of Windows S erver 2016 and 2019)	
Microsoft Add-on	Microsoft .NET ™ Framework	4.0, 4.5

* The thin client environment does not support the embedded softphone and video call feature.

To use the MiCollab Client embedded softphone, a USB headset or handset is required.

Supported USB handsets include:

- VoipVoice® Cyberphone 654

Supported USB headsets include (see MiCollab Client Engineering Guidelines for a complete list of Plantronics supported headsets):

- Jabra® GN 2000 USB
- Jabra GN 2100 USB
- Plantronics® CS50-USB
- Plantronics Blackwire C610

Note:
Supported Headsets and Handsets were tested with the MiCollab Client product. However, there are known limitations:

Volume adjustments made on a Plantronics headset during an active call are not reflected in the active call window.

Jabra GN 2000, 2100 and Plantronics Blackwire C610: Mute button is not functional even if configured.

Jabra GN 2000: While on an active call, the Audio does not automatically recover if the headset is unplugged and plugged back in.

Note:
Effective in MiCollab Client 6.0 SP2, when selecting Plantronics headsets under Softphone Settings (Desktop Client configuration), some functionality are pre-defined: Call Answer, Call End, Mute and Unmute.

MiCollab Client interoperates with the following software:

- **Supported Personal Information Managers**

  The following Personal Information Managers (PIMs) are supported for use with MiCollab Client :

  - Act! 2008 & 2011
  - Lotus Notes R8.0, R8.5 , 8.5.2 and 9.0
  - Outlook 2007, 2010 (32-bit & 64), 2013 (32-bit & 64),2016(32 and 64 bit)
  - Google Calendar and contact integration
- Supported Instant Messaging Applications

  The following Instant Message (IM) clients are supported for use with MiCollab Client :

  - MiVoice Skype for Business, Lync 2010, 2013

MiCollab Client integrates with Google (Calendar and Contacts), Microsoft Exchange Server, or Microsoft Graph Server.

MiVoice for Skype for Business is an application that integrates with Skype for Business and allows Skype for Business users to use Mitel telephony features through its feature rich MiCollab Client infrastructure.

The MiCollab Client Web Portal provides remote access to a subset of MiCollab Client features from one of the following supported Web browsers :

- Microsoft Edge 20
- Microsoft® Internet Explorer® (IE) 9, 10, or 11 (see note for IE9)
- Mozilla® Firefox®
- Apple® Safari 9.0 or later

- Google Chrome 46 or later

Note:
IE9 users could use the Google Chrome Frame plug-in to get real-time data and have chat, presence and call control functionality. However, the plug-in will no longer be updated and supported effective Jan 2014. The plug-in will continue to work if you already have it installed otherwise upgrade to IE10 or later to get all the functionality.

MiCollab for Mobile for Android is a stand-alone client that users install on their Android mobile phones. The client provides automatic Dynamic Status updates based on the user's current location. Location options include GPS and Bluetooth. In addition, the client provides access to call logs, messages, and Corporate Contacts.

MiCollab for Mobile for iPhone

MiCollab for Mobile for iPhone client application provides Dynamic Status updates based on time and GPS location. In addition, MiCollab for Mobile provides an integrated environment in which you can communicate with corporate contacts, and access and manage visual voice mail and call history.

When integrated with MiCollab Client , MiCollab Audio, Web and Video Conferencing (formerly known as Audio and Web Conferencing - AWC) provides users with conferencing, chat, annotation, document transfer, desktop and application sharing, and other collaboration features in real time. Collaboration is a licensed feature and must be purchased for MiCollab Client .

MiCollab UC-Client (previously known as MiCollab Mobile) is still available.

Note:
Refer to the ***MiCollab Client Engineering Guidelines*** for supported versions.

1.5 About Licensed Features

Below are the list of licensable features for MiCollab Client. Two of the features are server-level licensed features:

- **Federation**: Considered to be "in use" at all times.
- **Peering**: Considered to be "in use" at all times.

The table below provides descriptions for all licensed features.

Feature	Description
Auto Answer	Incoming calls are answered at the first ring by the selected device (Desk Phone or Softphone). Users enable and disable this feature from the Dynamic Status dialog box on the Desktop Client. **Note**: Auto Answer conflicts with the Dynamic Extension Express feature on the MiVoice Office 250 PBX. **Note**: Auto answer is not supported on SIP soft phones.
Call Forwarding	The Call Forwarding feature allows users to: • forward to any non-PRG destinations. • add preferential routing. • send calls to dynamic extensions. When users are not licensed for Call Forwarding, they can still send calls to their desk phones, softphones, and voice mail. In addition, users can set Do-Not-Disturb and Auto Answer options.
Chat	Users can participate in online chat sessions with other MiCollab Client users also licensed for chat. Users access

Feature	Description
	the **Chat** submenu from the Corporate Contacts context menu.
Collaboration Integration	Users can access MiCollab Audio, Web and Video Conferencing (formerly known as Audio and Web Conferencing - AWC) features from the **Collaboration** submenu (available from the main menu) and the **Start Collaboration** option from the Corporate Contacts context menu.
Compact Mode	Users can switch between the full mode and compact mode Desktop Client interfaces.
Console Option	Users have access to the Console from the Desktop Client main menu. The Console provides access to attendant functions such as answer, transfer, hold, and the ability to view and change another user's status. By default, console users run in Universal presence mode. **Note**: This feature must be purchased. Also, users who are licensed for the Console Option automatically have Universal Presence enabled for all local corporate contacts. This excludes contacts from peered MiCollab Client Services and external IM servers.
Desk Phone	Users' desk phone extensions, as programmed on the PBX, are integrated with MiCollab Client.

Feature	Description
	Note: This feature must be purchased. Also, purchasing x licenses of this features automatically provides x number of all of the non-purchasable features.
Desktop client SDK	This license is required for MiVoice for Skype for Business feature. **Note**: MiVoice for Skype for Business Deskphone only users: those users only require the Desktop client SDK feature. MiVoice for Skype for Business Softphone only users OR those users with a Softphone and an associated Deskphone will require the Softphone feature in addition to the Desktop client SDK feature.
Do-Not-Disturb (DND)	Users can enable and disable DND for each type of Dynamic Status. When DND is enabled, callers receive a busy tone and a Do-Not-Disturb message and incoming calls are not logged in the call log. Users enable and disable this feature from the Dynamic Status dialog box on the Desktop Client.
Dynamic Status	Users can add statuses and configure the following Dynamic Status elements:

Feature	Description
	• Status Name (for example, **In the office** or **Gone for the day**) • Optional custom text • Instant Message availability and auto reply • Preferential Routing • Phone Settings (DND and Auto Answer) Users can manually change their Dynamic Status at any time using the MiCollab Client interface. The new status is then communicated to other MiCollab Client users. In addition, Dynamic Status is also automatically updated in response to the user's Outlook calendar entries. **Note**: This feature must be purchased.
External Dial	Users can dial an external number from an integrated application such as Microsoft Word, Outlook, and Internet Explorer. The user may need to complete some configuration in the application to enable external dialing.
Federation	The Federation feature provides MiCollab Client users with expanded IM capabilities. When the MiCollab Client Service is licensed for this feature, you can configure federation for the Enterprise on the Federation Tab, and users can view IM presence and chat with federated IM contacts using the Desktop Client's Chat window.

Feature	Description
	Note: This feature must be purchased and is a server-level license. Therefore, it will not appear in any feature profiles. Also, MiCollab Client 4.0 IM server support is limited to Microsoft Office Communicator Server (OCS) 2005, and 2007 R2, and IBM Lotus Sametime Server 8.5 and 8.5.1.
Knowledge Management	Users can index computer files and documents associated with a contact. When the user receives and incoming call, the Knowledge Management popup window appears presenting the user with a list of files associated with the caller including e-mail messages, contact entries, and documents (Microsoft Word, Excel ® PowerPoint ® , Outlook and Adobe ® Portable Document Format).
Launchpad	Users can access the Launchpad view, which provides quick access to frequently completed actions, from their Desktop Client. Actions include dialing a number, browsing to a URL, running a program, and exploring a folder.
Mobile Handoff	Users on Mobile device can use the Call Handoff feature (ability to push a call to other devices within the Personal Ring Group). This feature is limited to users on MiVoice Business communication platforms only.

Feature	Description
	Note: **Handoff Feature Code**: As a prerequisite, the MiVoice Business Feature Code for Handoff must be programmed. If this feature is added to an existing server, the PBX need to be synchronized with MiCollab Client before the feature can be used (also see Synchronization Tab).
Mobile SIP Softphone	Allows user to have SIP-Based Softphone on Android and iOS clients. This feature is supported on MiVoice Office 250 and MiVoice Business systems only (MiVoice Business 5.0 SP2 and later release). **Note**: You must have the " MiCollab Mobile Client for Smart Devices" license enabled before you can enable the "Mobile SIP Softphone" license.
Office Communicator Integration	Users can send and receive instant messages using the Microsoft Office Communicator IM client, from the Desktop Client. Similar to the Chat feature, users can access the Office Communicator submenu from the Contacts context menu.
Peering	The Peering licensed feature allows you to configure communication paths with other MiCollab Client Services for the purposes of sharing presence information and providing communication features between Enterprises.

Feature	Description
	Note: This feature must be purchased and is a server-level license. Therefore, it will not appear in any feature profiles.
Phone Button Programming	Users can configure the buttons on their IP phone from the Mitel Integrated Configuration Wizard. This feature is limited to users on MiVoice Business communication platforms only.
Presence	MiCollab Client Service uses **Dynamic Presence** (which is a replacement for Universal and On-Demand Presence) for telephony presence. The Desktop client will display presence for the contacts in the current view. **Note**: Console users will see presence information for all your corporate contacts. **Note**: An account with a Deskphone, Softphone, Stand-alone Web Portal, or Mobile Client for Smart Devices license has telephone presence even when the Presence feature is not selected in the feature profile.

Feature	Description
Presence on Mitel Sets	Users can configure presence information for multiple contacts on their Desktop Client. This feature is limited to users on MiVoice Business communication platforms only.
Presence on Mitel InAttend	InAttend Users can view presence* information for contacts associated with MiCollab Client. **Note**: This feature is limited to users on MiVoice MX-ONE and MiVoice 5000 communication platforms only.
Softphone	Users' softphone extensions, as programmed on the PBX, are integrated with MiCollab Client. **Note**: This feature must be purchased.
Stand-alone Mobile Web Portal	The Mobile Web Portal provides users with remote access to a subset of MiCollab Client features, such as configure and change their Dynamic Status, access call history data, view corporate contacts, access voice mail messages, and configure account options.
Stand-alone Web Portal	The Web Portal provides users with remote access to a subset of MiCollab Client features, such as configure and change their Dynamic Status, access call

Feature	Description
	history data, view corporate contacts, access voice mail messages, and configure account options.
MiCollab Mobile Client for Smart Devices	Users can install and use the MiCollab Mobile Client application on their Android, iPad, or iPhone mobile device. The MiCollab Mobile Client application provides Dynamic status updates based on location, time, WiFi, GPS and/or Bluetooth (depending on the device). The application also provides an integrated environment in which users can manage Dynamic Status, communicate with corporate contacts, and access visual voice mail and call history. The MiCollab Mobile Client for Smart Devices was formally known as the Locator.
Video Calls	Users have access to video presence for Corporate Contacts and can participate in point-to-point and multi-party video sessions. Video services for the MiCollab Client Desktop Client are provided by Mitel MiCollab Audio, Web and Video Conferencing.
Visual Voice Mail	Users have access to the following NuPoint UM voice mail features from the Visual Voice Mail view: • Receive message waiting indications • Play, forward, and delete voice mail messages • View, forward, and delete fax messages • Change the voice mail PIN

Feature	Description
	Note: This feature requires the user's mailbox to be configured on the NuPoint UM voice mail system.

* MiCollab Telephony Presence is not supported in InAttend.

1.6 Teamwork Mode

Teamwork Mode provides the ability for a user to have certain MiCollab Client functions without having a Mitel phone. In other words, a user will still be able to use certain non-telephony based features within the client even though the user does not have a desk phone or softphone.

Note:
Prior to release 5.1, a MiCollab Client user without any devices online and a hot desk user that was not logged in would go into offline mode. However, as of MiCollab Client 5.1 if the user has no devices associated with their account, they automatically go into Teamwork Mode.

Licensing: There are no new or additional licenses required specific to the Teamwork Mode feature. Licenses for individual features such as Chat, Visual Voicemail, etc...are still required.

1.7 Administrator Tasks

The MiCollab Client system includes several different components and functions. The system must be properly configured and maintained to ensure that users are provided with the features and functions available in the product.

As the MiCollab Client Administrator, your responsibilities include the following:

- Provisioning MiCollab Client
- Maintaining MiCollab Client

- Troubleshooting MiCollab Client

1.7.1 Provisioning MiCollab Client

After you install and configure the MiCollab Client blade on the MSL server, you must provision the MiCollab Client system using the MiCollab Client Service administrator interface.

Follow the steps below, in order, to provision the MiCollab Client system using the MiCollab Client Service administrator interface:

1. Create an Enterprise.
2. Add Feature Profiles.
3. Add PBX nodes.
4. Add collaboration servers (*optional*).

> **Note**:
> The Unified Communicator Express/YA Collaboration Module is no longer a supported collaboration product for MiCollab Client .

5. Configure the Enterprise fields and options.
6. Add user accounts using one of the following methods:
   - Add user accounts automatically by configuring an AD/LDAP Synchronizer, and then completing a manual synchronization. Refer to the Licensed Features and Synchronization topic for details.
   - Add user accounts automatically by configuring a PBX Node Synchronizer, and then completing a manual synchronization. Refer to the Licensed Features and Synchronization topic for details.
   - Add user accounts manually by clicking Add Account from the Accounts tab. Accounts that you create manually are not affected if you later configure an AD/LDAP or PBX Node Synchronizer and then complete a synchronization.
7. Configure Automatic Call Distribution (ACD) settings (*optional*).
8. Configure Peering with other MiCollab Client Services or external servers (*optional*).
9. Configure IM and presence Federation (*optional*).
   - When you configure federation from the Peering tab, federated contacts are displayed in a separate list in the user's corporate directory from the Desktop Client's Contacts View.
   - When you configure federation from the Federation tab, instruct users to manually add the federated contacts to the Desktop Client. Users should create

a new personal contact, and then add the IM login information (for example, john_smith@ocs.com) for the contact using the **MiCollab Client Login** option.

10. Send a Welcome E-mail Message to MiCollab Client users.

The procedure above covers the configuration required in the MiCollab Client Service Administrator Interface ***only*** . It ***does not*** cover the additional configuration required at the site. Click here to read more.

The MiCollab Client product is integrated with the site's communication platform and network. In addition, this product can be integrated with other Mitel applications. Therefore, configuring and deploying the entire system requires access to network and telephone equipment, communication system software, and peripheral software products. The entire deployment process involves the following high-level tasks:

1. Configure the PBX for MiCollab Client .
2. Install and configure the integrated Mitel applications.
3. Install and/or configure the MiCollab Client Service component. (Procedure varies based on MiCollab Client Service deployment type.)
4. Access the MiCollab Client Service Administration page.
5. Provision MiCollab Client as documented in this topic.
6. Install MiCollab Client software.
7. Configure access for remote users.

For comprehensive information about all of the tasks required for MiCollab Client deployments, refer to the ***MiCollab Client Administrator Guide***, available on the Mitel Document Center Web site.

1.7.2 Maintaining MiCollab Client

MiCollab Client administrator maintenance tasks are described briefly below. For comprehensive maintenance information, refer to the ***MiCollab Client Administrator Guide*** available on the Mitel Document Center Web site.

Server and Client Upgrades

To upgrade MiCollab Client , download and install a new MiCollab Client Service software blade. The blade contains the client software `.msi` file. This file must be deployed to users to complete the upgrade.

MiCollab Client Service Administration

To access the MiCollab Client Service Administration page, click **MiCollab Client Service** under Applications in the MSL Server Manager navigation panel. This page provides access to MiCollab Client Service administrator tasks.

MSL Server Manager Administration

The MSL Server Manager Administration menu provides options for the following server-related tasks :

- **Backup**: Performs a backup of the MSL server (and MiCollab) data.
- **View log files**: Allows you to view log files. Select a log file from the Choose a log file to view list, and then click **Next**.
- **Event viewer**: Shows the current alarm state for the system, followed by a number of events recorded depending on the current age setting for the page.
- **System information**: Allows you to set access privileges to the system information about your server. After enabling the service, click the link to view the information.
- **System monitoring**: Allows you to view monitoring graphs, which can help you analyze the system's performance.
- **System users**: Allows you to add, modify, or remove administrator users for the server.
- **Shutdown or reconfigure**: Allows you to reboot the server, shut down the server, or perform a full system reconfiguration.

Note:
These tasks are covered in the *Mitel Standard Linux Installation and Administration Guide,* available on the Mitel Document Center Web site.

1.7.3 Troubleshooting MiCollab Client

MiCollab Client includes various error messages, utilities, and logs to help troubleshoot issues. All the available troubleshooting information for MiCollab Client , including Calendar Integration troubleshooting, is documented in the Troubleshooting chapter of the *MiCollab Client Administrator Guide*.

If you encounter a problem with the product, you can download this document from the Mitel Document Center Web site and troubleshoot the issue.

If you cannot resolve the issue yourself, contact Mitel Technical Support for assistance.

1.7.4 Contacting Technical Support

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

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

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

1.8 The Administrator Interface

1.8.1 Enterprise Tab

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web and Mobile Portal users (see table for details).

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab-integrated mode.

The Enterprise tab includes fields and options for the Enterprise or company.

The first step to provisioning MiCollab Client is to create an Enterprise. Click **Create Enterprise**.

After you have created an Enterprise, select it from the list box and then configure the fields and options for the Enterprise from the following areas.

Settings

The **Settings** area includes fields for specifying basic Enterprise information.

Note:
You cannot change this field after you create the Enterprise if PBX nodes have been defined. Once PBX nodes have been defined, this field cannot be deleted unless all PBX nodes are deleted first.

To configure Enterprise Settings:

1. If required, edit the following Enterprise settings:

   - **Description**: (Required) Type a description for the Enterprise, for example, **Acme Company-Phoenix Arizona**. By default this field is blank. The Enterprise Description:
     - is limited to 1-128 characters in length.
     - must contain alpha-numeric characters (dashes included).
     - cannot contain vertical bars (|).
   - **Enterprise domain**: (*Required*) Type a domain for the Enterprise. The Enterprise domain does not need to be a resolvable DNS name or a registered domain name, however, it does need to follow the DNS suffix format. The Enterprise domain should be unique to the Enterprise so that peered servers do not have the same Enterprise domain. Mitel suggests using the site location or Enterprise ID as part of the Enterprise domain (for example, **Phoenix.xyzcompany.com**, where **Phoenix** is the Enterprise ID).
   - **Voice mail server**: (*Optional*)
     - When **NuPoint** is selected, the Voicemail server field displays the FQDN of the NuPoint server. The field is "read-only" in this case.
     - When **Embedded** is selected, the Voicemail server field is hidden.
     - When **MiCollab Advanced Messaging** is selected, the Voicemail server field is enabled and administrator needs to provide the URL for the clients accessing MiCollab Advanced Messaging Web Client.

       MiCollab Advanced Messaging (MAM) integration

       The integration of MiCollab Advanced Messaging provides the user access to the responsive Web-interface for managing Voicemails.

       The user needs to provide the credentials to the MiCollab Advanced Messaging Web Client on MiCollab Clients. The credentials to access MiCollab Advanced

Messaging are not stored by the MiCollab Client but cached by the web interface (depending on user's browser settings on the device).

Precondition:

- The user needs to have a valid Visual Voicemail license.
- The server hosting for MiCollab Advanced Messaging must have a valid, trusted certificate. Refer to the MiCollab Advanced Messaging documentation for details.
- The MiCollab Advanced Messaging Web Client should be enabled for HTTPS and have a valid trusted certificate.
- For PBX platforms that supports MiCollab Advanced Messaging. Refer to the *MiCollab Client Administrator Guide > Table 20: Voice Mail Server Types*.
- The MiCollab Advanced Messaging must have the MiCollab Advanced Messaging Web Client installed.

Note:
The MAM Client URL should be resolvable and accessible from the internet when the MiCollab Client will be used outside on the local LAN.

Enabling MiCollab Advanced Messaging for a new MiCollab installation

The type of Voicemail for the installation needs to be selected in the Server Manager on the following page: MiCollab Client Service > Configure MiCollab Client Service > Enterprise > Settings > Voice mail server type.

Enabling MiCollab Advanced Messaging for an existing MiCollab installation

An existing MiCollab user will not get the new roles/templates automatically when upgraded to MiCollab 8.0. The admin must manually create the role/template to remove NuPoint and to change the MiCollab Client feature profile. This is required to let the clients show the MiCollab Advanced Messaging in the Voicemail tab.

- **Administrator e-mail**: (*Optional*) Type the e-mail address for the MiCollab Client Service administrator. An e-mail message is sent to this address when On-Demand presence is enforced. The maximum length for this field is 255 characters.
- **Switch type**: This field is editable when there are no PBX nodes defined on the PBX nodes tab. Once the Switch type field is set, all PBX Nodes created will be that

type. After a PBX Node is created, the Switch type field cannot be changed unless all PBX Nodes are deleted.

When creating a new enterprise that will not have any PBX nodes and only have Teamwork Mode accounts, the switch type can be left at the default value of “Mitel Communications Director” (the value will be ignored).

- **Collaboration server type**: (*Optional*) Select a collaboration server to use with MiCollab Client. Options include:

  - None (default)
  - MiCollab Audio, Web and Video Conferencing

  If you do not intend to use collaboration features, set this field to **None** (default). If you have already added and configured a collaboration server, you cannot configure the option here.

> **Note**:
> The Mitel Your Assistant Collaboration Module is no longer supported as a collaboration server type. Refer to the Collaboration tab topic for more information.

- **Avatar URL**: To enable MiCollab Avatars for Aquarius 69xx Sets (6920, 6930 and 6940), configure the Avatar URL displayed in this field on MiVoice Business in Online Services URL Form.
- **Language**: (*Required*) Select a language for the Enterprise from the list. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. The user's language setting determines which language the Welcome E-mail Message is generated in for that user.
- **Time zone**: (*Required*) Select the time zone where the Unified Communications server is physically located from the list box. The time zone where the Unified Communications server is located may be different than the time zone where the Enterprise is located.

2. Click **Apply** to save the information, or click **Reset** to clear your changes.

Calendar Integration

This feature enables the MiCollab Client administrator to configure either a Google Server, Office 365, or an Exchange Server from which the MiCollab Clients can

fetch calendar availability information and update their Dynamic Statuses. Exchange Integration supports Exchange 2013, Exchange 2016, and Exchange 2019.

From the Calendar Type drop-down menu, select **Google, Office 365,** or **MS Exchange**.

Some of the user permissions that are mandatory are as follows:

1. When Calendar Integration is done with Office 365 using OAuth 2.0:

   - API Permissions - The Office 365 administrator has to grant **full_access_as_app** application permissions for Office 365 Exchange Online API.
   - URL Access required - Client's firewall should allow the URL's mentioned below:

     - **outlook.office365.com** - Access for URL *outlook.office365.com* is also required when Calendar Integration is done with Office 365 using Basic authentication
     - **login.microsoftonline.com**

   If you want to **enable calendar integration**, click the checkbox.
2. When Calendar Integration is done with Office 365 using OAuth 2.0 (Microsoft Graph):

- API Permissions - The Office 365 administrator must grant following API permissions from Microsoft Graph:

  Delegated Permissions:

  - Calendars.Read
  - Calendars.Read.Shared
  - Calendars.ReadWrite
  - Calendars.ReadWrite.Shared

  Application Permissions:

  - Calendars.Read
  - Calendars.ReadWrite
- URL Access Required - Client's firewall should allow the URL's mentioned below:
- **login.microsoftonline.com**
- **graph.microsoft.com**

Note:

If permissions are not given and test connection is performed, the administrator may get the error message:

"***Invalid calendar server credentials.: Invalid credentials.***"

To overcome this, the administrator must provide the API permissions mentioned above.

If MS Exchange or Office 365 is selected then: (if Google is selected go to step 4)

1. Enter the URL of your Exchange Server. The URL corresponds to Exchange Web Services (EWS). The exact URL depends on how your exchange server is configured but is usually in the format ***https://<hostname>/EWS/exchange.asmx***. For Office 365, refer to https://outlook.office365.com/ews/exchange.asmx.
2. The version of the Exchange Server is entered automatically when you successfully test the connection.

Note:

When connecting to a 2010 SP3 Exchange Server, the version may still be shown as SP2 on the MiCollab Client server-manager.

3. Enter the username and password that you use to log into the Exchange Server. This user does not necessarily have to have administrative privileges on the Exchange Server. Any user who can view other users' calendar availability information will suffice. If you are unsure what to enter here, contact your Exchange Server administrator.

   a. If you want to use Impersonation, select the appropriate radio button. If Impersonation is enabled, then MiCollab Client users will not have to provide their

exchange password to use Calendar Integration. However, they still have to provide their Exchange username and primary e-mail address

b. Enabling Impersonation can have security implications and requires administrative privileges on the Exchange Server.

c. If you want to use Delegation, select the appropriate radio button.

Refer to the following Microsoft websites for more details on Microsoft Exchange version details:

Note:
Exchange 2019: https://docs.microsoft.com/en-us/Exchange/new-features/new-features?view=exchserver-2019

Settings required on Exchange Server for MiCollab Meeting Center

- Exchange Subscription Type selected as Impersonation or Delegation.
- For Impersonation, users need to have ApplicationImpersonation as Management Role and Access Rights as LimitedDetails.
- For Delegation, users need to have Access Rights as LimitedDetails.

Use following command to change Management Role on Exchange Management Shell, where serviceAccount is username: New-ManagementRoleAssignment –Name:impersonationAssignmentName –Role:ApplicationImpersonation –User:serviceAccount

Use following command to change Access Rights on Exchange Management Shell: Add-MailboxFolderPermission -Identity user1@mitel.com:\Calendar -User user2@mitel.com -AccessRights LimitedDetails

where,

- user1: user ID of the mailbox or calendar you want to get access to.
- user2: user ID of the service account you use or configure on Admin portal.

Note:
Only Basic Authentication is supported on MiCollab while communicating with the Exchange Server.

4. You can access the Advanced Calendar Integration Settings. The default values for these settings works appropriately under most circumstances so normally, these do not need to be adjusted. Change them only if you have very particular needs, such as high network latency. Be aware that changing these values affects calendar integration across ALL enterprises.
5. Test your connection to ensure that MiCollab Client can connect to either the Google Server or Exchange Server and communicate with it properly. If after clicking on the **Test Connection** button you receive an error stating "**Invalid calendar server credentials**", you need to troubleshoot the issue.
6. Click **Apply** to save the changes or **Reset** to clear the changes.

Calendar Integration for Office 365

The authentication protocol for Calendar Integration with Office365 can be either Open Standard for Authentication 2.0 (OAuth 2.0), OAuth 2.0 (Microsoft Graph), or Basic Authentication protocol.

Basic Authentication mechanism is a process where the username and password are provided for authentication purposes, whereas in case of OAuth 2.0 tokens are being used for authorization.

OAuth 2.0 (Microsoft Graph) also uses the OAuth 2.0 tokens, with the difference being, instead of Exchange it uses Microsoft Graph Server APIs to fetch the calendar details.

Pre-requisites

- To use OAuth 2.0, an application must have an application ID issued by Azure Active Directory. On the **Request API** page, select **Exchange** under **Supported Legacy APIs** followed by **Application Permissions** and then select **full_access_as_app.** Then click **Add Permissions.**

  For more details on configuration, refer to **Configuration > Cloud Service Provider section.**

Note:
In case of any changes in API permission from Microsoft Graph and EWS OAuth2.0 in Office 365, the same will be reflected in MiCollab after 60 minutes.

To use OAuth 2.0 (Microsoft Graph), an application must have an application ID issued by Azure Active Directory. On the **API Permissions** page, select **Microsoft Graph** then **Delegated Permissions** and give **Calendars.Read, Calendars.Read.Shared, Calendars.ReadWrite, Calendars.ReadWrite.Shared**permissionsfollowed by **Application Permissions** with **Calendars.Read**, **Calendars.ReadWrite** permissions. Then click **Add Permissions**and**Grant Admin consent**

Once the configuration under Cloud Service Provider is successful, the MiCollab Administrator can enable Calendar integration from MiCollab Client Services.

Perform the following steps under MiCollab Client Services:

1. Navigate to the **Applications** > **MiCollab Client Service** > **Enterprise**.
2. Under **Calendar Integration**, select the **Calendar Type** as **MS Office365**.
3. The administrator can select the **Authentication Protocol** for Office 365 as:

   - Basic,
   - OAuth 2.0, or
   - OAuth 2.0 (Microsoft Graph)

   In order to enable OAuth 2.0 or OAuth 2.0 (Microsoft Graph), the administrator must select the respective Authentication Protocol's radio button.
4. For Exchange Subscription Type:

   - the default option selected is **Impersonation**, if **OAuth 2.0** is selected as Authentication Protocol. It will be applicable for all 9.2 servers including the new deployed and upgraded servers.
   - the default option selected is Impersonation, if OAuth 2.0 (Microsoft Graph) is selected as Authentication Protocol. It will be applicable for all 9.6 servers including the new deployed and upgraded servers

Note:
The default Authentication Protocol would be selected as Basic

Note:
After a backup restore, the client credentials will not be part of the MiCollab backup. Therefore, the admin must reconfigure OAuth 2.0 settings at Cloud Service Provider section and then enable Calendar Integration.

Note:

Default subscription type is not supported in Calendar Integration for Office 365 with OAuth 2.0 Authentication Protocol.

In the Default subscription type, the MiCollab users have to provide their Exchange or Office 365 password from the client (Web, PC, or Mobile client) to use Calendar Integration.

Default subscription type is not supported in Calendar Integration for Office 365 with OAuth 2.0 (Microsoft Graph) Authentication Protocol.

For more information on different calendar sharing options, refer to the following Microsoft links:

- Outlook
- Outlook Web Access

Trusted Servers

This area provides a table of trusted servers for MiCollab Client. After you configure peering with one or more MiCollab Client Services, they are automatically added to this table.

Note:
If the peered server IP address is changed, add or edit the IP address in the **Trusted Server Details** page, to view the presence state of the users.

The table includes three columns:

- **Description**: Indicates the description you provide for the trusted server.to
- **IP address/hostname**: Indicates the server's IP address or hostname.
- **Type**: Indicates one of the following trusted server types:
- *Presence Proxy*: Presence proxy servers are required to provide presence information such as status and login notification to remote users. If you do not have any remote users (all users are located at the site where the Unified Communications server is located), you do not need to add presence proxy servers.
- *IM*: An IM trusted server provides Instant Messaging presence to MiCollab Client users on the local Enterprise.
- *Peer*: A peer trusted server provides presence information for corporate contacts on peered MiCollab Client Services.

You can complete the following tasks for trusted servers:

- Click the **Add Server** link to add a new trusted server.
- Click the **server name link** to edit the corporate location.
- Delete a trusted server.

  If you delete a peered server, you can also delete it as a trusted server, as part of your cleanup activities.

  To delete a trusted server:

  1. Select the server you want to delete from the Trusted Servers table.
  2. Click the **Delete Server** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the server, or click **Cancel** to cancel the deletion.

Launchpad Settings

The Launchpad is an area on the MiCollab Client Desktop Client interface where the user can quickly navigate to a URL, dial a phone number, run a program, or explore a folder. The Launchpad entries that you configure here apply to every user that is licensed for the Launchpad feature.

This area of the Enterprise tab provides a table that lists the Launchpad entries you add for MiCollab Client . The table includes three columns:

- **Label**: Indicates the label or description that you provide for Launchpad entry.
- **Action**: Indicates what occurs when the user accesses the Launchpad item. There are two actions that you can configure for the user: **Dial a number**, and **Browse to a URL**.
- **Value**: Indicates the phone number or URL that corresponds to the action you selected.

You can Add, **Edit**, and **Delete** Launchpad entries. Any changes you make to Launchpad settings will not be shown in the Desktop Client until the user restarts the client.

USB Devices

The MiCollab Client Desktop Client supports several headsets and handsets (see list under Requirements).

To use a USB device with MiCollab Client , users must create a USB device profile using the MiCollab Client Desktop Client. If the user's account includes the **User can manage USB device profiles** option (Account Details Page – Account Settings – **USB Devices**), he or she can upload the profile to the Unified Communications server.

The USB devices displayed in this area include the device information from the profiles created and uploaded by users. The device information is read-only and cannot be edited. You can however, **Sort** the information and **Delete** USB devices from the server.

Plus Dialing Settings

This area of the Enterprise tab includes fields for specifying plus dialing settings.

Note:
Starting with MiCollab Client 5.1, some of the dialed digit processing happens locally within MiCollab Client. Due to this, if some dialing settings are changed in the server-manager, all clients within that enterprise (or for that PBX) should be restarted. Following are the settings affected by this:

- At the enterprise level:
  - Plus Dialing settings -> Country code
  - Plus Dialing settings -> International access code
  - Plus Dialing settings -> Long distance access code

- At the PBX Node details level:
  - Plus Dialing settings -> Country code
  - Plus Dialing settings -> International access code
  - Plus Dialing settings -> Long distance access code
  - Extension length
  - Dialing prefix

The plus dialing settings include:

- **Country code**: This field should be set to the country code of the country where the PBX resides. If an E.164 call is placed to a number within the user's "home" country, the country code will be stripped off of the digit string by MiCollab Client .
- **International access code**: This field indicates the international dial code that must be dialed for international calls from the country where the PBX resides. If the MiCollab Client determines that the call is being placed outside of the user's country (based on the PBX country code), MiCollab Client will pre-pend the International Prefix.
- **Long distance access code**: This field indicates the Toll digit for the country where the user's PBX resides. For any E.164 dialed calls within the user's home country, MiCollab Client will prepend the toll digit.

Note:
It is important that sites using E.164 (plus dialing) settings set up ARS on the PBXs to strip the Toll Digit for local calls.

Note:
During an avatar search, the CLID translation string is stripped off from the directory number.

CLID Translation

CLID Translation: For more details on this field, please refer to the help for CLID translation field in the PBX Node Details page.

Note:
If CLID Translation is explicitly specified at the PBX node level, that setting will override the CLID Translation setting at the enterprise level.

Default Account Settings

This area of the Enterprise tab includes the default values that will apply to MiCollab Client accounts when they are created. The values you configure here apply to all accounts whether you create them manually (Adding and Editing Accounts), or you create them automatically by configuring an AD/LDAP or PBX Node synchronizer (Synchronization tab).

If required, you can edit the values for any account from the Account Details page.

To configure default account settings:

1. Configure the account **Login Settings**:

   - **Country**: Select the country that the MiCollab Client users reside in. By default, this option is set to United States.
   - **PBX node**: Select the PBX node that services users from the list box. The list includes all the PBX nodes you have configured on the PBX Nodes tab. If you have not configured PBX Nodes yet, the list box is empty.
   - **Account code length**: Account codes provide a way to track phone usage. Select the account code length from the list box. Options include 0-12. You can configure account code details on the ACD Settings tab.

     - *Enable ACD features in client*: Select this option to provide users with Automatic Call Distribution (ACD) features in the MiCollab Client Desktop Client.
     - *Allow user to upload display picture*: Determines if users can upload their own display picture from the Desktop Client.
     - *Allow picture download support for Previous Clients (unsecure)*: Allows users to download *picture for previous MiCollab Clients.*
     - *Enable E911 Warning*: Displays a warning whenever the user launches the softphone client. The warning states that the softphone may not be able make

calls to the appropriate emergency 911 public safety authorities in some locations. By default, this option is enabled.

- *Enable Self Deployment*: Allows the user to self-deploy MiCollab Client.
- *Provision new MiCollab Client for PC*: Select to provision MiCollab Client for PC for all users under the Enterprise. By default, this option is disabled.
- Enable TLS certificate validation for legacy clients: Select to enable validation of TLS certificate for legacy clients. By default, this option is disabled.

- **Sort Order**: Select the order type you want for displaying the names on MiCollab Clients.

  - Select **First Name** to display the contacts' first name in the directory and search results. By default, **First Name** is selected as sort order.
  - Select **Last Name** to display the contacts' last name in the directory and search results.

Note:
Changing the sort order value at server will not impact the setting of existing users. Sort order value of server will come into effect only for new users.

Note:
If an existing server is upgraded to include this setting, the server will have default value as First Name. It will not have any impact on the Client setting.

Note:
If the sorting value is changed to Last Name, this value will persist even after the upgrade or on restoring backups.

- **Auto Upgrade Client**: Auto upgrade client provides an option to control the automatic client upgrades.
  - Select **Enable** to push the client upgrade popup notification (if there is a new version of the client available) for all users under the Enterprise (provided that **Default**or **Enable** is set in **Accounts** > **Account Settings**). By default, this option is enabled. The users will get a client upgrade pop-up notification.
  - Select **Disable** to disable the client upgrade notification for all users under the Enterprise (provided that **Enable** is not set in **Accounts** > **Account Settings**).
- **Corporate Directory Settings**:
  - Download limit
- The (Really Simple Syndication) **RSS Window** is an optional embedded window that provides RSS feeds from a selected URL to the user's Legacy Desktop Client. Configure the following **RSS Window** settings:
  - *URL*: Type the URL to use as the default RSS Window location.
  - *Always on*: Select this option if you want the RSS Window to always appear on the user's Desktop Client.
  - *User modifiable*: Select this option if you want to allow users to change the default URL.
- Select a **Collaboration Server** from the list. The list includes all the collaboration servers you have configured on the Collaboration tab. If you have not configured collaboration servers yet, this field displays the message, "No collaboration servers defined."
- If desired, enable the **Users can manage MiCollab corporate locations**. This field allows users to manage Corporate Locations from their MiCollab Mobile Client and upload the information to the MiCollab Client Service . By default, this option is disabled.
- The MiCollab Client Desktop Client supports various Universal Serial Bus (USB) devices. Configure account **USB Devices** options:
  - *User can configure local USB devices*: Select this option to allow users to configure USB devices in the MiCollab Client Desktop Client.
  - *User can manage USB device profiles*: Select this option to allow users to manage (upload, edit, delete) USB device profiles on the Unified Communications server

from their desktop client. When you enable this option, the *User can configure local USB devices* option is automatically enabled.

2. Click **Apply** to save the information, or click **Reset** to clear your changes.

Corporate Locations

This area of the Enterprise tab allows you to manage corporate locations for use on the MiCollab Client Mobile client. The corporate locations table includes the following information:

- **Name**: The name that you provided for the location.
- **Radius**: The circular area surrounding the location.
- **Latitude**: The latitude of the location.
- **Longitude**: The longitude of the location.

You can complete the following tasks for corporate locations:

- Click the Add Location link to add a new corporate location.
- Click the **location name link** to edit the corporate location.
- Click  to show the corporate location on Google Maps ™ .
- Delete a corporate location. **To delete a corporate location:**

1. Select the corporate location that you want to delete from the table.
2. Click the **Delete Location** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the server, or click **Cancel** to cancel the deletion.

Call Log Settings

This field allows the option to **Show Missed Calls for Key Line**. Once enabled, the Call History will display missed calls for key line numbers.

This feature is disabled by default.

To enable the Centralized Call History feature for MX-ONE, refer to **Adding and Editing PBX Nodes** > **Subscribing Centralized Call History from MiVoice MX-ONE** section for more details.

Reset Password Settings

When this option is enabled, clients are required to change their password on initial login. This option is enabled by default.

Note:
The Reset Password setting works only for legacy desktop clients.

External Ldap Search Settings

External Ldap Search Settings is used to enable external search feature at the Enterprise level. To enable/disable external LDAP search:

1. Tick the **External Ldap Search Settings** checkbox. By default, this checkbox is disabled. Similarly, uncheck the checkbox to disable the external LDP search.
2. Click **Apply** to save the information.

Jetty Configuration Settings

To enable/disable the jetty process:

1. Tick the **Enable Jetty Process** checkbox. By default, this checkbox is enabled. Similarly, uncheck the checkbox to disable the jetty process.
2. Click **Apply** to save the information.

MiTeam Classic Configuration

Check to enable MiTeam Classic. MiTeam Classic provides Cloud-based collaboration features for UCC Premium users. Note that MiTeam Classic is only supported for MiCollab Client in Integrated mode. Refer to the ***MiCollab Client Administrator Guide*** for MiTeam Classic integration requirements.

Email Notification Settings

The textbox contains the default **from** email address for sending notifications mails. The default value is uca.no.reply@<servername>.<domain name>.

The address can be changed so that emails will be sent from the updated email address.

Presence Privacy Configuration Settings

This setting controls whether the user's presence information (dynamic status, telephony status, video availability, and calendar advisory) is displayed to other users or not. The user's IM availability is not controlled by this setting.

Presence Privacy Service: By default this setting is **Disabled**.

- Set the **Presence Privacy Service** value to **Disabled** to disable the presence privacy feature.
- Set the **Presence Privacy Service** value to **Enabled** to enable the presence privacy feature.

Show Presence for all users: This setting is only available if **Presence Privacy Service** is **Enabled**. By default the **Show Presence for all users** setting is checked.

- If this setting is checked, the presence information of users on local and peered servers is displayed.
- If this setting is unchecked, no presence is shown to users on local and peered servers unless they are added in the presence allowed list of the user.

Limitations

- The server will not send updated presence packet on toggling presence **Presence Privacy Service** setting at the server. Presence will be updated only when there is change in the presence status or when the user logs out and then logs in.
- **Presence Privacy Service** is not supported in Co-located mode.
- On peered servers, the Presence Privacy setting at the local server will be given preference. For example, if the setting on peered server A is **Enabled** and the setting on peered server B is **Disabled**, peered user's presence will be displayed based on the local server setting and not the server where the user actually exists.
- Telephony presence status of other users does not turn off immediately. The user must re-login to the client. When user is re-logged into the client, telephony presence will turn off from corporate directory, call history, search tab, and from legacy console.
- Video call functionality will not work for users when the presence privacy setting is enabled.

Note:
After you create an Enterprise, you cannot edit the **Enterprise ID** field. However, you can delete the Enterprise and start over.

You can also do the following from this page:

- Click the Add an Enterprise link to create a new Enterprise.

- Click the Delete This Enterprise link to delete an Enterprise.

To delete an Enterprise:

1. Select the Enterprise from the list box.
2. Click the **Delete this Enterprise** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the Enterprise, or click **Cancel** to cancel the deletion.

1.8.1.1 Adding and Editing Corporate Locations

You can add and edit corporate locations for use on the MiCollab Mobile Client if you know the latitude and longitude coordinates for the location.

Note:
You can obtain longitude and latitude coordinates from Google Maps ™ if you log into your iGoogle account. Google Maps provides tools to account holders that display latitude and longitude coordinates as a tooltip and mark the coordinates for a specified location.

The MiCollab Mobile Client displays the corporate location in the client interface. Users can then associate the corporate location with one of their Dynamic Statuses. Then, when users enter the corporate location, the MiCollab Mobile Client automatically updates their Dynamic Status.

To add or edit a corporate location:

1. Type a **Name** for the corporate location. The Name is limited to 32 characters in length and must contain alpha-numeric characters, dashes, and/or spaces.
2. Type the **Radius** for the corporate location and then select feet or meters. The radius is the circle that surrounds the location. The default radius is 1000 feet.
3. Type the **Latitude** of the location. Latitude is limited to 16 characters in length, including numeric characters, the minus sign (-) and period (.). The valid range is -90.0 to 90.0.
4. Type the **Longitude** of the location. Longitude is limited to 16 characters in length, including numeric characters, the minus sign (-) and period (.). The valid range is -90.0 to 90.0.
5. Click **Create** or **Save**. You are returned to the Enterprise Tab.

After you create Corporate Locations, you can edit the associated fields at any time.

Note:
MiCollab Mobile Client users must restart the client to see recently-added corporate locations.

1.8.1.2 Adding and Editing Trusted Servers

The trusted servers table identifies servers that can connect to the local MiCollab Client Service without authentication.

Note:
If the peered server IP address is changed, add or edit the IP address in the **Trusted Server Details** page, to view the presence state of the users.

Note:
When you configure a peer MiCollab Client Service on the Peering tab, a Trusted Server entry is automatically created for the peer server with the "peer" server type. For peer trusted servers, you can edit the **Description** only.

To add or edit a trusted server:

1. Type a **Description** for the trusted server. The Description is limited to 64 characters in length and must contain alpha-numeric characters, dashes, and/or spaces.
2. Type the **IP address/hostname** for the server. The IP address must be a valid IP address or fully qualified domain name.
3. Select one of the following server types:
   - **Presence**: Trusted presence servers are permitted to receive presence information from the contacts on this MiCollab Client Service .
   - **IM**: Trusted IM servers are permitted to exchange Instant Messages with contacts on this MiCollab Client Service .
   - **Peer**: Trusted peer servers are permitted to exchange communication information with contacts on this MiCollab Client Service .
4. Click **Create** or **Save**. You are returned to the Enterprise Tab.

After you create a trusted server, you can edit the associated fields at any time.

Note:
The following procedure must be done on MiCollab Client 5.1 to resolve peering on a server which had a changed IP address, failure to do so will cause peering not to work. Go to the Enterprise Tab, expand Trusted Servers, select the peered server whose IP address changed and in the Trusted Server Details page edit the field "IP address/hostname" with the correct IP address.

Note:
Whenever the peered server address is changed, the server address must also be updated in the peer trusted servers list.

1.8.1.3 Creating an Enterprise

Creating an Enterprise is the first step to provisioning MiCollab Client.

On this page, configure basic information about a company to create an Enterprise.

To create an Enterprise

1. Configure the following Enterprise Settings.

   - **Enterprise ID**: (*Required*) Type a unique identifier for the Enterprise, for example, **Phoenix**. By default this field is blank. The Enterprise ID:

     - is limited to 4-32 characters in length.
     - must contain alpha-numeric characters (dashes included).
     - cannot contain spaces, vertical bars, commas, semicolons, or colons (| , ; :).

Note:
You cannot change this field after you create the Enterprise if PBX nodes have been defined. Once PBX nodes have been defined, this field cannot be deleted unless all PBX nodes are deleted first.

- **Description**: (*Required*) Type a description for the Enterprise, for example, **Acme Company-Phoenix Arizona**. By default this field is blank. The Enterprise Description:
  - is limited to 1-128 characters in length.
  - must contain alpha-numeric characters (dashes included).
  - cannot contain vertical bars (|).
- **Enterprise domain**: (*Required*) Type a domain for the Enterprise. The Enterprise domain does not need to be a resolvable DNS name or a registered domain name, however, it does need to follow the DNS suffix format. The Enterprise domain should be unique to the Enterprise so that peered servers do not have the same Enterprise domain. Mitel suggests using the site location or Enterprise ID as part of the Enterprise domain (for example, **Phoenix.xyzcompany.com**, where **Phoenix** is the Enterprise ID).
- **Voice mail server**: (*Optional*) Type the IP address or the hostname of the Enterprise's NuPoint UM voice mail server, for example, **phx-acme-Nupoint**. If you do not have a NuPoint UM voice mail server, leave this field blank.
- **Administrator e-mail**: (*Optional*) Type the e-mail address for the MiCollab Client Service administrator. An e-mail message is sent to this address when On-Demand presence is enforced. Maximum length for this field is 255 characters.
- **Switch type**: (*Required*) Select the communications system (switch) that the Enterprise currently uses from the list box.

  By default, MiVoice Business is selected.

Note:
You cannot change this field after you create the Enterprise if PBX nodes have been defined. Once PBX nodes have been defined, this field cannot be deleted unless all PBX nodes are deleted first.

- **Collaboration server type**: (*Optional*) Select a collaboration server to use with MiCollab Client . Options include:
  - None (default)
  - MiCollab MiCollab Audio, Web and Video Conferencing

  If you do not intend to use collaboration features, set this field to **None** (default). If you have already added and configured a collaboration server, you cannot configure the option here.

Note:
The Mitel Your Assistant Collaboration Module is no longer supported as a collaboration server type. Refer to the Collaboration tab topic for more information.

- **Language**: (*Required*) Select a language for the Enterprise from the list. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. The user's language setting determines which language the Welcome E-mail Message is generated in for that user.
- **Time zone**: (*Required*) Select the time zone where the MiCollab Client Service is physically located from the list box. The time zone where the MiCollab Client Service is located may be different than the time zone where the Enterprise is located.

2. Click **Create** to create the Enterprise.

After you create the Enterprise, you are returned to the Enterprise tab where you must complete additional Enterprise-related settings.

1.8.1.4 Advanced Calendar Integration Settings

The Advanced Calendar Integration settings enable you to adjust calendar integration settings specific to your network.

Note:
The default calendar integration settings are optimal in most cases. You should only modify them if you have some special requirements, such as high network latency. These settings are applied globally, across all enterprises.

Google

- **Calendar duration per fetch**: Determines how much calendar information is retrieved each time a fetch is performed. The recommended value is 24 hours worth of information - see Note 3.
- **Calendar onpeak fetch Interval**: Determines how often the calendar information is fetched during the onpeak time period . The recommended value is to poll calendars every 45 minutes. The range is 5 to 480 minutes - see Note 4..
- **Calendar offpeak fetch interval**: Determines how often the calendar information is fetched during the offpeak time period . The recommended value is to poll calendars every 240 minutes. The range is 5 to 1440 minutes - see Note 4.
- **Start peak time:** Peak period start time, default is 0700 hours. The allowed range is 0000 to 2359 - see Note 4.
- **End peak time:** Peak period end time, default is 1730 hours. The allowed range is 0000 to 2359 - see Note 4.
- **Request accumulation delay**: Determines the delay to accumulate free/busy requests. The range is 1 to 300 seconds; the default is 30. Lower values may result in unnecessary duplicate event fetches from the Google server – as the server can send multiple event notifications for a single calendar event creation or deletion.
- **Maximum users per fetch:** Fetch at most 20 calendars per poll request (recommended). The range 1 to 20. Higher values will result in fewer (but larger) network requests. Lower values will result in more (but smaller) network requests.

Common Settings:

- **Parallel connections**: Determine the number of parallel connections to the server. The recommended value is 6. Higher values can be useful in the case of high network latency. Higher values also result in higher network loads.
- **Connection timeout**: Determines how long the connection can be lost before a timeout is flagged. The recommended value is 30 seconds.
- **Error limit:** Determines how many timeouts can occur while communicating with the Google server before the MiCollab Client Service temporarily suspends

communication with the Google server. The recommended value is 5 timeouts. Higher values cause the MiCollab Client Service to tolerate more timeouts from the Google server - see Notes 1 and 2.

- **Error duration:** Determines the time interval within which timeouts are considered. For example, if the Timeout Duration is 5 minutes (which is the recommended value), then timeouts that happened before 5 minutes are not considered when determining whether or not to temporarily suspend communication with the Google Server - see Notes 1 and 2.
- **Retry delay after errors**: Determines how long MiCollab Client suspends communication with the Google server before retrying. This applies to most errors caused due to admin configuration, or some issue with MiCollab Client -Google server communication. The default value is 15 minutes - see Notes 1 and 2.

Note:

The **Error limit, Error duration**, and **Retry delay after errors** parameters are used for timeout error throttling. In other words, when <Error Limit> timeouts happen within <Error Duration>, then the MiCollab Client Service waits for <Retry delay> before re-initiating communication with the Google server. Before MiCollab Client retries, the administrator can at any time test the connection with the Google server from the Enterprise tab, apply the settings, and cause MiCollab Client to immediately start communicating again.

Note:

Similar to the above note, non-timeout errors (such as incorrect authentication credentials, network reachability issues, etc.) will cause the communication with the Google server to be disabled and retried after <Retry delay> interval. When the communication is disabled, the MiCollab Client administrator can change settings, apply the changes and cause MiCollab Client to immediately retry the communication again.

Note:
By default, the Calendar Integration Module retrieves 24 hours of calendar information for a user, starting at the present time. Once the first 15 hours elapse, the Calendar Integration Module once again retrieves information for the next 24 hours. If, during those first 15 hours, any calendar events are created/delete/modified, then the Calendar Integration Module will again retrieve 24 hours of information starting at the current time.

Note:
Google calendar imposes a daily limit (10,000 requests by default) on how many requests can be made to it. To conserve the number of Google requests, MiCollab Client allows the Administrator to setup an onPeak interval during which time, the polling is done frequently. Outside of this time (for example, outside of normal office hours), the polling frequency is reduced, thus reducing the number of requests. If you need a bigger quota (more than 10,000 requests per day), please login to the console at https://code.google.com/apis/console#access and request more Quota.

MS Exchange

- **Calendar duration per fetch**: Determines how much calendar information is retrieved each time a fetch is performed. The recommended value is 24 hours worth of information - see Note 3.
- **Calendar fetch Interval**: Determines how often the calendar information is fetched. The recommended value is 15 hours - see Note 3.
- **Event subscription notification frequency**: Determines how often subscription information is sent. The recommended value is 90 minutes. Lower values result in more subscription traffic and processing. Higher values will reduce processing but delay the detection of possible subscription losses on the exchange server.
- **Subscription delay**: Determines the delay after each subscription is performed. The recommended value is 50 milliseconds. Lower values result in spikes of traffic and CPU. Higher values increase the amount of time taken to subscribe all users.
- **Request accumulation delay**: Determines the delay to accumulate free/busy requests. The range is 1 to 10 seconds; the default is 10. Lower values may result in unnecessary duplicate event fetches from exchange server – as the exchange server can send multiple event notifications for a single calendar event creation or deletion.

- **Maximum users per fetch:** Fetch at most 100 calendars per poll request (recommended). The range 10 to 100. Higher values will result in fewer (but larger) network requests. Lower values will result in more (but smaller) network requests.

Common Settings:

- **Parallel connections**: Determine the number of parallel connections to the server. The recommended value is 6. Higher values can be useful in the case of high network latency. Higher values also result in higher network loads.
- **Connection timeout**: Determines how long the connection can be lost before a timeout is flagged. The recommended value is 30 seconds. Higher values will wait longer for the calendar server to respond, but can delay the detection of unresponsiveness.
- **Error limit**: Determines how many timeouts can occur while communicating with the Exchange server before the MiCollab Client Service temporarily suspends communication with the Exchange server. The recommended value is 5 timeouts. Higher values cause the MiCollab Client Service to tolerate more timeouts from the Exchange server - see Notes 1 and 2.
- **Error duration**: Determines the time interval within which timeouts are considered. For example, if the Timeout Duration is 5 minutes (which is the recommended value), then timeouts that happened before 5 minutes are not considered when determining whether or not to temporarily suspend communication with the Exchange Server - see Notes 1 and 2.
- **Retry delay after errors**: Determines how long MiCollab Client suspends communication with the Exchange server before retrying. This applies to most errors caused due to admin configuration, or some issue with MiCollab Client -Exchange server communication. The default value is 15 minutes - see Notes 1 and 2.

Note:

The **Error limit, Error duration**, and **Retry delay after errors** parameters are used for timeout error throttling. In other words, when <Timeout Limit> timeouts happen within <Timeout Duration>, then the MiCollab Client Service waits for <Retry delay> before re-initiating communication with the Exchange server. Before MiCollab Client retries, the administrator can at any time test the connection with the Exchange server from the Enterprise tab, apply the settings, and cause MiCollab Client to immediately start communicating again.

Note:
Similar to the above note, non-timeout errors (such as incorrect authentication credentials, network reachability issues, etc.) will cause the communication with Exchange server to be disabled and retried after <Retry delay> interval. When the communication is disabled, the MiCollab Client administrator can change settings, apply the changes and cause MiCollab Client to immediately retry the communication again.

Note:
By default, the Calendar Integration Module retrieves 24 hours of calendar information for a user, starting at the present time. Once the first 15 hours elapse, the Calendar Integration Module once again retrieves information for the next 24 hours. If, during those first 15 hours, any calendar events are created/delete/modified, then the Calendar Integration Module will again retrieve 24 hours of information starting at the current time.

MS Office 365

The authentication protocol for Calendar Integration with Office365 can be either Open Standard for Authentication 2.0 (OAuth 2.0), OAuth 2.0 (Microsoft Graph) or Basic Authentication protocol.

Basic Authentication mechanism is a process where the username and password are provided for authentication purposes, whereas in case of OAuth 2.0, tokens are being used for authorization.

OAuth 2.0 (Microsoft Graph) also uses the OAuth 2.0 tokens with difference being instead of Exchange it uses Microsoft Graph Server APIs to fetch the calendar details.

For initial details on configuration, refer to the following section under MiCollab Admin Help: **Configuration > Cloud Service Provider.**

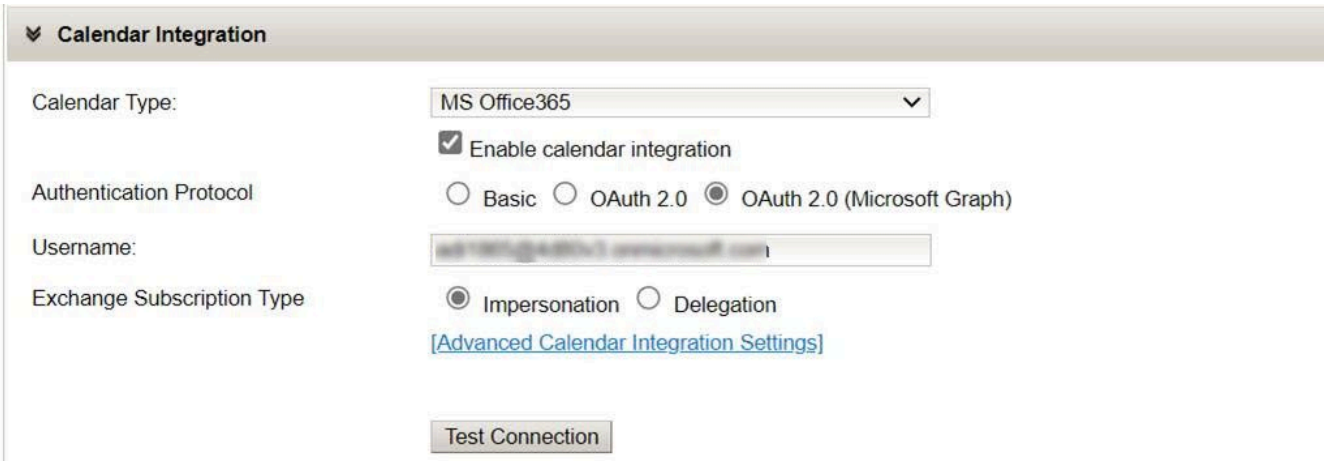
Once the configuration under **Cloud Service Provider** is successful, the MiCollab Administrator can enable Calendar integration from MiCollab Client Services.

Perform the following steps under MiCollab Client Services:

1. Navigate to the **Applications > MiCollab Client Services > Enterprise.**
2. Under **Calendar Integration,** select the **Calendar Type** as **MS Office365.**
3. Select the **Authentication Protocol** for Office 365 as:

   - **Basic**,
   - **OAuth 2.0**, or
   - **OAuth 2.0 (Microsoft Graph)**

   In order to enable OAuth 2.0 or OAuth 2.0 (Microsoft Graph), the administrator must select the respective Authentication Protocol's radio button.



Note:

The API permission for MS Graph must be given to app in Azure Active Directory.

Note:

The administrator must test the connection to switch between OAuth 2.0 (Microsoft Graph) and OAuth 2.0

Note:

The **Username** field is mandatory to configure the calendar integration with Office 365 using OAuth 2.0 protocol.

The **Username** should be a primary SMTP address.

4. For **Exchange Subscription Type**, the default option selected is **Impersonation** if OAuth 2.0 (Microsoft Graph) is selected as Authentication Protocol. It will be applicable for all 9.6 servers including the new deployed and upgraded servers.

Note:
After a backup restore, the client credentials will not be part of the MiCollab backup. Therefore, the admin must reconfigure OAuth 2.0 settings at the Cloud Service Provider section and then enable Calendar Integration.

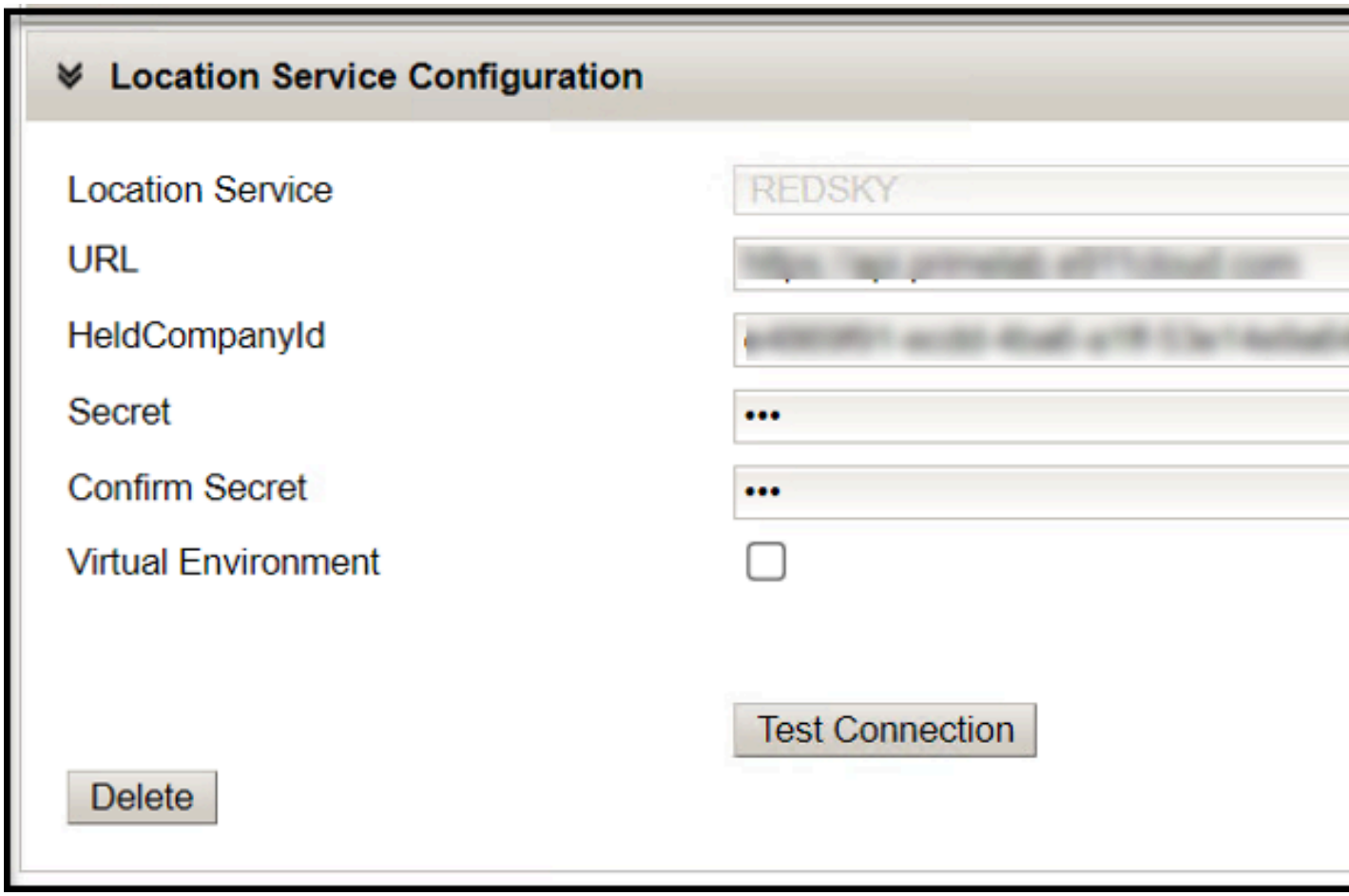
Note:
Default subscription type is not supported in Calendar Integration for Office 365 with OAuth 2.0 Authentication Protocol.

1.8.1.5 Location Service Configuration

The Location Service Configuration performs the Emergency Location configuration in the administrator portal. You can configure the Location Service Configuration settings under **MiCollab Client Service > Configure MiCollab Client Service> Enterprise Tab > Location Service Configuration.**

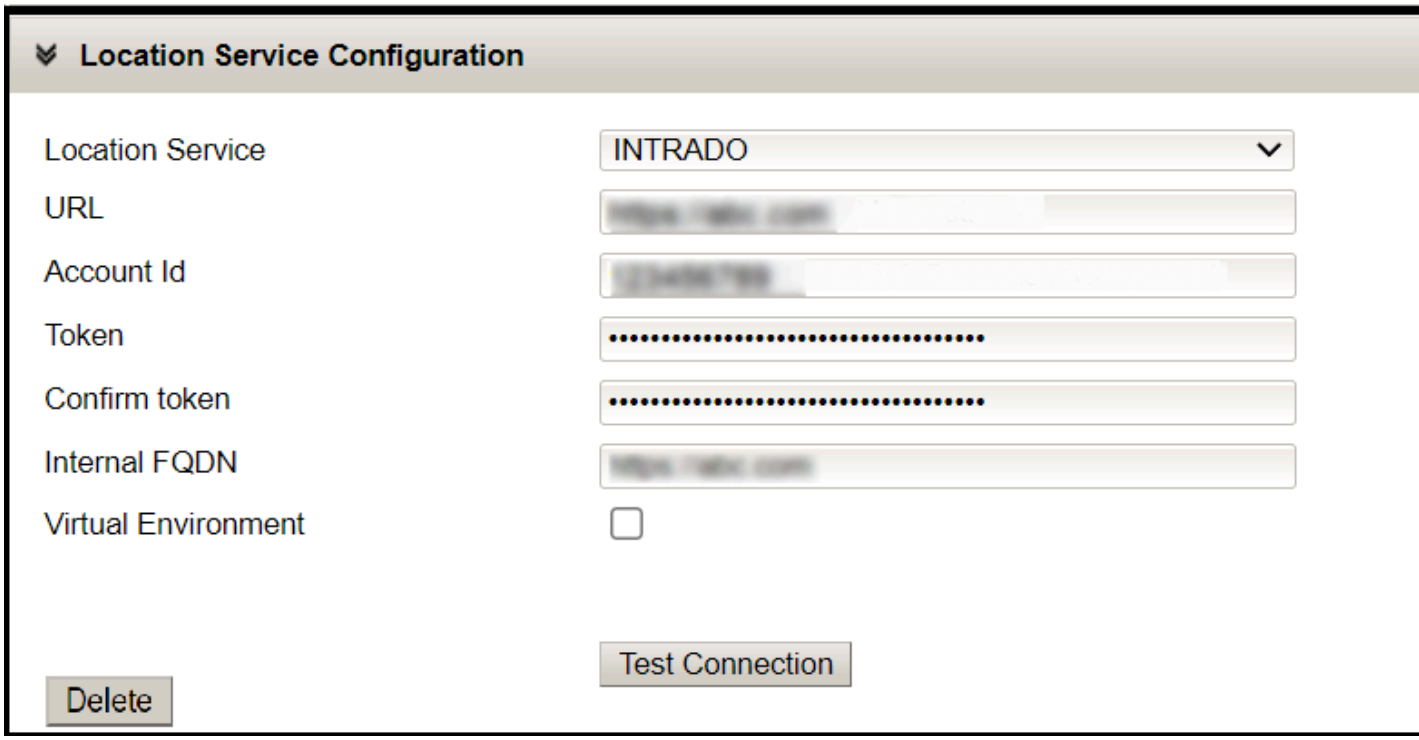
Under the **Location Service Configuration** tab, in the **Location Service** field**,** the administrator can select the option from the drop-down menu either as **Redsky** or **Intrado**.

Representation of Location Service Configuration for Redsky



For RedSky, the values/parameters of the fields (that is, **URL**, **HeldCompanyId**, and **Secret**) can be obtained from the RedSky Portal. Refer to the RedSky Solution document for more information.

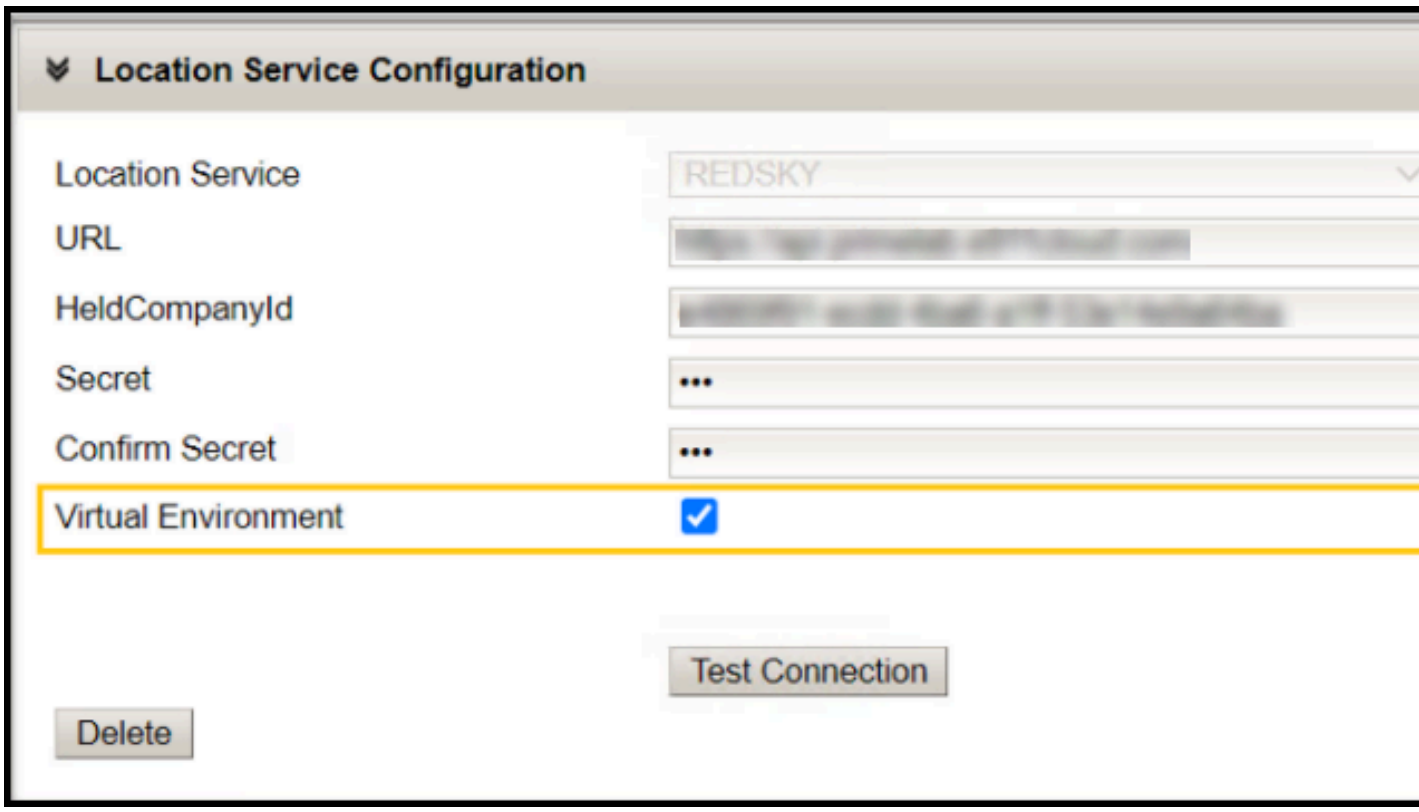
Representation of Location Service Configuration for Intrado



For Intrado, the values/parameters of the fields (that is, **URL**, **Account Id**, and **Token**) can be obtained from the Intrado Portal. Refer to the Intrado Solution document for more information.

The valid value/parameter of the field **Internal FQDN** should be entered by the Administrator on the server.

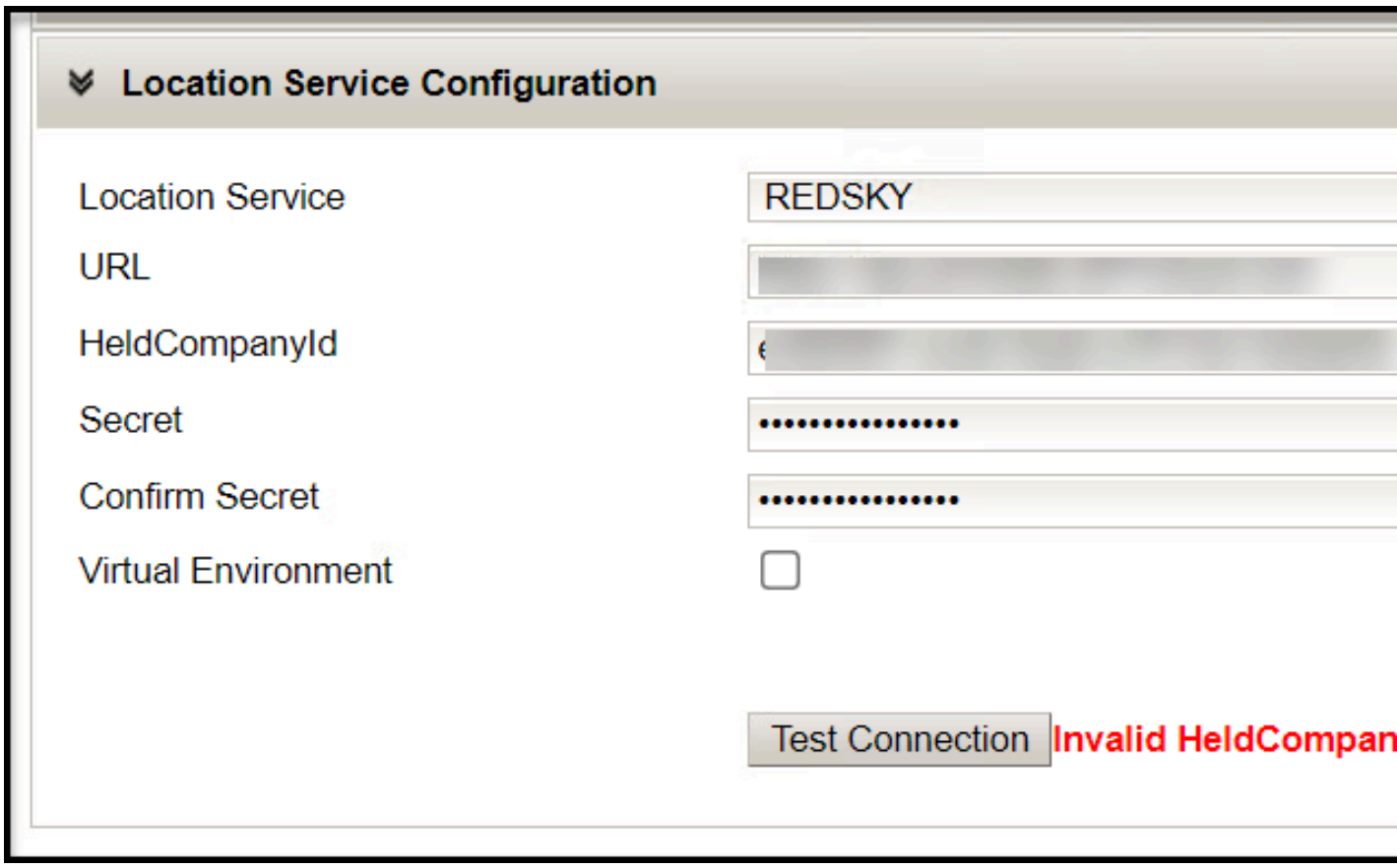
If Clients are running virtually in VMWare Horizon, Citrix or RDS, then select the **Virtual Environment** option.



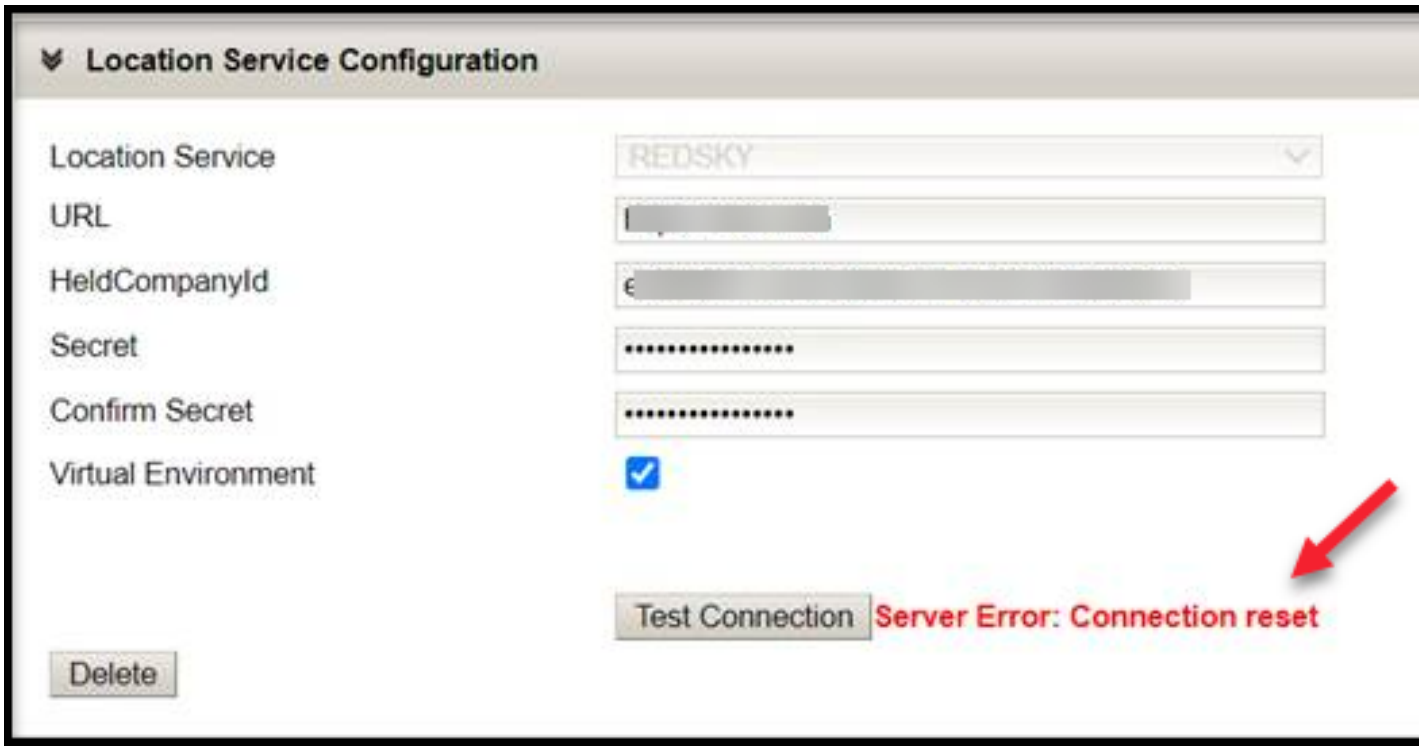
Note:
It is always advisable to change any Emergency Location configuration during off-service hours so that the users are not impacted.

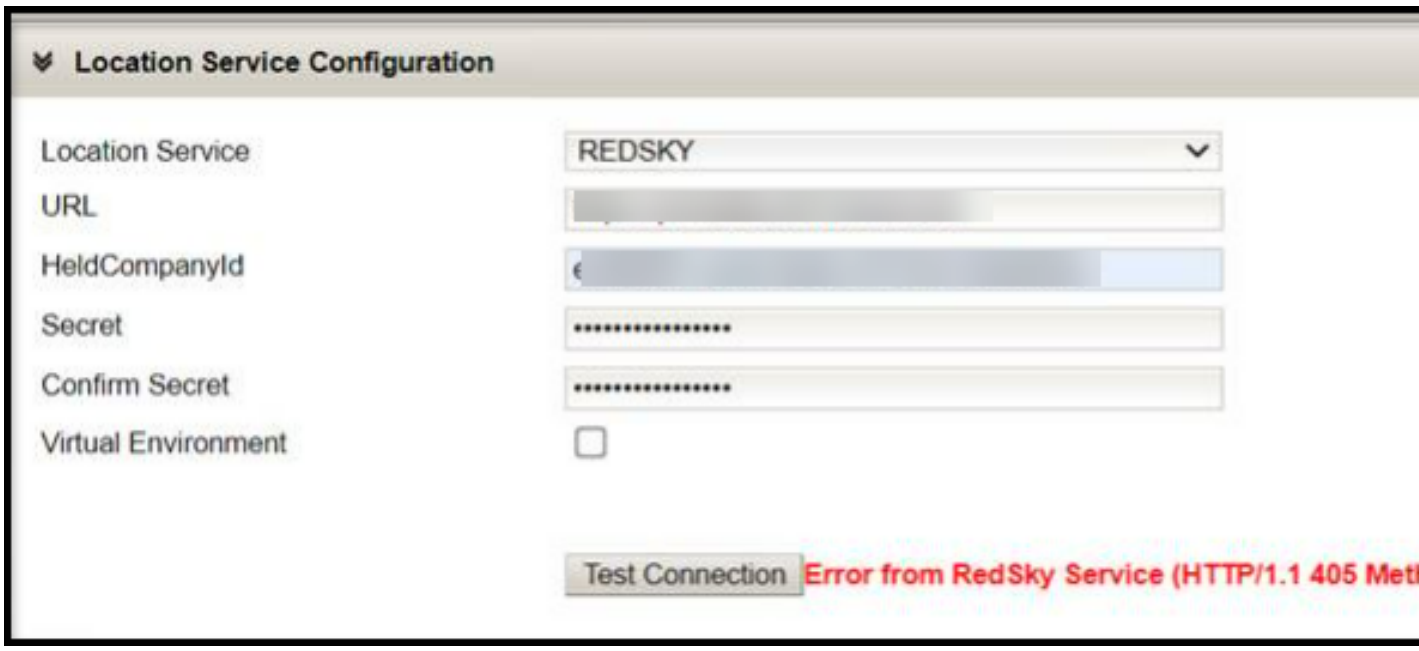
Once the field parameters are entered, click on the **Test Connection** button. This option helps the administrator to test if the entered details are valid or not.

If the **HeldCompanyId** or **Secret** value is incorrect, it will display the following error message ***Invalid HeldCompanyId or Secret***.

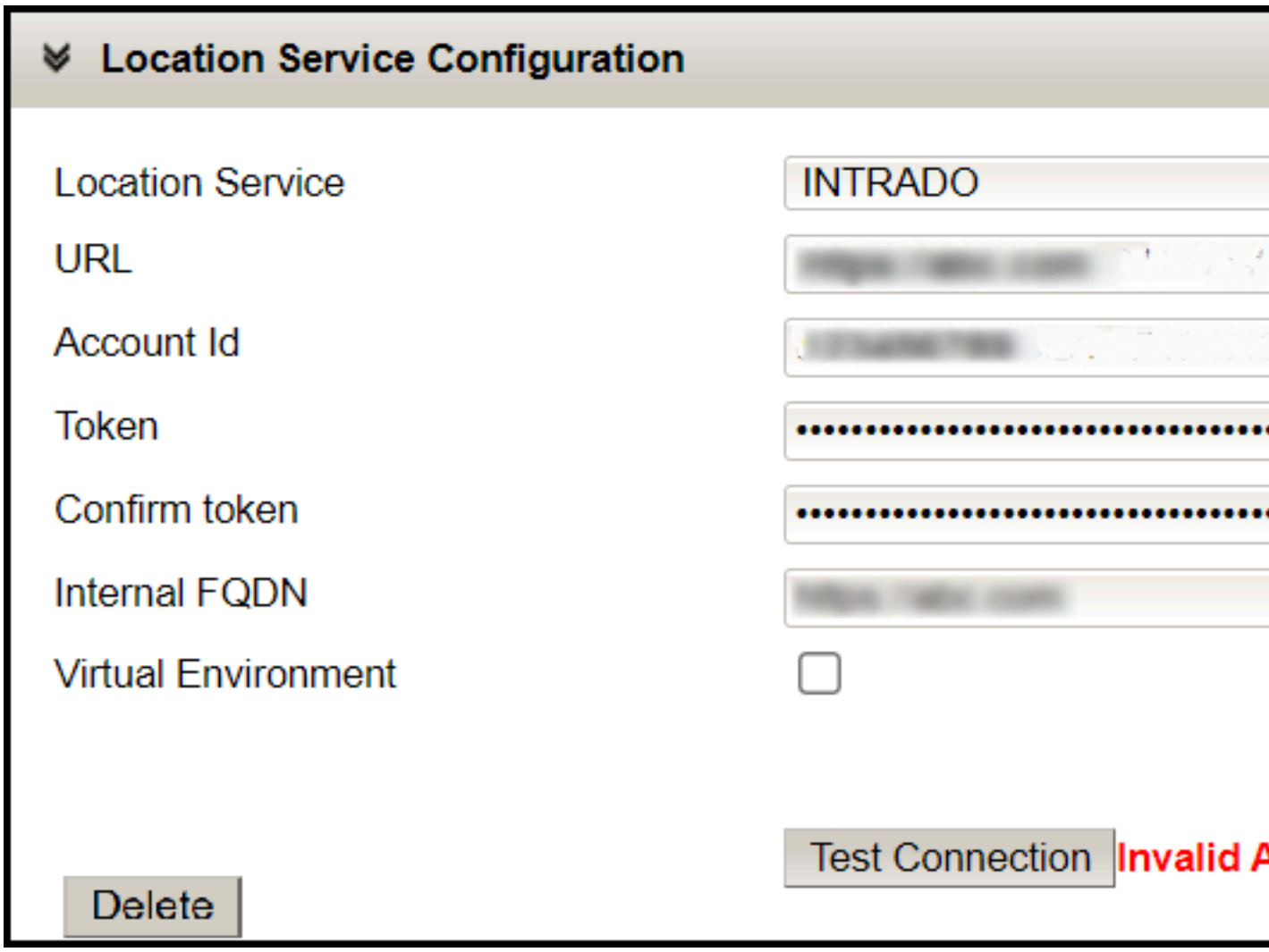


In case if the URL is incorrect, it will display either ***Server Error: Connection reset*** or error message along with the error code.

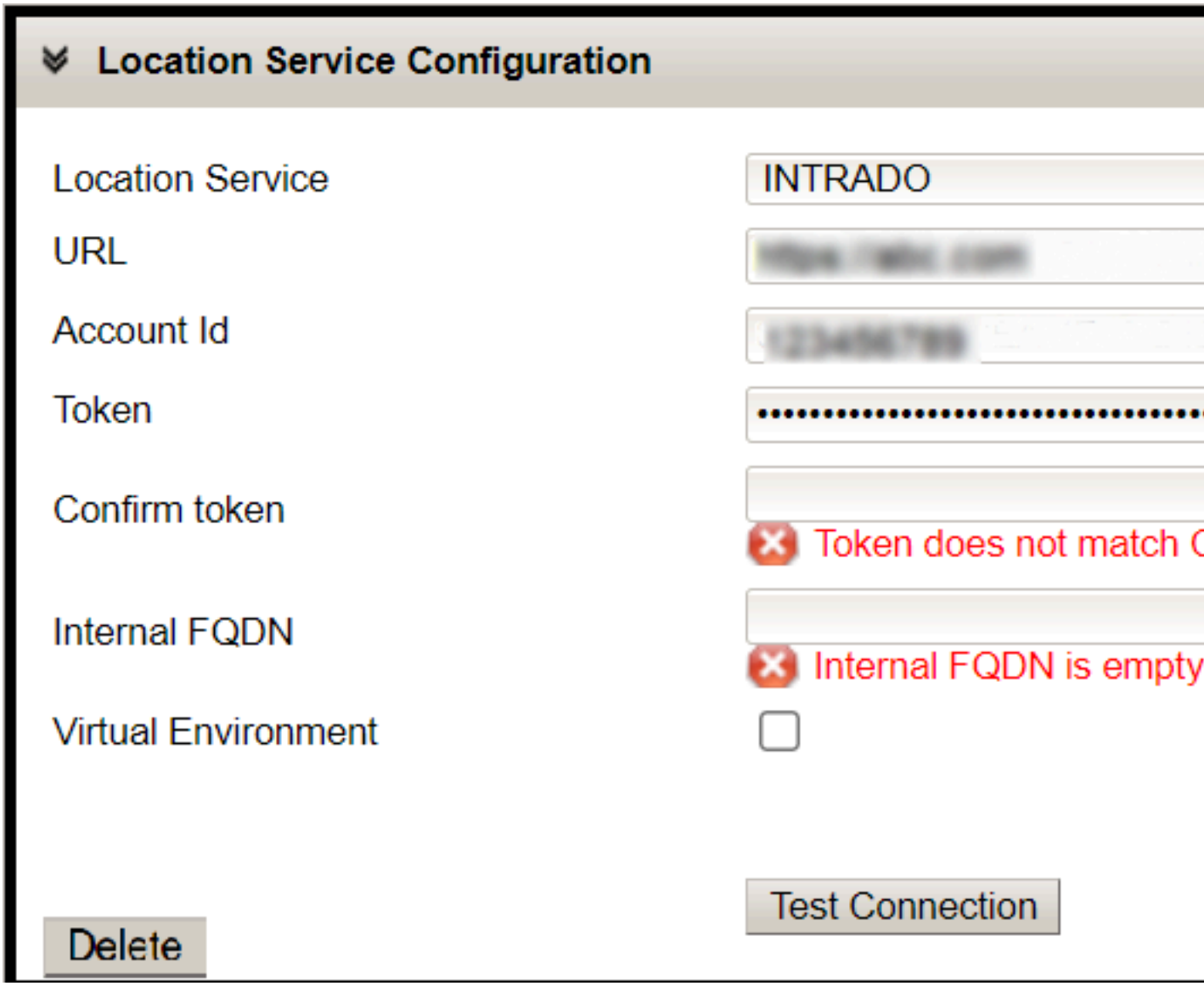




If the Account Id or Token is incorrect, it will display as ***Invalid Account Id or Token***.



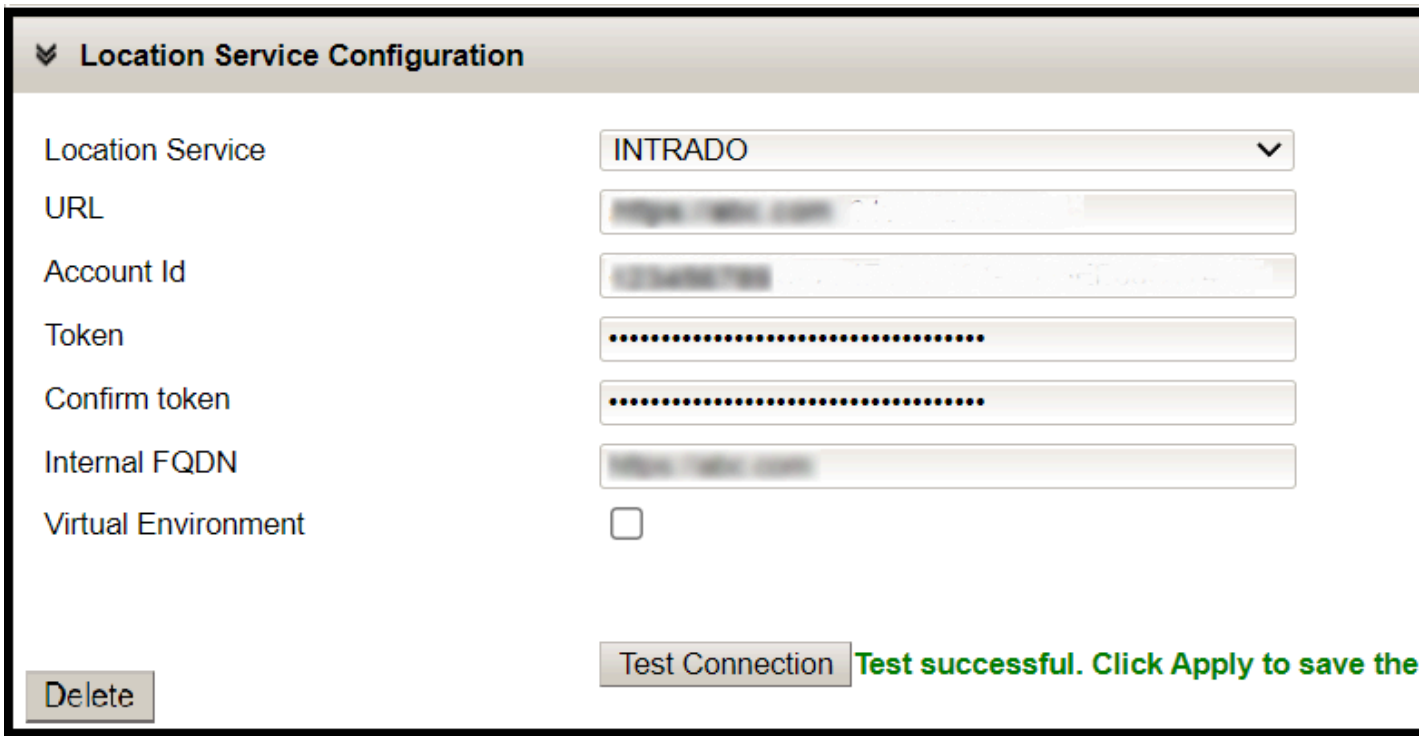
If the Token does not match or the Internal FQDN field is left empty, it will display the error as ***Token does not match Confirm token*** and ***Internal FQDN is empty***.



Note:
All the parameters are mandatory, and if any of the fields are left empty, the UI will display the error messages.

In the case of a successful connection, a success message is displayed.

For Example:



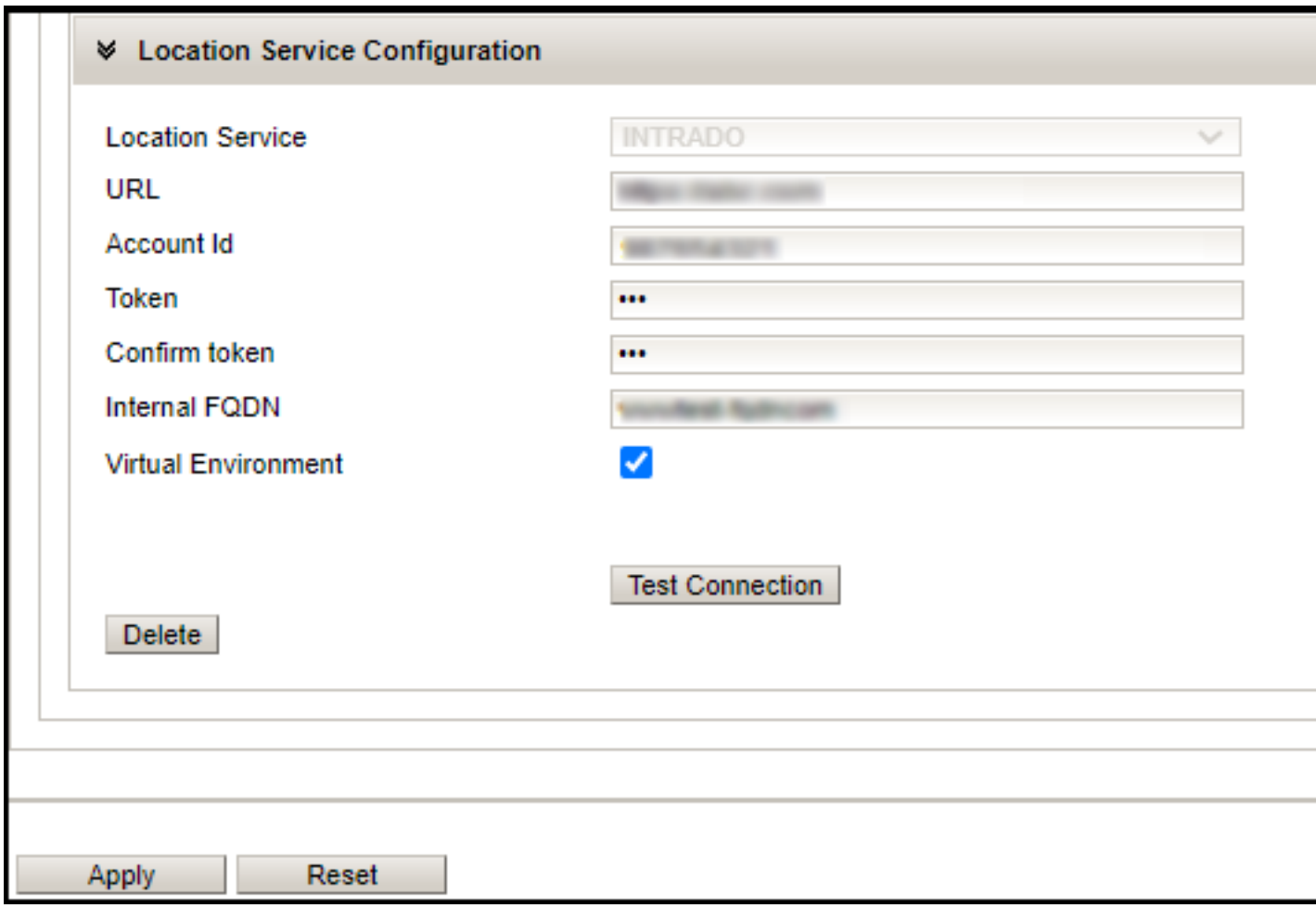
Note:
The connection timeout and request timeout are currently configured to 10secs.

Note:
If you want to switch the service from Redsky to Intrado or vice-versa, click the **Delete** button to clear the existing service data and then switch to the other service.

After providing the necessary details, click **Apply** to save the given information or click **Reset** to clear your changes.

Note:

Clicking the Apply or the Reset button will save or clear all the settings provided in the Enterprise tab.



1.8.2 Synchronization Tab

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab - integrated mode.

Using synchronization, you can quickly populate the MiCollab Client accounts list based on your existing PBX node, Active Directory (AD), or Lightweight Directory Access Protocol (LDAP) corporate directory. In addition, you can schedule periodic synchronizations to keep your MiCollab Client accounts and corporate directory synchronized.

From the Synchronization tab, select the Enterprise from the list box, and then select a synchronization type .

Synchronization Type

To select a synchronization type:

1. Select one of the following synchronization options:

   - **None**: Select this option if you do not want to populate your account list using a corporate directory synchronizer. If you select this option, you will need to add all MiCollab Client accounts manually.
   - **Active Directory/LDAP Synchronizer**: Select this option if you want to populate the MiCollab Client accounts database using the company AD or LDAP directory. You will then need to add an AD/LDAP synchronizer. To provide ongoing synchronization between MiCollab Client and the AD/LDAP directory, you can schedule automatic synchronizations. You can also complete manual synchronizations. When you click the **Sync Now** button, the AD/LDAP directory is synchronized with the MiCollab Client Service . Refer to the Common AD/LDAP Field Mappings topic for information about field mappings between AD and LDAP.
   - **PBX Node Synchronizer**: Select this option if you want to populate the MiCollab Client accounts database using the user/extension information programmed for the PBX node database. To provide ongoing synchronization between MiCollab Client and the PBX node database, you can schedule automatic synchronizations. You can also complete manual synchronizations. When you click the **Sync Now** button, all of the PBX nodes are synchronized with the MiCollab Client Service .

   Note:
   After you complete phone extension configuration changes (add, delete, move, change) on the PBX, perform a manual synchronization (**Sync Now**) to ***immediately*** update the affected MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization.

   In addition, for those MiCollab Client users whose extensions are affected by the configuration changes you make on the PBX, instruct the users to exit and then restart their MiCollab Desktop Clients to refresh extension information.
2. Click **Apply**.

After you select a synchronizer, you can complete the following tasks:

- Perform a manual synchronization .

  To perform a manual synchronization, click **Sync Now**. The MiCollab Client accounts database is synchronized with the AD/LDAP directory or the PBX Node database.
- Schedule a day and time to perform automatic synchronizations.

  Schedule automatic synchronizations for the MiCollab Client accounts database and the AD/LDAP directory or the PBX node database.

  To schedule automatic synchronizations:

  1. Specify the following to schedule the synchronization:
     - The frequency (in days) the synchronization should occur.
     - The hour the synchronization should start.
     - The minute the synchronization should start.
     - Whether the synchronization should occur in the AM or PM.
  2. Click **Apply** to save the information, or click **Reset** to clear your changes.
- ***For Enterprises configured for AD/LDAP synchronizers only***, you can also do the following:
- Click Add to add an AD/LDAP synchronizer and configure the settings.
- Click an AD/LDAP Synchronizer link to edit it.
- Delete an AD/LDAP synchronizer. When you delete an AD/LDAP synchronizer, all the accounts associated with the synchronizer are also deleted.

  To delete an AD/LDAP synchronizer:

  1. Select the AD/LDAP synchronizer you want to delete from the list.
  2. Click the **Delete** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the synchronizer, or click **Cancel** to cancel the deletion.
- Check the status of the last AD/LDAP synchronization.

> **Note**:
> For synchronization failures, refer to the Synchronization Error Messages topic.

- ***For Enterprises configured for PBX Node synchronizers only***, you can also do the following:
- Check the status of the last PBX Node synchronization on the PBX Nodes tab.
- View PBX Node synchronization details on the PBX Node Details page.

- Specify a feature profile to use for all accounts created during the PBX node synchronization.

Note:
Before specifying a Feature Profile, refer to the Licensed Features and Synchronization topic.

To specify the feature profile to use for PBX node accounts:

1. Create the feature profile for the PBX node on the Features tab.
2. On the Synchronization tab, select the appropriate feature profile from the list box.
3. Click **Apply** to save the information, or click **Reset** to clear your changes.

- Enable or disable the Synchronize Dynamic Extensions only option.

This option specifies if new accounts are created or not during the synchronization process. By default, this option is disabled. Options include:

- **Disabled**: When this option is disabled (not selected) the synchronization process pulls data (including Dynamic Extension information) from the PBX nodes and creates MiCollab Client accounts.
- **Enabled**: When this option is enabled (selected) the synchronization process does not create new accounts. It does however, pull Dynamic Extension data from the PBX node to update existing MiCollab Client accounts. When you enable this option, you must manually create the accounts first.

Note:
The following are valid character ranges for LDAP synch. Anything outside of these is invalid character for LDAP synch:

0x9, 0xA, 0xD, 0x20 to 0xD7FF, 0xE000 to 0xFFFD, 0x10000 to 0x10FFFF

Synchronization Rules for MiVoice Business:

Note:
On MiVoice Business , PRG stands for - **Personal Ring Group**. MDUG - stands for **Multi Device User group**.

1. After creating users with MDUG/PRG, perform a manual PBX synchronization (**Sync Now**) to *immediately* update the MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization.
2. Starting from MiCollab Client 5.1, user can have either a MiNet Softphone or a SIP softphone, but not both.
3. The MiCollab Client will recognize numbers on MiVoice Business with device type as 'App Server Port' or '5020 IP' with MAC address starting with A1:21:00 as MiNet Softphone. Numbers on MiVoice Business with device type as 'MiCollab Client Endpoint' will be recognized as 'UC Endpoint', if user does not have a MiNet Softphone. If user has both number types, then MiCollab Client will assign the MiNet Softphone as User softphone.
4. If user has deskphone and softphone , and no PRG or MDUG on MiVoice Business , then the first name, last name and department fields in MiVoice Business has to match exactly (including case) for the deskphone and softphone for MiCollab Client PBX sync to associate the two phones for same user. This restriction does not apply if user has PRG or MDUG on MiVoice Business and the deskphone and softphone are part of the PRG.
5. When user has PRG or MDUG on MiVoice Business , the first name,last name and department of PRG pilot is used to identify the account in MiCollab Client . The PRG pilot will be assigned as user deskphone or as user softphone.
6. If user has multiple deskphones or SIP phones or MiNet softphones, then PRG or MDUG has to be defined in MiVoice Business and all the user devices have to be part of the group for MiCollab Client to pull in all the phone numbers for that user.
7. When a phone number is deleted in MiVoice Business then it will still show up in MiCollab Client for that account when one or more of the following is true:

   a. The number was manually added in MiCollab Client by the administrator.
   b. Some of the user's dynamic statuses are still pointing to that number for call routing purposes.

   To remove the number from MiCollab Client database, the user has to login to the desktop client and update the dynamic statuses pointing to the deleted number. User has to update the Make Call from setting within each status to point to a different

number. Once all the references are removed, the user can delete the number from MiCollab Client database.

Note:
Rule 6 also applies to MiVoice Office 250.

1.8.2.1 Adding and Editing AD/LDAP Synchronizers

Adding an AD/LDAP synchronizer is a two-step process: configure Connection Settings, and then configure Field Mappings.

To help you generate the LDAP path, which is a required field under Connections, use the LDAP Path Assistant.

LDAP Path Assistant

The LDAP Path Assistant can make it easier to formulate the LDAP URL for a synchronizer, provided that the synchronizer is connecting to an Active Directory server. The Assistant may not work with other kinds of LDAP servers.

To use the assistant, enter the fully qualified domain name (FQDN) of the domain controller in the Assistant. The Assistant will then create an LDAP URL with the format ldap://<*domain-controller-name*>/<*DC= separated top level domain controller name components*>

For example:

- **Domain controller name**: test-controller.mitel.com
- **Resulting LDAP path**: ldap://test-controller/DC=mitel,DC=com

Note:
The path assistant is only intended to assist you in the creation of LDAP URL. Path assistant may ***not*** always work depending on how your LDAP server is configured.

The **Search context** is an LDAP path relative to the absolute path specified in the **LDAP path** field. Together, the values you configure for the **LDAP path** and **Search**

context fields determine which LDAP object is the starting point for the search query. For example, if you use the following hierarchy in your LDAP database:

XYZ Company

-> New York Branch

-> Sales Department

-> US Sales

-> Eastern US

To synchronize all accounts from the Eastern US Organizational Unit, you would specify the LDAP fields as follows:

- **LDAP path**: ldap://ldap.example.com/DC=example,DC=com
- **Search context**: OU=NewYork Branch, OU=Sales Department, OU=US Sales, OU=Eastern US

If your search should begin at the root object (for example, the XYZ Company object), you can leave the Search context blank.

To add an AD/LDAP Synchronizer:

1. Configure the AD/LDAP **Connection Settings**.

   Connection Settings allows MiCollab Client to connect to the AD/LDAP directory and import information. Add or edit the following Connection Settings:

   - **Description**: (*Required*) Type a short description for the AD/LDAP synchronizer. This field has a maximum length of 64 characters.
   - **Domain name**: (*Required*) Type the domain name for the AD/LDAP synchronizer. The value can be any unique value. This field has a maximum length of 128 alphanumeric characters, and supports dashes, and periods.
   - **Show LDAP Path Assistant**: Click **Show LDAP Path Assistant**, enter the fully qualified domain name (FQDN) of the domain controller, and then click **Generate Path**. The LDAP path field is populated. Click **Hide LDAP Path Assistant**.

Note:
The LDAP Path Assistant is only intended to assist you in the creation of the LDAP URL. Depending on how your LDAP server is configured, it may not always work.

- **LDAP path**: (*Required*) Type the full LDAP path of the synchronizer will use when connecting to the directory server. This field has a maximum length of 255 characters. Example: ldap://directory.mitel.com/DC=mitel,DC=com

  - **Server supports paging results**: Clear this setting if the LDAP server does ***not*** support paging results extension (refer to IETF rfc2696). Windows Server® 2003 Active Directory and ApacheDSTM servers do support paging results.
  - **Do not import disabled accounts from AD**: This setting is applicable only when connecting to an Active Directory server. DO NOT check this for other kinds of LDAP servers. If checked, MiCollab Client will not import disabled accounts from Active Directory. To find out if an account is disabled or not, on ActiveDir server, open the "Active Directory Users and Computers" tool, navigate to the account, right-click on the account, and select Properties. Under the Account tab -> Account Options, the "Account is disabled" field will show the account status.
- **Search context**: (*Optional*) This field points to the LDAP object on the sub-tree where the search query is run. If you complete this field, the value MUST be relative to the initial context specified by the **LDAP path** parameter. If you leave this field blank, then the query search is performed on the LDAP root object pointed to by the "LDAP path" parameter. This field has a maximum length of 255 characters. Example: (ou=Sales).
- **User query**: (*Optional*) If specified, this field should be a valid LDAP query string, which is used to selectively query for and import user accounts. If your leave this field blank, the query string (|(objectClass=person)(objectClass=user)) is used. This field has a maximum length of 255 characters.
- **Username**: (*Optional*) Type the username for the directory server.
  The username can be an LDAP distinguished name. Example: CN=Administrator,OU=engineering,DC=directory,DC=mitel,DC=com. If the directory server is Active Directory, it can be the qualified Active Directory username. Example: engineering\jsmith.

Note:
The specified user must have privileges to read information relevant to all accounts that expect to be synced into MiCollab Client .

- **Password**: (*Optional*) Type the password for the directory server.
- **Default feature profile**: (*Required for Account AD/LDAP Synchronizers only. This field is not displayed for external server AD/LDAP Synchronizers*) Select the feature profile you want to apply to the accounts created by the synchronizer. By default, the **Default Feature Profile** is selected.

Note:
The Default Feature Profile does not include any features. To assign features to users when you create accounts during the initial synchronization, you must first create a Feature Profile that includes the features you want to use, and then you can select it here. Refer to the Licensed Features and Synchronization topic before selecting a Feature Profile.

- **Timestamp**: MiCollab Client Service uses the modification timestamp on LDAP objects to optimize processing. This is mainly used for display picture importing and MiCollab Client tries to import only those display pictures which have changed on the LDAP server since the last time MiCollab Client did a successful sync.
  - **Timestamp attribute**: This is the attribute name of the LDAP field which contains the modification timestamp. In case of Active Directory, the attribute is ***whenChanged***. If your LDAP server has some other attribute name, specify that instead.

Note:
If this attribute is left blank, MiCollab Client Service will try to import display pictures for all eligible accounts, regardless of when they were modified. While a blank timestamp attribute is not a recommended configuration for regular use (because display picture import can consume substantial cpu/memory), it can be used to force a re-import of all display pictures if required for troubleshooting, error recovery, etc. To do this, blank out the timestamp attribute and perform a sync. After the sync, set the timestamp attribute back to its original value and sync again.

- **Timestamp syntax**: The format of the timestamp value contained in the timestamp attribute. For Active Directory, this is X680 format. Some older LDAP servers may use the X208 format.

2. Do one of the following:

- If you are adding a new AD/LDAP synchronizer, click **Next**.
- If you are editing an existing synchronizer, click **Save**.

3. Configure the **Field Mappings** between the directory and the MiCollab Client accounts.

   Field Mappings specify how AD/LDAP database fields are mapped to MiCollab Client account fields when the information is synchronized.

   a. If required, edit the default values in the **Account Information** field. The table below defines the field mappings from AD/LDAP objects to MiCollab Client accounts. Based on the fixed label and description provided for each field, determine if you need to edit the default values. To edit a field, delete the existing value and type a new value in the text box.

Field	Default Value	Description
Directory key	objectGUID	This is the unique key that identifies the account in the directory. If the directory object does not have a value for this field, it is not imported.
PBX node	facsimileTelephoneNumber	Identifies the PBX node, or switch, that the user's

Field	Default Value	Description
		phone is configured on. If the directory object does not have a value for this field, it is not imported.
First name	givenName	The user's first name. This field can be blank.
Middle name	initials	The user's middle name. This field can be blank.
Last name	sn	The user's last name. This field can be blank.
Login ID	sAMAccountName	The login ID that the MiCollab Client Desktop Client uses to authenticate with the MiCollab Client Service . This field can be blank.
Desk phone extension	ipPhone	The user's desk phone extension. This field can be blank.
Soft phone extension	otherIpPhone	The user's soft phone extension. This field can be blank.
Company name	company	The user's company name. This field can be blank.
Address	streetAddress	The user's street address. This field can be blank.

Field	Default Value	Description
City	l	The user's city. This field can be blank.
State/Province	st	The user's state. This field can be blank.
ZIP/Postal code	postalCode	The user's ZIP/postal code. This field can be blank.
Display picture	jpegPhoto	The user's display picture. This field can be blank.

b. Add, Edit, or Delete **Phone Numbers**, **E-mail Addresses**, and **Instant Message (IM) Addresses** from the existing tables.

c. Do one of the following:

- If you are adding a new AD/LDAP synchronizer, click **Done**.
- If you are editing an existing synchronizer, click **Save**.

After you create an AD/LDAP synchronizer, you can edit the associated fields at any time.

Refer to the Common AD/LDAP Field Mappings topic for information about field mappings between AD and LDAP.

1.8.3 PBX Nodes Tab

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab-integrated mode.

The PBX Nodes tab provides a table for the PBX nodes you have added to the Enterprise.

Select the Enterprise from the list box and the following information is displayed for each PBX node configured:

- **IP Address**: Indicates the IP address for the PBX server.
- **Description**: Indicates the description that you provide for the PBX node.
- **Version**: (MiVoice Business only): Indicates the software version the PBX is currently running.
- **Extension Length**: Specifies the number of digits used for extensions on the PBX node.
- **Voice Mail Number**: Specifies the voice mail extension for NuPoint UM on the PBX node.
- **Last Sync**: Specifies the date of the last PBX node synchronization.
- **Sync Status**: Specifies the status of the last PBX node synchronization. Results include **In Progress**, **Success**, **Success with Info** and **Failure**. You can view synchronization details from the PBX Node Details page.

Note:
For synchronization failures, refer to the Synchronization Error Messages topic.

CSTA settings

The following fields are only displayed when MiCollab Client is integrated with MiCollab and MiVoice MX-One or MiVoice 5000.

- Port: Type the port MiCollab Client uses for MiVoice MX-One or MiVoice 5000 . This setting should remain at default. If the PBX port number changes, the PBX administrator needs to inform you so you can modify this setting.
  - MiVoice MX-One : Default value is 8882.
  - MiVoice 5000 : Default value is 3211. In rare instances, there may be multiple ports for the MiVoice 5000 . Type the port numbers, up to three, separated by a semi-colon.

Note:

If you change the Feature Access Code on UCA, you need to restart the client.

- Extended checking of the phone device: Default is Off. Turn on only when directed by support.
- Print PDU: MiVoice 5000 only. Default is Off. Turn on only when directed by support.
- Number of log files: MiVoice 5000 only. Type the number of log files to store. Default value is 10.
- Maximum file size: MiVoice 5000 only. Type the maximum log file size. Default value is 3 MB.
- Protocol file: MiVoice 5000 only. Type the name of the file used for the trace. Default is pdutrace.
- XML trace active: MiVoice MX-One only.
- Use phone number block: Type the device range to handle devices only in this range. For MiVoice 5000 the range is 2001 to 3001
- Group Call Pickup Feature Access Code: This option is visible to both PBX types, MX-One and MiVoice 5000. This option helps to store the feature access code which is provisioned in MX-One for Group Call Pickup in the UCA database.

Note:

If the Group Call Pickup Feature Access Code (FAC) is changed in the administrator portal, then no notification is sent to the clients. Clients will need to re-login to get the updated FAC details.

Note:

MiVoice 5000 : PDU log files are stored in the default log folder for CSTAProxy / UCA: /opt/intertel/log. View and retrieve PDU log files using the default MiCollab log file viewer.

You can complete the following tasks for PBX nodes:

- Sort the information in the table.
- Select one or more entries in the table.
- Click the Add Node link to add a PBX node.
- Click the PBX node link in the **IP Address** column to edit the PBX node.
- Delete a PBX node.

  To delete a PBX node:

  1. Select the node you want to delete from the PBX node list.
  2. Click the **Delete Node** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the node, or click **Cancel** to cancel the deletion.
- Synchronize specified PBX nodes.

  To synchronize one or more nodes:

  1. Select the nodes you want to synchronize.
  2. Click the **Synchronize** link. A dialog box appears prompting you to confirm the synchronization.
  3. Click **OK** to start the synchronization, or click **Cancel** to cancel the synchronization.

> **Note**:
> The **Synchronize** link only appears when the PBX Node Synchronizer has been enabled on the Synchronization tab. The **Synchronize** link does not apply to multi-node Mitel MiVoice Office 250 sites that are configured for synchronization with a CT Gateway. For this type of configuration, all of the nodes can be synchronized using the **Sync Now** button on the Synchronization tab.

- Click  to open the PBX Administration Tool .

  Using the PBX administrator's Web window, you can complete configuration, maintenance, and diagnostic tasks for the PBX node, without logging out of the Unified Communications administrator interface. Close the PBX administrator's Web window when you have finished updates to the PBX node.

- Click  to complete a Line Monitor Cache refresh (***MiVoice Business only***).

  During a Line Monitor Cache refresh, the MiCollab Client Service requests updated information for the MiVoice Business phone lines configured for MiCollab Client . On average, the refresh takes one second per single-line set and two seconds per three or four-line set.

  Note:
  System Performance . During a line monitor cache refresh, clients are taken offline temporarily, and then automatically returned to service with the new line configuration. Schedule line monitor cache refreshes during low traffic periods. No server reboot is required.

- Refresh the information on the page.

1.8.3.1 Adding and Editing PBX Nodes

You can add new PBX nodes and edit existing PBX nodes on the PBX Node Details page.

Note:
The fields on the PBX Node Details page vary between MiVoice Business , MiVoice Office 250 , MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400 PBX nodes. Some fields are PBX-specific and do not appear if they are not required for the PBX.

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab - integrated mode. MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400 are only supported in MiCollab integrated mode. Refer to the MiCollab Administrator Help for more information.

If you are configuring multiple MiVoice Office 250 nodes, click here to review information about using a CT Gateway.

For multiple MiVoice Office 250 nodes, you can streamline the synchronization process by configuring synchronization between the Unified Communications server and a single CT Gateway supporting the multi-node configuration.

After you configure the CT Gateway for synchronization, you do not need to complete synchronizations for each PBX node. When the MiCollab Client Service synchronizes with the CT Gateway, the required data for all of the associated PBX nodes is updated on the Unified Communications server.

To configure CT Gateway synchronization:

1. Add each PBX node in the multi-node configuration to the MiCollab Client Service (Adding and Editing PBX Nodes).
2. Add the CT Gateway as the final PBX node in the configuration (Adding and Editing PBX Nodes).
3. Configure PBX Node synchronization (Synchronization tab).

Remember the following guidelines when configuring a CT Gateway for multiple MiVoice Office 250 nodes:

- You cannot synchronize individual PBX nodes. However you can synchronize all nodes using the **Sync Now** button on the Synchronization tab.
- All PBX-node level settings, including **Voice mail server** and **Voice mail public number**, should be configured for the actual PBX node, and not the CT Gateway node.
- Each node's Session Manager must have a DB Programming account with a password that matches the password set for the single CT Gateway node.
- The CT Gateway must be running software version 4.4.01 or higher.
- All nodes configured on the CT Gateway must be communicating (up and working) so that the PBX synchronizer will synchronize all of the accounts. If one or more of the MiVoice Office 250 nodes are not communicating with the CT Gateway, the node will not be synchronized as indicated by the message that is generated under the PBX Nodes tab.
- All nodes connected to the CT Gateway must be using OAI protocol version 10.0 or later (MiVoice Office 250 v3.2 or later). Node connections to the CT Gateway that are not running protocol version 10.0 or later must be removed from the CT Gateway, or the nodes must be upgraded to v3.2 or later.
- It is recommended that all duplicate extensions between nodes be removed before installing the CT Gateway. If this is not done, one of the accounts with the duplicate extension information will be deleted during the synchronization.

Note:
You are not required to configure the resilient node.

To add or edit a PBX node:

1. Configure the PBX node Settings.

- **Description**: (*Required*) Type a name for the PBX node. By default, this field is blank. The Description field is limited to 1-64 characters in length, and must contain alpha-numeric characters (dashes and spaces included).
- **Hostname**: (MiVoice Business Only - ***Required***) Type the IP address or hostname for the MiVoice Business PBX node in this field. By default, this field is blank.

Note:
The values for the following read-only fields apply to MiVoice Business PBXs only and are generated after the MiCollab Client Service synchronizes with the PBX.

  - **Version**: Indicates the software version that the MiVoice Business PBX is currently running.
  - **Handoff feature code**: Indicates the feature code programmed for the Handoff feature on the MiVoice Business PBX.

  As a prerequisite, the MiVoice Business Feature Code for Handoff must be programmed. If this feature is added to an existing server, the PBX need to be synchronized with MiCollab Client before the feature can be used.
- **Internal IP address/hostname**: (*MiVoice Business only - Required*) Type the internal IP address or hostname for the Mitel MiVoice Business PBX node in this field. If your PBX configuration includes an expanded Processing Server (PS1), type the IP address of the base server in this field and type the IP address of the PS1 in the OAI IP address/hostname field.
- **External IP address/hostname**: (*Mitel MiVoice Business / Mitel MiVoice Office 250 Only - Optional*) Type the external IP address or hostname for the PBX node. This field applies to remote MiCollab Client softphones in teleworker mode. The External

IP Address/Hostname provides a communication path between remote users and the PBX. By default, this field is blank.

- **Extension length**: (*Required*) Extension length is the maximum length that can be configured for a PBX DN. The DN extension can range from 1 to the maximum extension length. Select the number of digits used for internal extensions on the PBX. Options include 3-7 digits. By default, this field is set to 4.
- **Registration code**:(*MiVoice Business Only-Required*) Type the registration code as configured on the MiVoice Business PBX. The valid length is 1-10 digits, and valid characters include 0-9, *, and #.

  The registration code corresponds to the Set Registration Access Code or Set Replacement Access Code, programmed in the MiVoice Business System Administration Tool (Systems Options Assignment form). These codes, typically 3 characters in length, can be a maximum of 10 characters long. A single Set Registration and Set Replacement Access Code applies to all IP devices on the system. Set Registration and Set Replacement Access Codes make up the first part of an IP device Personal Identification Number (PIN). The second part of the PIN is the IP device extension. For example, if an IP device has a PIN of 9991000, 999 is the Set Registration/Replacement Access Code and 1000 is the extension number.

  The registration code can be one to 10 characters in length, and can include digits 0-9, *, and #. By default, this field is blank.
- **Dialing prefix**: (*Optional*) Type the number that the user dials to obtain an outside line on the system. The dialing prefix is inserted automatically when the user makes a call from the History view, or from an imported contact. The dialing prefix can be 1-32 digits in length, and can include digits 0-9. By default, this field is blank.

  The dialing prefix is not inserted by MiCollab Client when the number dialed starts with the ‘-‘ character (a hyphen). For example, if the number dialed by the MiCollab Client is -4809619000, then the number dialed by the PBX is 4809619000 (without the hyphen). If the number dialed by the MiCollab Client is 4809619000, then the number dialed by the PBX is 94809619000, where 9 has been defined as the PBX node outgoing prefix.
- **Voice mail server:** (*Specific to NuPoint voice mail only - Optional. If an embedded voice mail is in use, then do not enter it.*) Type the IP address or hostname for the node’s voice mail server. The voice mail server configured here serves all accounts assigned to this node. If this field is left blank, all accounts assigned to this node will use the voice mail server configured on the Enterprise tab. If required, you can configure a different voice mail server on a user's account, which will override the voice mail server you configure here and on the Enterprise tab. The voice mail server can be 1-128 characters in length.
- **Voice mail number**: (*Required*) Type the voice mail extension for NuPoint UM. If required, you can configure a different voice mail extension on a user's account,

which will override the extension you configure here. The voice mail number can be 1-32 digits in length, and can include digits 0-9. By default, this field is blank.

If MiCollab Client is running in integrated mode and you change the voice mail number, it is applied to all MiCollab Client accounts on the PBX. If MiCollab Client is running in co-located mode, it is just applied to new accounts (see following option).

- **Apply voice mail number to all accounts**: (*Optional*) This option is only present when MiCollab Client is running in co-located mode. It allows you to quickly change the **Voice mail number** for all accounts on the node configured for the same voice mail number. After you change the Voice mail number, select this option, and then click **Save**. All accounts that were configured for the previous Voice mail number are updated to the new Voice mail number.
- **Voice mail public number**: (*Optional*) Type the voice mail public number for NuPoint UM. If required, you can configure a different voice mail public number on a user's account, which will override the voice mail public number you configure here. The voice mail public number can be 1-32 digits in length, and can include digits 0-9. By default, this field is blank.
- **No answer timer**: (*Optional*) Type an amount of time, in seconds, slightly less than the amount of time that will elapse before an incoming unanswered call is directed to voice mail. This setting is used by MiCollab Client for call forwarding. The No answer timer can be 0-60 seconds in length. By default, this field is set to 16 seconds.
- **Username**: (*Required only for* MiVoice Business) Type the username of the preconfigured account on the PBX node that will be used by the MiVoice Business PBX node synchronizer. The username field can be 1-64 characters in length. By default, this field is blank.

  To configure an MiVoice Business PBX node synchronizer, an administrator user account must exist on each MiVoice Business node (User Authentication Profiles in the MiVoice Business System Administration Tool). This account must have System Access enabled. The MiVoice Business user name and password must be specified in the properties of each switch that will be synchronized.

  Note:
  For security reasons, you can create an administrator user account that has System Access enabled, with No Access as the assigned Access Type using the System Administrator Policies form.

- **Password**: (*Required only for* MiVoice Business) Type the password of the preconfigured account on the PBX node that will be used by the PBX node

synchronizer. This is the password for the MiXML, and MiTAI connection to the node. The password can be 1-64 characters in length. By default, this field is blank.

Note:
Make sure that you enter the correct MiVoice Business System login credentials. If the credentials are incorrect, the ***PBX_PROXY_MitaiOpenPBXFailed*** alarm is triggered. If this occurs, reenter the correct credentials, and restart the ***PBX_PROXY*** module from the ***MiCollab Client Service Diagnostics*** page or perform a **Line Monitor Cache** refresh from the ***PBX Nodes*** page. The login credentials that you reenter take effect only after you perform either of these two operations.

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

- **Internal OAI IP address/hostname:** (***Mitel MiVoice Office 250 Only)*** This field is only required when the Mitel MiVoice Business PBX node includes an expanded Processing Server (PS-1). Type the internal IP address of the PS-1 in this field. Type the IP address of the base server in the Internal IP address/hostname field.
- **External OAI IP address/hostname:** (Mitel MiVoice Office 250 Only -Optional) This field is only required when the Mitel MiVoice Business PBX node includes an expanded Processing Server (PS-1). Type the External IP address of the PS-1 in this field. This field applies to remote MiCollab Client SIP softphones in teleworker mode. The External IP Address/Hostname provides a communication path between remote users and the PBX. By default, this field is blank.
- **OAI port** (***Mitel MiVoice Office 250 Only - Required)***: Type the port number used for the OAI connection to the MiVoice Business node. The range for this field is 1-65,535. By default, this field is 4000.
- **OAI password**: (***Mitel MiVoice Office 250 Only - Optional)*** Type the password of the preconfigured account on the PBX node that will be used by the PBX node synchronizer. This is the password for the OAI connection to the node. The password can be 1-64 characters in length. By default, this field is blank.
- IP/Digital Telephone Database Programming Password: (***Mitel MiVoice Office 250 Only – Optional***) Type the password required by Administrator phones, when

programming the Mitel MiVoice Business system through the phone. The password can consist of up to eight numeric characters. By default, this field is blank. In Mitel MiVoice Business Database Programming, this field is located under System \Phone-Related Information\IP/Digital Telephone Database Programming Password \Edit Password.

- Language: (***Optional***) Select a language from the list if you want to override the Enterprise language settings for the PBX. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting overrides the PBX setting. The user's language setting determines which language the Welcome E-mail Message is generated in for that user.
- Reload Dialed Digits Processing Template Files: Select the dialed digits processing logic to be used when a MiCollab Client user enters a phone number from the client. Once the dialed digit processing files are modified, clicking on this button will reload the files into the MiCollab Client system. This will update the processing logic for all PBXs across all enterprises on that MiCollab Client Service .

Note:
The dialed digits processing logic should not be modified unless instructed to do so by Mitel support personnel. Since this affects the very way numbers are dialed from MiCollab Client , incorrect processing may render useless large parts of the system.

2. Configure the Plus Dialing Settings .

   This area of the PBX Node Details page includes fields for specifying plus dialing settings.

Note:
Starting with MiCollab Client 5.1, some of the dialed digit processing happens locally within MiCollab Client. Due to this, if some dialing settings are changed in the server-manager, all clients within that enterprise (or for that PBX) should be restarted. Following are the settings affected by this:

- At the enterprise level:
  - Plus Dialing settings -> Country code
  - Plus Dialing settings -> International access code
  - Plus Dialing settings -> Long distance access code
- At the PBX Node details level:
  - Plus Dialing settings -> Country code
  - Plus Dialing settings -> International access code
  - Plus Dialing settings -> Long distance access code
  - Extension length
  - Dialing prefix

The plus dialing settings include:

- Country code: This field should be set to the country code of the country where the PBX resides. If an E.164 call is placed to a number within the user's "home" country, the country code will be stripped off of the digit string by MiCollab Client .
- International access code: This field indicates the international dial code that must be dialed for international calls from the country where the PBX resides. If the MiCollab Client determines that the call is being placed outside of the user's country (based on the PBX country code), MiCollab Client will pre-pend the International Prefix.
- Long distance access code: This field indicates the Toll digit for the country where the user's PBX resides. For any E.164 dialed calls within the user's home country, MiCollab Client will prepend the toll digit.

Note:
It is important that sites using E.164 (plus dialing) settings set up ARS on the PBXs to strip the Toll Digit for local calls.

Note:
The Plus Dialing Settings on the PBX Node tab override those on the Enterprise tab.

Note:
starting with + and strips the (0) from the digit string before processing the dialed digit string for insertion of the international access code and the long distance code. This change addresses the needs of European customers who have numbers such as +44(0)<number> in their contacts. The (0) in the number is optional, based on the location from which the user is calling the number. For example, if the number +44(0)6665544 is dialed from the MiCollab Client by a user in the United States SA, then the number dialed by MiCollab Client is 011446665544 where 011 is the international access code and 44 is the country code of the United Kingdom. If the same number is dialed from the MiCollab Client by a user within the United Kingdom, then the number dialed by MiCollab Client is 006665544, where 0 is the dialing prefix, the dialing prefix, and also the long distance code defined for the PBX node under the Plus Dialing settings.

3. Configure the CLID Translation.

   CLID Translation: This field is only applicable to 3300 type PBX. This field should be set to a list of comma separated digits (such as 0, 00). The MiCollab Client Service will them remove these leading digits from incoming numbers before generating call records and call history information.

   At most, one digit string (the first one that is applicable) will be applied to any given number. For example, suppose the incoming number is 001143476276 and the CLID translation is specified as 00, 11. The MiCollab Client Service will translate

that number into 1143476276, due to the fact that the first CLID translation string (00) matched the leading digits of the incoming number. The fact that the next CLID translation string (11) matches the now leading digits of the incoming number is inconsequential because the CLID translation has already been done once.

Note:
This feature is only applicable to 3300 type PBX.

Note:
Whitespaces in the field are ignored.

Note:
If the field is empty, then the CLID translation settings at the enterprise level will take effect. If the enterprise level CLID translation string is empty as well, then no translation is done.

4. Configure the default Dynamic Status Phone Settings. Set the defaults according to the PBX node type: MiVoice Business or MiVoice Office 250 .

   These default settings are used on the Dynamic Status page in the desktop client.

   - Forward my calls to:
     - Use PBX Default *(default)*
     - Voice Mail

Note:
The Under these conditions option is available only if Forward my calls to is set to Voice Mail.

- Under these conditions:
  - Busy *(default)*
  - No Answer
  - Busy and No Answer

  These default settings are used on the Dynamic Status page in the desktop client.

- When I am on the phone:
  - Use PBX Default *(default)*
  - Voice Mail
- If I do not answer:
  - Use PBX Default *(default)*
  - Voice Mail

5. *For MiVoice Business PBX nodes*, schedule Line Monitor Cache refreshes.

   During a Line Monitor Cache refresh, the MiCollab Client Service requests updated information for the MiVoice Business phone lines configured for MiCollab Client . On an average, the refresh takes one second for a single-line set and two seconds for three and four-line sets.

Note:

System Performance During a line monitor cache refresh, clients are taken offline temporarily, and then automatically brought online to the service with the new line configuration. Schedule line monitor cache refreshes during low-traffic periods. No server reboot is required.

To schedule line monitor cache refreshes:

a. Select a day or days of the week to perform the refresh.
b. Select an hour, minute, and specify AM or PM to schedule the refresh.

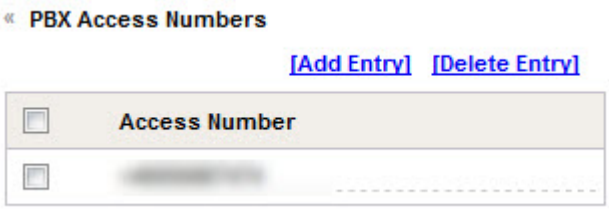
6. *For MiVoice Office 250 PBX nodes,* skip to the step 4.
7. Configure the **PBX Access Numbers**.

   This number is used for Call Through feature and should match the DID number (DID number terminating on the Hot Desking Access Number) configured on MiVoice Business and the R3 number configured on MiVoice MX-ONE. Multiple access numbers can be configured depending on the PBX configuration.

Note:
Call Through feature is supported on MiVoice Business 8.0 SP3 and later and MiVoice MX-ONE 7.0 and later.

To configure the PBX access number in MiCollab:

a. Go to **MiCollab Client Service** > **PBX Nodes** and select the node to be used.
b. Under **PBX Access Numbers**, click **Add Entry**.



c. Enter the Access Number in the **Add value** text box.

Note:
It is recommended that you configure the PBX access numbers in E.164 format so that these numbers can be dialed from any country. For example, the Country Code for India is +91, and the PBX Access Number will be +91xxxxxxxx.

d. Click **Save**.

To add multiple access numbers, repeat steps 2 through 4.

To delete an access number, select the number and click **Delete Entry**.

Note:
For Call Through feature to work, configure the PBX and MiCollab for Mobile Client as mentioned in the below sections.

PBX configuration for Call Through feature MiVoice Business configuration

- **T1 PRI and Hot Desking Access Number configuration**

  T1 PRI Trunk must be configured. For information on Trunk Configuration, see *MiVoice Business System Administration Tool Online help*.

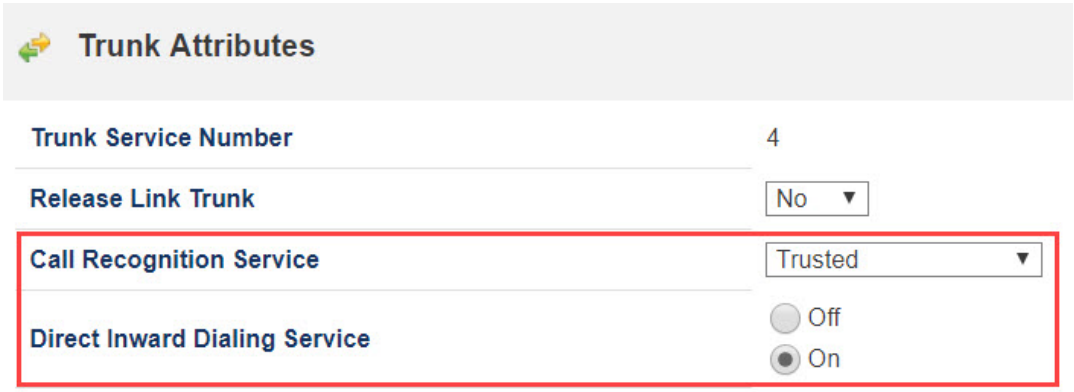
  The Hot Desking Access Number must be configured on MiVoice Business and a corresponding PSTN access number (DID) must be configured on the MiVoice Business and the PSTN gateway. This PSTN access number must be configured to route the calls to the Hot Desking Access Number. For more information about

configuring the Hot Desking Access Number and the DID number, see *MiVoice Business System Administration Tool Online Help*.

- Call Recognition Service (CRS) configuration

To define trunk attribute parameters:

a. Go to **MiVoice Business System Administration Tool** > **Trunk Attributes** form.
b. Select the configured **Trunk Service Number** (for the above T1 PRI Trunk) and click **Change**.
c. Select **Trusted** against **Call Recognition Service** and select **On** against **Direct inward Dialing Service**.



d. Click **Save**.

- Suppress Dial Tone configuration

When the called party ends the call, the calling party (initiating the Call Through call) receives a dial tone. This can be turned off from the **Hot Desk External User – Dial Tone on Call Complete** setting in *MiVoice Business System Administration Tool> Class of Service Options* form.

- DTMF Tone configuration

Call Through feature is dependent on CRS being activated. For added security, a Class of Service feature must be enabled for users to be able to have their DTMF tones acted on by the call manager. This can be enabled from the **Hot Desk External**

User – Allow DTMF Dialing setting in *MiVoice Business System Administration Tool> Class of Service Options* form.

MiVoice MX-ONE configuration

- **T1 PRI configuration**

  T1 PRI number must be configured on MiVoice MX-ONE. For more information about creating a trunk code and configuring the PRI Trunk, see *MiVoice MX-ONE Provisioning Manager User Task > Users* section.
- **Remote Number R3 configuration**

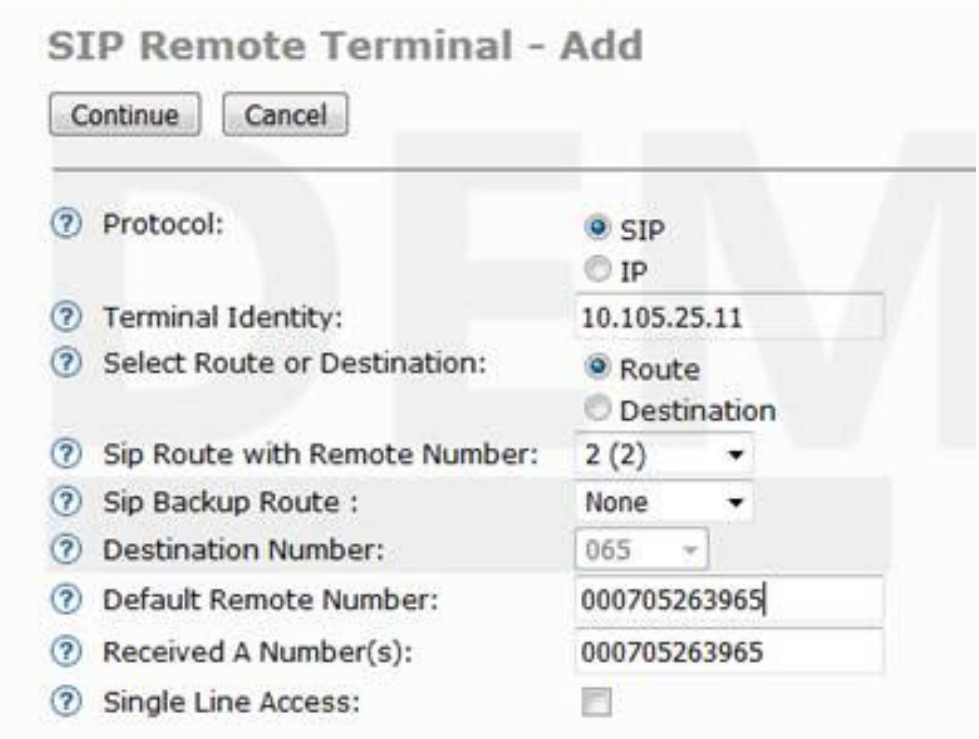
  a. Create the Remote Number R3 for the user.

  b. Configure the user in MiVoice MX-ONE Provisioning Manager:

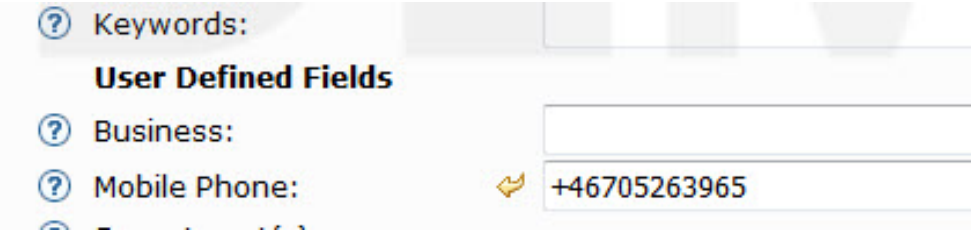
  c. Provision the Remote Extension number.

  i. Initiate a remote extension for ISDN Trunks(under **Services**> **Extension**).

  ii. Initiate a remote extension for SIP trunks.



iii. Enter the mobile number for the user (under **Users**> **User**).



Note:
Make sure that the mobile number is configured for the user in MiCollab Server Manager (Users and Services).

- **Subscribing Centralized Call History from MiVoice MX-ONE**

  In the **Call Log Settings** tab, you can enable or disable the Centralized Call History feature on MiCollab. If you enable this feature, MiCollab Server synchronizes Call History logs for all its users from the interfacing MX-ONE. MiCollab does this by subscribing to the MX-ONE for Call History events for all configured phone numbers of its users.

Note:

If this feature is disabled, MiCollab Client Service shall not subscribe to the MX-ONE for Call History events and will behave as earlier, that is, it will create its own Call History entry in its database whenever any user completes any incoming, outgoing, or missed call.

Note:

This feature is available on MiCollab version 9.5 onward and shall only work with MX-ONE version 7.4 SP1 or above.

It is necessary that you configure the appropriate settings on MX-ONE and MiCollab to enable the Call History feature.

Configuration on MX-ONE:

a. Must enable the **Enable Centralized Name And Number Log** for all MX-ONE CSPs for which this feature is required. There are two ways to do this:

- **Using SNM User Interface:** From the **SNM** tab, select **Telephony**> **Extension**> **Common Service Profile**. Select the CSP that is required to be modified, and then select the **Service Category**tab. After this, click on the **Enable Centralized Name And Number Log** checkbox to enable it for the selected CSP. Do these steps for all CSPs for which this feature needs to be enabled. Refer to the MX-ONE document on SNM GUI for more details.
- **Using the command line:**Set attribute **cnnlog**to **1x** for all the extension profiles of MX-ONE for which this feature is required. Refer to MX-ONE documentation [Section 6.1.2 of Document ID 38_15431-ANF90114] for details on how to set this attribute.

Note:

Without enabling **Enable Centralized Name And Number Log** settings for all the required CSPs, MX-ONE will send empty responses preventing MiCollab Client users from viewing the updated Centralized Call History entries on the Client UI.

b. FQDN of MiCollab Client Service must be reachable from MX-ONE. This is done using 'sudo -H mxone_maintenance' on MX-ONE and then select **DNS settings** > **Forwarders** > **Change setting for DNS forwarding**. Alternatively, you can provide an entry of MiCollab Service's hostname and IP address in the /etc/hosts file of MX-ONE. Refer to MX-ONE documentation for details on DNS forward settings.

c. Valid SSL certificates must be deployed on the MX-ONE so that MiCollab server communicates with MX-ONE over HTTPS. Without a valid certificate on MX-ONE, the feature would not work, and enabling this feature on MiCollab shall fail.

d. It is recommended to create a new DN (Directory Number) on the MX-ONE system, and then specify the same DN and password for the **Username**and **Password**fields under **Enable Centralized Call History** checkbox on the MiCollab Client Service Admin Portal. Refer to below **Configuration on MiCollab** section for more details.

Note:

If you modify the DN and (or) password on the MX-ONE, you must also update the **Username** and **Password** fields for the **Centralized Call History feature** on the MiCollab Client Service Admin Portal.

Configuration on MiCollab:

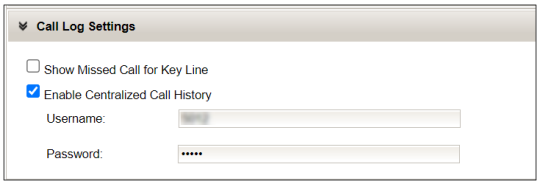
a. Valid SSL certificates must be deployed on MiCollab → Web Server so that MX-ONE can send Call history events securely over HTTPS.

b. To enable the Centralized Call History feature on MX-ONE, go to **MiCollab Client Service** > **Configure MiCollab Client Service** > **Enterprise Call Log Settings**, and configure the settings for the **Centralized Call History** feature.

- Select the **Enable Centralized Call History** check box, and then provide correct values in the **Username** and **Password** fields.

Note:

For **Username** and **Password** fields, provide the same DN and password that were created initially as specified in the step (**d**) of **Configuration on the MX-ONE**section.



c. After configuring the above-listed settings, click **Apply**. The server will validate the credentials (user name and password). If the credentials are valid, the feature will be enabled and the server will be subscribed to MX-ONE for the Centralized Call History feature for all users.

Note:

If the DN and (or) password are incorrect, the validation fails, in which case, the settings made will not be saved, and the Centralized Call History feature will remain disabled on the MiCollab.

Note:

Clicking the **Apply** or the **Reset** button will save or clear all the settings provided in the **Enterprise** tab.

Below are the possible failure scenarios when the admin tries to enable the **Centralized Call History** feature in the MiCollab Client Service Admin Portal:

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
I class="- topic/p ">Invalid Call History Username or Password	Admin has provided an incorrect user name and (or) password to enable the **Enable Centralized Call History** in the **Call Log Settings** tab.	Verify that the correct DN (Directory Number) and password are specified in the **Username** and **Password** fields. It must match the DN and password created on MX-ONE, as specified in step (d) of **Configuration on MX-ONE** section.
Server Error occurred during fetching of certificate from MX-ONE	MiCollab Client Service Admin Portal is unable to communicate with MX-ONE over HTTPS because the SSL	Check and correct the SSL certificate deployed on MX-ONE by

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
PBX: Unable to retrieve SSL certificate.	certificate on MX-ONE is either not installed or is invalid or expired.	referring to the MX-ONE documentation.
Server error during call history credentials authentication: connection refused or connection time out.	Due to network issues, a Timeout occurred while communicating with MX-ONE.	Try again after some time. If the problem persists, check the network connection between MiCollab and MX-ONE. Check whether all services are running appropriately on MX-ONE.
Error from MX-ONE PBX while validating Call History credentials - received 500 Internal Server Error.	MiCollab Client Service is unable to communicate with MX-ONE due to some 5xx response code from MX-ONE.	Check with the MX-ONE administrator to verify and solve the problem.
class="- topic/p ">Server error during call history credentials authentication: <error message>	MiCollab Client Service is unable to communicate with MX-ONE due to an error code.	Contact the MX-One administrator with the error message.

Below are the possible failure scenarios after the **Centralized Call History** feature is enabled on the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
MiCollab Client Service subscribes to MX-ONE for the Call History events for all the users.	Subscription to MX-ONE failed for one or more DN’s due to the 4xx or 5xx response code.	Carry out the appropriate steps according to the response code:

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
Note: The subscription request is sent in below three instances,		**a.** For the 401 or 403 response code, check and correct the **Username**and (or) **Password**field of the **Client Log Settings** tab on the MiCollab

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
• immediately after the Call History feature is enabled on the MiCollab Server,		Client Service Admin Portal. **b.** For the 408 (or request timeout) response code, check and correct the network

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
• after the restart of the MiCollab Client Service,	**Note**: The user DN for which subscription failed shall not be able to view the latest Call History logs from MX-ONE.	connection between MiCollab and MX-ONE.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
• and periodically after every 12 hours upon expiration of the subscription.		c. For any other 4xx response code, check the problem with the DN and take necessary action to correct its configuration on MX-ONE. d. For any other 5xx response code, check and confirm that MX-ONE and all its services are up and running. After taking the above remediation steps, try again by either disabling and enabling the feature or by restarting the MiCollab Client Service Admin Portal.
After the MX-ONE user completes any incoming, outgoing, or missed call, the MiCollab Client Service requests MX-ONE for the latest Call History records.	The request sent by the MiCollab Client Service to MX-ONE fails due to any other error response code. **Note**: Corresponding Call History entry will not be visible on MiCollab Clients.	Carry out the appropriate steps according to the response code: a. For the 401 or 403 response code, check and correct the **Username**and (or) **Password**field of the **Client Log Settings** tab on the MiCollab Client Service Admin Portal. b. For the 408 (or request timeout) response code, check and correct the network connection between

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
		MiCollab and MX-ONE. c. For any other 4xx response code, check the problem with the DN and take necessary action to correct its configuration on MX-ONE. d. For any other 5xx response code, check and confirm that MX-ONE and all its services are up and running. After taking the above remediation steps, try again by either disabling and enabling the feature or by restarting the MiCollab Client Service Admin Portal.
After the MX-ONE user completes any incoming, outgoing, or missed call, MX-ONE sends a Call History event to the MiCollab Client Service.	MiCollab Client Service did not receive the event sent by MX-ONE, due to which the corresponding Call History record is not visible on MiCollab Client.	To retrieve the unlisted Call History entries, either restart the MiCollab Client Service from the admin portal Or Try to disable **and** enable the feature again from the MiCollab Client Service Admin Portal.
MiCollab Client end user deletes single, multiple,	The request for deletion sent from MiCollab Client Service to MX-ONE fails,	Carry out the appropriate steps according to the response code:

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
or all Call History entries from any MiCollab Client.	due to which the MiCollab Client end user will not be able to delete the Call History entries. **Note**: An appropriate error message is displayed on the MiCollab Client UI.	a. For the 401 or 403 response code, check and correct the **Username**and (or) **Password**field of the **Client Log Settings** tab on the MiCollab Client Service Admin Portal. b. For the 408 (or request timeout) response code, check and correct the network connection between MiCollab and MX-ONE. c. For any other 4xx response code, check the problem with the DN and take necessary action to correct its configuration on MX-ONE. d. For any other 5xx response code, check and confirm that MX-ONE and all its services are up and running. After taking the above remediation steps, try again by either disabling and enabling the feature or by restarting the MiCollab Client Service Admin Portal.

class="- topic/p ">Scenario	class="- topic/p ">Problem	class="- topic/p ">Mediation
MiCollab Client end-user attempts to delete some Call History entries of MX-ONE while the admin has disabled the **Centralized Call History** feature in the MiCollab Client Service.	Cannot delete the MX-ONE Call History entries if the **Centralized Call History** feature is disabled. **Note**: Displays **Unable to remove Call History Records** on the MiCollab Client UI.	NONE - This is a known limitation.
The MiCollab Client Service is down, during which any MX-ONE user configured on MiCollab completes a call (incoming, outgoing, or missed) using a desk phone.	As a result, both the MiCollab Client Service and the MiCollab Client will not update the Call History entry for this MX-ONE call made by the user during the downtime.	During the startup of the MiCollab Client Service, the MiCollab Client Server fetches all the missed Call History entries for all users from the last updated date or time. If the Call history entries for the latest date or time for any DN are unavailable, the Server will retrieve Call History entries for the past 24 hours.

For all the failure scenarios described above, a Warning Alarm will be triggered, providing the details of the DN, error response code, and error message in the MiCollab Client Service Admin Portal.

Note:

In the MiCollab Client Service Admin Portal, the admin will be able to view the alarms (like Major, Critical, and Clean) based on the type of error. Go to the **Event log** page to view the relevant error details.

From a MiCollab Client end-user perspective, there will be no perceptible change in the MiCollab Client Call History tab. When you enable the MX-ONE call history feature, the Client will seamlessly work as earlier.

MiCollab for Mobile Client settings

To enable Call Through functionality in MiCollab for Mobile Client:

a. In MiCollab for Mobile Client, go to **Settings** > **General**.
b. Select **My Numbers** and tap **Mobile** or **Remote Extension** if configured.
   - For **Mobile**, tap **Call Through** to enable the setting.
   - For **Remote Extension**, tap **Call Through** and select the configured mobile number from the prompt to enable the setting.
c. Tap **Save**.

Note:
For more information on Call Through feature for end-users, refer to ***MiCollab for Mobile Client Quick Reference Guide*** > ***Call Through*** section.

8. For MiVoice MX-ONE only: Configure the **MX-ONE Status Settings** for the selected PBX node.
   - Select the **Disable MX-ONE Statuses** check box to disable the additional MX-ONE statuses and diversion profile integration for all users in the selected PBX node. The

default status **In the Office** will be selected for all users having an additional MX-ONE status.

- Clear the **Disable MX-ONE Statuses** check box to enable the additional MX-ONE Statuses and diversion profile integration for all users in the selected PBX node.

Note:
A confirmation is displayed after the settings are saved or created. Click **Ok** to apply the settings.

Click **Refresh** to view the current status of the operation:

- NONE
- FAILED
- SUCCESS
- Enabling In Progress
- Disabling In Progress

9. Do one of the following:

- Click **Create** to create the PBX node.
- Click **Save** to save the updated information for the PBX node.
- Click **Cancel** to return to the PBX Node tab without making changes.

You are returned to the PBX Nodes tab.

After you add a PBX node, configure the PBX node synchronizer, and perform a synchronization, you can view read-only synchronization details for the last synchronization completed.

To view synchronization details

Click **Synchronization Details** to expand the page. The details displayed include:

- Start Time
- Stop Time
- Status
- Details

To add System CLI Number

System CLI Number

Note:
This setting is applicable only for MiVoice Business Communication Platform.

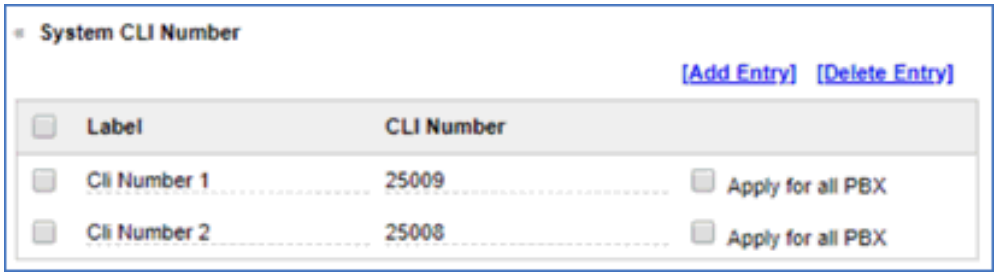
Note:
System CLI Number is applicable for calls made to external numbers only. This feature is not applicable for internal calls and softphone calls.

System Calling Line Identification (CLI) Number feature enables the caller to select which phone number must be displayed to the called party. The caller can select the preferred number from the**Edit status** > **Show my outgoing number** dropdown menu in the client. For each Dynamic Status, the users will have the option to select the preferred CLI Number for outgoing calls.

The administrator configures the CLI Numbers for users. The selected CLI Number will be displayed during outgoing CTI and Call Through (FMC) calls.

To configure the CLI Number in MiCollab:

1. Go to **MiCollab Client Service** > **PBX Nodes** and select the node to be used.
2. Under **System CLI Number**, click **Add Entry**
3. Enter the CLI Number in the **Add value** text box. Select Apply for all PBX, to add the CLI Number for all PBXs in the MiCollab Client Service.



4. Click **Save**.

To delete a CLI Number, select the number and click **Delete Entry**.

Note:
If a CLI Number is applied to all PBXs and the administrator deletes the CLI Number entry, the number will be automatically removed in all PBXs.

Note:
Privacy numbers cannot be used as CLI number. This is a limitation on MiVoice Business Communication Platform.

Note:
The Ring groups, Hunt Groups, Personal Ring Groups, and Multi Device User Groups having an associated DID number will be added automatically in CLI Number list on performing PBX sync.

Note:
Non-DID numbers MUST NOT be used as a CLI Number.

ONS Feature Settings

One Number Service feature will be disabled by default on MiCollab 9.2 server. To enable the feature, the administrator must clear the **Pre 7.3 MX-ONE** option.

Reload Dialed Digits Processing Template Files

Once the dialed digit processing files are modified, clicking the **Reload Dialed Digits Processing Template Files** button reloads the files into the MiCollab Client system. This

will update the processing logic for all PBXs across all enterprises on that MiCollab Client Service .

Note:
The dialed digits processing logic should not be modified unless instructed to do so by Mitel support personnel. Since this affects the very way numbers are dialed from MiCollab Client , incorrect processing may render useless large parts of the system.

1.8.4 Accounts Tab

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab Integrated mode.

The Accounts tab provides a table that lists all of the MiCollab Client accounts for each Enterprise.

Select the Enterprise from the list box and the following information is displayed for each account configured:

- **Type**: There are two types of accounts as indicated by the accounts icons:
- *Synchronized accounts* : These accounts are created automatically during synchronizations between the MiCollab Client accounts database and the AD/LDAP directory *or* PBX node database.
- *Manually-created accounts*: These accounts are created manually using the add or copy functions (see below).
- **PRG**: **Yes** indicates that the account has a Personal Ring Group (PRG) configured on the PBX. **No** indicates the account does not have a PRG.

Note:
For MiVoice Business 5.0 and later only, this field also enables Multi-Device User Groups. Note that with MDUG, once a user is busy in a call, any attempt by that user to originate a new call from another device within the MDUG group, using the MiCollab Client OR physically going off-hook from that device, results in a call failed indication.

- **Active:** Indicates if the account is active. This column is only shown if there is at least one account that is not active. Inactive accounts indicate that the account is not properly licensed.
- **Last Name**: Indicates the user's last name.
- **First Name:** Indicates the user's first name.
- **Desk Phone**: Indicates the extension for the user's desk phone.
- **Soft Phone**: Indicates the extension for the user's UC Advanced softphone.

Mitel Phone Model	MiVoice Business PBX	MiVoice Office 250 PBX
5020 IP Phone	yes	no
AppServerPort	yes	no
5224 IP Phone	no	yes

Note:
Provision the 3300 with 5020 IP device type for resilient MiCollab Client softphones.

Note:

SIP Softphone connected to MiVoice Business PBX must be configured as:

- Device Type = MiCollab Client Endpoint
- Key with Line Type = Multicall
- Button Dir. Number matching the number of the device
- Ring Type = Ring.

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

- **PBX Node**: Indicates the IP address for the PBX node server.

Note:
If the PBX Node column is blank, the account is considered to be in Teamwork mode and not associated with any PBX node.

You can complete the following tasks for accounts:

- Search for an account.

  The search function is not case sensitive and it is a "contains" type search versus a "starts with" type search. For example, if you search using the search string "br", the search will return all of the accounts that include "br" in either the first or last name.

  Searched fields include:

  - First Name
  - Last Name
  - Desk Phone
  - Softphone

  To search for an account:

  1. Type a search string in the Search text box. You can search accounts using:
     - Alphabetical characters: Type a name, a group of letters, or a single letter in the Search box.
     - Numeric characters: Type a full extension, a group of numbers, or a single number in the Search box.
  2. Click **Search**. The list of account names matching the search string is displayed.

  To clear the Search box, click Clear.
- Click Add Account to add a new account.
- Delete an account. **To delete an account:**

  1. Select the account you want to delete from the account list.
  2. Click the **Delete Account** link. A dialog box appears prompting you to confirm the deletion.
  3. Click **OK** to delete the account, or click **Cancel** to cancel the deletion.

- Send a welcome e-mail.

  Welcome e-mail messages provide the user with the following information and links:

  - MiCollab Client Login ID and Password (required to log in to MiCollab Client user interfaces)
  - Desk phone extension
  - Softphone extension
  - MiCollab End User Portal URL (provides access to the End User Portal)
  - MiCollab for PC Client (*micollab_pc.msi*) download URL, if MiCollab for PC Client is configured for the user
  - MiVoice for Skype for Business (*mivoice_sfb.msi*) download URL
  - MiCollab MAC Desktop Client download URL
  - MiCollab Mobile Client (iOS and Android) download URL
  - MiCollab Web Client download URL
  - MiCollab Client Quick Reference Guide URL (provides basic MiCollab Client installation and feature usage information)
  - Legacy Skype for Business Client (*MitelMiVoiceForLync.msi*) download URL
  - Local Android Client (*MitelUCAdvanced.apk*) download URL

  Before you send a welcome e-mail to the user, make sure you have programmed an e-mail address for the user's account in the **Contact Information** section of the Account Details page.

  To send a welcome e-mail:

  1. Select the account or accounts from the account list.
  2. Click the **Send Welcome E-mail** link. A dialog box appears prompting you to confirm the action.
  3. Click **OK** to send the e-mail message, or click **Cancel** to cancel.
- Sort the information in the table.
- Select one or more entries in the table.
- Activate an inactive account.

  To activate an account:

  1. Select the account you want to activate from the account list.
  2. Click the **Activate** link. A dialog box appears prompting you to confirm the activation.
  3. Click **OK** to activate the account, or click **Cancel** to cancel the activation.
- Click the First/Last Name link to edit account information.

- Click the copy icon  to quickly create a new account based on the values configured for the associated account.

  To copy account fields and create a new account:

  1. Select the account you want to copy and click the copy icon  . The Account Details page opens and the non-user-specific fields are populated with the values from the copied account.
  2. If required, edit the following pre-populated fields:
     - PBX node
     - Voice mail number
     - Language
     - Country
     - Feature Profile
  3. Complete the remaining user-specific account fields:
     - First name
     - Middle name
     - Last name
     - Login ID
     - Password
     - Desk phone
     - Soft phone
     - Mailbox number
  4. Click **Create**.
- Refresh the information on the page.

Note:
When adding an account manually the PBX node must be set to 'None' for account to be in Teamwork mode.

When using Active directory sync, the PBX node value in active directory should be set to <enterpriseId>.local and no deskphone or softphone number must be assigned to the user account in active directory.

1.8.4.1 About Login IDs

MiCollab Client credentials are communicated to the user via a Welcome E-mail Message that you can generate for each user after you provision the system.

MiCollab Client credentials include:

- Fully Qualified Domain Name (FQDN) for the MiCollab Client Service (required for the Desktop Client installation)
- MiCollab Client Login ID (simple, or fully qualified Login ID – used to log in to the MiCollab Client user interfaces)
- MiCollab Client Password (used to log in to the MiCollab Client user interfaces)

You can also log in to the MiCollab client using the UPN. The ***UserPrincipalName*** (UPN) attribute must be in the internet-style sign-in format where the username is followed by the @ sign and a domain name.

Note:
The UPN login is supported only in the integrated mode.

Note:
The presence of the peered users with the login ID as UPN will be seen only when both the peered servers are on MiCollab version 9.4 and above.

The value entered for the **Login ID** field on the Account Details page provides the simple Login ID for the user. If you are managing a single Enterprise deployment, users are provided with a simple Login ID (for example, john_smith) via the Welcome E-mail Message.

The Login ID:

- must be unique.
- supports ISO8859-1 characters.
- can be between 2 and 113 alphanumeric characters in length.
- can be numeric, but should not conflict with any other user's DN. The user can use his own DN as a Login ID.

The UPN login specifications are as follows:

- The userPrincipalName (UPN) attribute must be in the internet-style sign-in format where the user name is followed by the @ symbol and a domain name. For example, username@abc.com.
- The maximum number of characters for the UPN attribute is **113**. A specific number of characters are permitted before and after the @ symbol; the specifications are as follows:
  - maximum number of characters for the username, that is the characters before the @ symbol should not be more than 64
  - maximum number of characters for the domain name following the @ symbol should not be more than 48
  - the @ symbol is required in each userPrincipalName value
  - the @ symbol cannot be the first character in each userPrincipalName value
  - the username cannot end with a period (.), an ampersand (&), a space, or with the @ symbol
  - the username should not have spaces
  - routable domains must be used; for example, local or internal domains cannot be used
  - unicode is converted to underscore characters
  - userPrincipalName cannot contain any duplicate values in the directory

Note:

MiCollab does not support the @ character as the first or last character in the UPN value.

1.8.4.2 Adding and Editing Accounts

The Account Details page provides the fields and options to create and configure an account. At a minimum, you must configure the **Login Settings** and **Licensed Features** sections of the Account Details page, when you create an account.

Then at a later time, you can edit the account information, and provide additional details for the account.

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

In addition, chat history is managed on this page.

To create an account:

1. Configure the account Create Account Details**(Login Settings).**

- **First name**: Type the first name for the account holder.
- **Middle name**: Type the middle name for the account holder.
- **Last name**: (*Required*) Type the last name for the account holder.
- **Login ID (case insensitive)**: (*Required*) Type the Login ID that the account holder will use to log in to the Desktop Client (for example, <***first name_last name***>). You can use upper or lower case for this field.
- **Password**: (*Required*) Type the password that the account holder will use to log in to the Desktop Client.
- **PBX node**: (*Required*) Select the PBX node that provides phone service to the account holder. Select [**None**] if the account is in Teamwork Mode and not associated with any PBX node.

> **Note**:
> A Teamwork Mode account that has a PBX Node value of [None] can be later moved to a real PBX node if they get assigned a phone on that PBX. However, an account that is assigned to a real PBX node cannot be moved back to Teamwork Mode.

- **Mailbox number**: Type the extension for the account holder's mailbox extension.
- **Voice mail server**: (*Optional*) This field can be used to override the **Voice mail server** field configured on the PBX Node Details page for the PBX node associated with this account. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default. The maximum length is 128 characters, and must include a valid IP address or hostname.
- **Voice mail public number**: (*Optional*) This field can be used to override the **Voice mail public number** field configured on the PBX Node Details page for the PBX node associated with this account. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default. The maximum length is 32 characters.
- **Language**: (*Optional*) Select a language from the list if you want to override the Enterprise and PBX language settings for this account. You can configure the language parameter on the Enterprise, PBX, or account level. The Enterprise language field sets the default language for all accounts on the Enterprise. The PBX language setting overrides the Enterprise setting, and the account setting

overrides the PBX setting. The user's language setting determines which language the Welcome E-mail Message is generated in for that user**.**

- **Country**: Select the country that the account holder resides in.
- Refresh line monitors on save: MiVoice Business only. If the primary MiVoice Business was not running when MiCollab Client started, the Mitai monitors for non-resilient devices are not set. Select this option to restart the Mitai monitors and receive updated line configuration from MiVoice Business .
- **Reset dynamic statuses on save**: If there are PRG/MDUG provisioning changes, including the addition or deletion of phones from PRG/MDUG, dynamic status needs to be created. Select this option to recreate dynamic statuses for this account.

  - A status reset removes all custom statuses and custom routing rules created by the end user.
  - The account language setting is used to determine which language to use for the new statuses created by the system.
  - Users need to log back into MiCollab Client after dynamic statuses have been reset.
- **Presence Privacy Configuration Settings**: This setting controls whether the user's presence information (dynamic status, telephony status, video availability, and calendar advisory) is displayed to other users or not.

  Show Presence for User: This setting is only available if **Presence Privacy Service** is **Enabled** at the Enterprise level. By default the **Show Presence for user** setting is checked.

  - If this setting is checked, the presence information of users on local and peered servers is displayed.
  - If this setting is unchecked, no presence is shown to users on local and peered servers unless they are added in the presence allowed list of the user.

Note:
If show presence to all setting is enabled at the Enterprise level and disabled at the Account level, account setting will always take the priority over the Enterprise setting (the user's presence will be **status unknown** to other users).

Limitations:

- **Presence Privacy Service** is not supported in Co-located mode.
- On peered servers, the Presence Privacy setting at the local server will be given preference. For example, if the setting on peered server A is **Enabled** and the setting on peered server B is **Disabled**, peered user's presence will be displayed based on the local server setting and not the server where the user actually exists.
- Telephony presence status of other users does not turn off immediately. The user must re-login to the client. When user is re-logged into the client, telephony presence will turn off from corporate directory, call history, search tab, and from legacy console.
- Video call functionality will not work for those users whose presence privacy setting is enabled.
- In MiCollab peered server setup, if one of the server is at version lower than MiCollab 9.0, users on that server will see the presence information of all users on all the peered servers irrespective of presence feature is enabled or disabled on those servers.
- If MiVoice Business Controller is lower than 9.0 and InAttend servers are SIP-based subscription, enabling the presence privacy setting will not impact the dynamic status and the telephony presence (presence status will not change to **status unknown**).

2. Configure the Licensed Features for the account.

   Select a Feature profile to assign to the account.

   The following information is displayed for the Feature profile:

   - **Profile features**: A read-only list of features included in the selected profile.
   - **Add-on features**: The list of features available to select from that are *not* included in the selected profile.

   To add/remove features to an account:

   a. **Select/deselect the features from the Add-on features list.**
   b. **Click Save.**

   > **Note**:
   > Both Web Portal features are set automatically when you select either one of them.

3. Click **Create**. You are returned to the Accounts tab.

To complete the account configuration, click the account name from the Accounts tab, and edit the account information.

> **Note**:
> If creating a Teamwork Mode account through AD/LDAP synchronization, fill out all fields in active directory as you would for a regular account except for the following:
>
> 1. Set PBX node value to <enterpriseId>.local, where <enterpriseId> is the ID of the enterprise being created and can be found on Enterprise Tab.
> 2. Do not fill out fields for desk phone and softphone.

To edit an account:

1. Edit the account Edit Account Details**(Login Settings).**

- **First name**: Type the first name for the account holder.
- **Middle name**: Type the middle name for the account holder.
- **Last name**: (*Required*) Type the last name for the account holder.
- **Login ID**: (*Required*) Type the Login ID that the account holder will use to log in to the Desktop Client (for example, <*first name_last name*>). You can use upper or lower case for this field.
- **Password**: (*Required*) Type the password that the account holder will use to log in to the desktop client.
- **Reset Password on Save**: Select this option to reset the account password to a random value. When you click **Save**, an e-mail message providing the new password is sent to the user. Make sure you have programmed an e-mail address for the account under the **Contact Information** section of this page. If the account does not have a programmed e-mail address, an error message is generated and the option is cleared.
- **PBX node**: (*Required*) Select the PBX node that provides phone service to the account holder. Optionally, select [*None*] if this account is to operate in Teamwork mode.
- **Primary Extension**: (*Required only for Priority Ring Group PBX synch only*) Type the primary extension for the account holder. Select the type of device of this primary extension (from drop-down menu select Deskphone, Softphone or SIP).
- **Mailbox number**: Type the extension for the account holder's mailbox extension.
- **Voice mail server**: (*Optional*) This field can be used to override the Voice mail server field configured on the PBX Node Details page for the PBX node associated with this account. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default. The maximum length is 128 characters, and must include a valid IP address or hostname.
- **Voice mail public number**: (*Optional*) This field can be used to override the Voice mail public number field configured on the PBX Node Details page for the PBX node associated with this account. Leave this field blank if you want to use the value specified for the PBX node. This field is blank by default. The maximum length is 32 characters.
- **Country**: Select the country that the account holder resides in.
- **Allow user to upload display photo**: Select this option if you want to allow the user to upload and save a photo to the MiCollab Client Service . When the photo is uploaded to the server, it is displayed on this page along with the user's other

account information. The user's photo is then displayed in the MiCollab Desktop and Web clients.

- **Upload new photo**: You can also upload a photo of the user to the server if you have one available. Uploaded photos must adhere to the standard guidelines.

Standard guidelines to upload a photo:

- Supported photo file types include **.jpg**, **.png**, and **.gif**.
- The maximum file size for photos is 25600 bytes.
- The administrator's interface does not allow you to crop photos.
- All uploaded photos will be resized to 128x128 pixels.

To upload a photo:

a. Click **Upload New Photo**.
b. Browse to the photo location.
c. Select the photo and click **Open**.
d. Click **Upload**. The photo is displayed on the page.

To cancel the upload, click **Cancel New Photo**.

Note:
Do not update AWV password from **MiCollab Client Service Configuration Account** tab when MiCollab is in integrated mode because updating AWV password may cause authentication issue while using MiTeam Classic feature.

2. Edit the Licensed Features for the account.

- Select a Feature profile to assign to the account.
- The following information is displayed for the Feature profile:
  - **Profile features**: A read-only list of features included in the selected profile.
  - **Add-on features**: The list of features available to select from that are *not* included in the selected profile.
- **To add/remove features to an account:**

a. **Select/deselect the features from the Add-on features list.**
b. **Click Save.**

Note:
Both Web Portal features are set automatically when you select either one of them.

3. Edit the Phone Numbers for the account

   Select **Add** to create a new device:

   - **Type**: the type can be either Desk Phone, MiNet Softphone, SIP Softphone, Phone, PRG, or Voice Mail.
   - **Label**: Enter a label for each device created.
   - **Number**: Enter an extension number for each device created.
   - **Published**: The option to publish the phone numbers can be selected.
     - On MiVoice 5000 communication platform, if the **Published** setting is unchecked, the phone number of the user will be obfuscated. The Client also obfuscates the number in the **Call History** and **Voicemail** menu for the called party. The called party will not be able to call back or copy the obfuscated number.
     - If **Privacy Flag** is set to **On** in MiVoice Business communication platform and the **Published** setting is unchecked in MiCollab, then the number will not be visible in MiCollab incoming calls, Search results, Call History, Contacts menu,

contact card, activity tab, voicemail history, and notifications. Following are the limitations:

- If the unpublished number was previously recorded in the call logs before the feature was enabled, then the menus such as, search, call history, voicemail history, contact card (hover-over), activity will display the number.
- In the incoming call window, the **Decline with a chat** option will not be shown for the user with private DN.
- If the user publish/unpublish the number using their MiCollab Client, then the privacy feature is terminated and the number will be visible in the corporate directory and contact card.
- Contacts from the peered servers are automatically synched after an interval of 6 hours. For an immediate effect, user must restart their MiCollab Client manually.
- For voicemail with privacy DN, the Client will only be able to show the name of the party who sent the voicemail and the chat functionality will be disabled.
- This feature is compatible with MiCollab Client 9.3 and older MiCollab Clients (prior to 9.3) with MiCollab 9.3 server and Privacy DN **ON**. Restart the MiCollab Client to see the changes.

- **Video Capable**: The option to indicate if SIP softphone is video capable.

Note:
On other communication platforms, the number will not appear in the contact card, but incoming calls, call history, and voicemail history will display the number.

Note:
Publishing MDUG non-prime numbers is not supported in MiCollab. Use PRG to publish the non-prime numbers.

Select **Create**. When adding a MiNet softphone, a random, unique MAC address is created and appears here. If MiCollab Client is in co-located mode, the field can be edited. If MiCollab Client is in integrated mode, the field is read-only.

To **Delete**: select an existing device and select Delete

To **Edit**: select  next to the desired device.

When switching from SIP softphone to MiNet softphone perform the following procedure to register the MiNet Softphone:

a. Delete the user name folder in "`C:\Users\\AppData\Roaming\Mitel\UC\`"

CAUTION:
Deleting the application folder will also remove all the existing settings for the user.

b. Re-launch the Legacy MiCollab Desktop Client application.

c. Switch from SIP softphone to MiNet softphone.

4. Configure the account **Contact Information**.

- **Company name**: Type the account holder's company name.
- **Address**: Type the street address for the company.
- **City**: Type the city where the company is located.
- **State/Province**: Type the state where the company is located.
- **ZIP/Postal code**: Type the zip code where the company is located.
- Add, **Edit**, and **Delete** the following for the account:
  - Phone Numbers: Includes the following types:
  - PRG: Includes PRG extensions programmed on the PBX. You can edit the **Label** only for these types of phone numbers.
  - EHDU: Includes phone numbers programmed as External Hot Desk User devices. You can edit the **Label** and **Number** for these types of phone numbers.
  - Phone: Includes other devices programmed for the account. You can edit the Label and Number for these types of phone numbers.

> **Note**:
> By default, phone numbers are published to the Corporate Contacts list. Deselect the Published option if you want the phone number to remain unpublished.

- E-mail Addresses
- IM Addresses

5. Configure the Account Settings.

The **Account Settings** area on the Account Details page allows you to overwrite the Default Account Settings (configured on the Enterprise Tab) for the specified account. *If necessary*, configure the following settings for the account:

- **Phone Settings**: Configure the following for the account holder's phone:
  - *Account code length*: Select the number of digits for account codes. Options include 0-12. The default is 0.
  - *Auto Upgrade Client*: Auto upgrade client provides an option to control the automatic client upgrades.
  - • Select **Default** to retrieve the client upgrade information from the Enterprise setting. By default, this option is set to default.
    - Select **Enable** to push the automatic client upgrade (if there is a new version of the client available) for the user. The user will get a client upgrade pop-up notification.
    - Select **Disable** to disable the client upgrade for the selected user.
  - *Enable ACD features in client*: Select this option if you want the account holder to have access to the ACD view and corresponding features in the Desktop Client.
- **RSS Window**: Configure the following for the account holder's RSS window:
  - *URL*: Type the URL of the RSS Web page that you want to appear in the account holder's RSS window on the desktop client. For example, **http://www.mitel.com/RSSNewsRelease**. RSS feeds are formatted by a script on the Unified Communications server that provides an HTML scrolling interface to the user.
  - *Always On*: Select this option if you want the RSS window to always be visible in the account holder's desktop client.
  - *User Modifiable*: Select this option if you want the user to be able to modify the URL from the Desktop Client.
- **Collaboration**: Configure the following collaboration settings for the account holder:
  - *Username*: Type the username that the account holder uses to log on to the collaboration Web interface.

Note:
Set the Username equal to MiCollab Audio, Web and Video Conferencing e-mail address.

- *Password*: Type the password that the account holder uses to log on to the collaboration Web interface.
- *Collaboration server*: Select the account holder's collaboration server, or select [Default] to use the collaboration sever configured for the Enterprise.

- **Mobile Settings:** If desired, enable the **User can manage MiCollab corporate locations** option. When this option is enabled the user can manage Corporate Locations from his or her MiCollab Mobile Client and upload the information to the MiCollab Client Service . By default, this option is disabled.
- **Client Upgrade Settings:** Select **Do not provision new MiCollab Client for PC** option to disable provisioning MiCollab for PC for the selected user.

Note:
Use this option in case of mixed deployment of MiCollab Clients (Desktop Client and MiCollab for PC for different users).

Note:
If *Provision new MiCollab for PC* option under Enterprise tab is disabled, then **Client Upgrade Settings** will not modify the default settings.

- **Group Presence Control Settings**: The default value is false. If desired, select the **Users can manage group presence** checkbox to allow MiCollab for Mobile users on MiVoice Business integrations only to update their group presence and retrieve the group list. Enable this checkbox to display the **Ring Groups** in the left drawer of the MiCollab Client.

Note:
This feature is supported on MiVoice Business . If enabled for other PBX types, you will receive an error message indicating support for MiVoice Business only.

Note:
The **Group Presence Control** COS option must be enabled for extensions on MiVoice Business for this feature to work.

Note:
Admin must configure a Ring Group in MiVoice Business and the user's DN needs to be added as a ring group member. After the sync between MiVoice Business and MiCollab, the user will be able to see the **Ring Groups** menu in the left drawer of the MiCollab Client.

- **USB Devices**: Configure the following USB device options:
- ***User can configure local USB devices***: Select this option if you want the account holder to have the ability to configure USB devices on his or her computer using the MiCollab Desktop Client.
- ***User can manage USB device profiles***: Select this option if you want the account holder to have the ability to manage (upload, edit, delete) USB device profiles on the Unified Communications server from the MiCollab Desktop client. Mitel recommends that you enable this option for a very limited number of users (1-2) on the system.

Note:
Enabling this option, automatically enables the **User can configure local USB devices** option.

6. Click **Save** to save the account information.

Note:
Accounts synchronized with the PBX: After you complete phone extension configuration changes (add, delete, move, change) on the PBX, perform a manual synchronization (**Sync Now** button on the Synchronization Tab) to ***immediately*** update the affected MiCollab Client accounts. If you do not perform a manual synchronization, the affected MiCollab Client accounts will be updated at the next scheduled synchronization.

In addition, for those MiCollab Client users whose extensions are affected by the configuration changes you make on the PBX, instruct the users to exit and then restart their MiCollab Desktop Clients to refresh extension information.

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab - integrated mode.

MiVoice Conference/Video Phone devices must be set to video enabled in order to allow video calls. See MiVoice Conference/Video Phone device for further details.

1.8.4.3 View Audit Report

The **View Audit Report** page lists all the emergency location changes, including why the emergency responders went to the inaccurate address, providing the administrator to verify in case there is a mismatch.

Here the administrator will be able to view the following data as listed below.

The initial panel displays the emergency call reports made by the end user, and the second panel lists the existing record for the user where the user still has not made the emergency call.

Note:

Unless another emergency call is made, the same record will get displayed.

1. **Unique Device Id** - The unique device identifier.
2. **Time When Existing Location Is Fetched** - It is the time when the client fetches its existing location from the location service.
3. **Time When New Location Is Updated** - It is the time when the user updates a new location. In case when the client proceeds into a new network and updates the newly detected location on the location service.
4. **Location URI Received From Location Service** - The location URI received by the client from the location service.
5. **No Location On Client Time** - It is the time when the client does not have a location defined, and the red icon appears on the client.
6. **Emergency Number Call Time** - The time when the client initiated the call to the emergency number.
7. **Location URI Sent During Emergency Call** - The location URI sent by the client during the emergency call.
8. **Client Type** - The type of client sending the request (that is, MAC /PC /WEB/ Android and iOS).
9. **MNH Version and Client Build Number**- The MNH version and client build number details is displayed.

Note:

All the time attributes in the audit report panel will be displayed in the UTC format.

The administrator cannot clear the audit log, and by default there will be no records. Under normal circumstances that there will be 1 or 2 records per user.

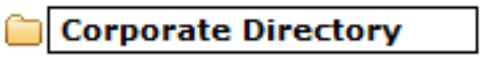
To download the audit records of a user, click the **Download** button at the bottom left of the window.

1.8.5 Corporate Directory Tab

The Corporate Directory tab provides a list of all the accounts for each corporate directory. When an account is included in the corporate directory, the user is listed as a corporate contact in the MiCollab Client Desktop Client Contacts view.

The directory structure for corporate directories varies based on how the corporate directory was generated.

Corporate directories generated from a PBX synchronization, or by manually creating the accounts include just one top level Corporate Directory folder .



All accounts are displayed in the Corporate Directory table, and there are no subfolders under the top-level Corporate Directory folder.

Corporate directories generated from an AD/LDAP synchronization typically include various organization groups and associated folders .

Subfolders, and the accounts that reside in them, correspond to the Organization Units present in the AD/LDAP Corporate Directory. If a folder is collapsed, you can expand it by doing one of the following:

- Click the arrow next to the folder.
- Click the name of the folder.
- Click the **Expand All** link.

If a folder is expanded, you can collapse it by doing one of the following:

- Click the arrow next to the folder.
- Click the **Collapse All** link.

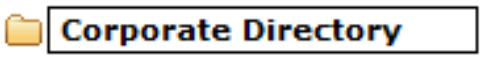
The corporate directory table provides the following information for the accounts in the directory:

- **Type**: There are two types of accounts as indicated by the accounts icons:
- *Synchronized accounts*  : These accounts are created automatically during synchronizations between the MiCollab Client accounts database and the AD/LDAP directory *or* PBX node database.
- *Manually-created accounts*  : These accounts are created manually using the add or copy functions.

- **Last Name**: Indicates the user's last name.
- **First Name:** Indicates the user's first name.
- **Desk Phone**: Indicates the extension for the user's desk phone.
- **Soft Phone**: Indicates the extension for the user's MiCollab Client softphone.

Local Corporate Directories

To see the list of accounts in the local corporate directory, click the top level **Corporate Directory** folder.



In some circumstances, you may not want to include all accounts as corporate contacts (for example, high-level company executives). You can remove individual accounts from the corporate directory, thereby removing the associated user from the list of MiCollab Client corporate contacts. Removing an account from the corporate directory group does not delete the account from the corporate directory. It merely removes the associated user from the list of corporate contacts in the MiCollab Client Desktop Client.

You can also **add** manually-created accounts to the corporate directory and include the associated users in the list of MiCollab Client corporate contacts.

For local corporate directories you can:

- **Sort** the information in the table.
- Select one or more entries in the table.
- **Refresh** the information on the page.
- Add accounts to the corporate directory.
- Remove accounts from the corporate directory.

To remove one or more contacts from the corporate directory group:

1. Select the contact you want to remove.
2. Click the **Remove** link. A dialog box appears prompting you to confirm that you want to hide the contact from the corporate directory group.
3. Click **OK** to remove the contact, or click **Cancel** to cancel the removal.

Peered Corporate Directories

To see the list of accounts for a peered server corporate directory, first expand the top-level Corporate Directory folder, and then click the sub-folder with the **Description** of the peered server (as configured on the Peer Server Details page).

When MiCollab Client Services are configured for peering, users are categorized by corporate directory in the MiCollab Client interfaces. Users between different corporate directories have equal access to presence information and communication features as they do with users from their own corporate directories. Users who have been removed from their corporate directory are not visible to other users.

For each peered server, the directory tree structure displayed under the local Corporate Directory folder mirrors the Corporate directory structure on the peer server itself. Because you do not have management access to peered corporate directories, the **Add** and **Remove** links will not appear when you click on a peered corporate directory folder.

For peered corporate directories you can:

- **Sort** the information in the table.
- **Refresh** the information on the page.

1.8.5.1 Adding Corporate Contacts

This page shows the list of accounts that are not currently included in the local MiCollab Client Service Enterprise's corporate directory group. When an account is not included in the corporate directory group, the associated user is not listed as a corporate contact in the MiCollab Client Desktop Client Contacts view.

You can add a synchronized account or a manually-created account to the local corporate directory group from this page.

Note:
You cannot add (or remove) accounts from a peered server corporate directory.

To add an account to the corporate directory group:

1. Select the account from the list.
2. Click **Add**. You are returned to the Corporate Directory tab, with the account added to the group.
3. Click **Cancel** to return to the Corporate Directory tab without adding accounts to the corporate directory group.

1.8.5.2 ACD Settings Tab

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

Automatic Call Distribution (ACD) is an optional feature for Enterprises using MiCollab Client . ACD is used by call centers to manage incoming calls to a single directory number. The calls are distributed among a group of logged in call center agents. When ACD is enabled for the agent, the Desktop Client provides an ACD view.

The ACD Settings tab includes fields and options used to configure ACD groups, account codes, and busy reasons. When an ACD agent starts his or her MiCollab Client , the MiCollab Client Service sends the ACD settings to the client and populates the ACD view.

Select the Enterprise from the list box and then configure the following areas for ACD settings.

ACD Groups (*MiVoice Business only*)

The MiVoice Business switch requires ACD agents to be included in ACD groups. The ACD Groups table contains the following column headings:

- **Group ID**: The Group ID should match the group ID of an ACD group configured on the MiVoice Business switch.
- **Switch IP**: The IP address of the MiVoice Business switch.
- **Agents**: The list of extensions included in the ACD group.

You can Add, Edit, or Delete ACD Groups.

In addition you can add and delete agent extensions to the groups.

To add agent extensions to the ACD group:

1. Click  . The ACD groups table expands to include an agent edit area.
2. Do one of the following:

   - To add a single extension, type the extension number in the first box and leave the second box blank.
   - To add a range of extensions, type the starting extension in the first box and the ending extension in the second box.

3. Click **Add**, and then click **Done**.

To delete agent extensions from the ACD group:

1. Click  . The ACD groups table expands to include an agent edit area.
2. Click  for the extension or range that you want to delete.
3. Click **Done**.

When you are finished configuring ACD Groups, click **Apply** to save the information, or click **Reset** to clear your changes.

Account Codes

To facilitate reporting, some call centers require account codes for ACD calls. At startup, account codes are sent to the desktop clients for the users (agents) who have been configured for the ACD feature. Agents can then apply the account code during the call from the Desktop Client's ACD view.

The Account Codes table contains the following column headings:

- **Code**: The numeric value for the account code (2-12 digits).
- **Label**: The description you provide for the account code.

You can Add, Edit, and Delete account codes.

When you are finished configuring Account Codes, click **Apply** to save the information, or click **Reset** to clear your changes.

Busy Reasons

The Busy Reasons section allows you to manage the ACD busy reasons provided by the switch. The number of busy reasons displayed is determined by the switch type (see table below).

The Busy Reasons table contains the following column headings:

- **Code**: The numeric value for the busy reason code.
- **Label**: The default description, (or description that you provide), for the busy reason code.

Code	MiVoice Business Default Label	MiVoice Office Default Label
0	No Reason	No Reason
1	At Lunch	At Lunch
2	Gone Home	Gone Home
3	Unavailable	Unavailable
4	Do-Not-Disturb	Do-Not-Disturb
5	In Meeting Until	In Meeting Until
6	On Vacation Until	On Vacation Until
7	Page Me	Page Me
8	Call Me At	Call Me At
9	Away from Desk	Away from Desk
10	Out of Town Until	Out of Town Until
11	Telecommuting	Telecommuting
12		Out Until
13		Leave Voice Mail
14		On Break

Code	MiVoice Business Default Label	MiVoice Office Default Label
15		In Training
16		Out of Office
17		Meeting Customer Until
18		Travelling
19		Off Site at

You cannot add or delete busy reason codes or labels. However, you can edit all of the busy reason labels except for the label for code 0 (No Reason). This busy reason code is predefined and cannot be changed.

When you are finished editing Busy Reason labels, click **Apply** to save the information, or click **Reset** to clear your changes.

1.8.6 Collaboration Tab

The Collaboration tab provides a table that lists all the collaboration servers that are configured for the Enterprise. Collaboration servers provide audio, video, web conferencing, and associated collaboration features to MiCollab Client users who are provisioned for the Collaboration Integration licensed feature.

Note:
Some configuration settings do ***not*** apply to MiCollab Client Stand-alone Web Client users (see table for details).

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab - integrated mode.

Additional information about the MiCollab Audio, Web and Video Conferencing collaboration server:

The collaboration server is the central hub for all conference sessions. Audio and web conferences require a server where the conference sessions are hosted, and all conference information flows through the server before being distributed to the MiCollab Client Desktop Client.

Mitel supports the MiCollab Audio, Web and Video Conferencing product for collaboration features.

MiCollab Audio, Web and Video Conferencing provides an integrated application to create audio and Web conferences, create video calls, share documents and applications, chat, and use collaboration tools such as whiteboarding and annotation to share information between users in real time.

Like MiCollab Client , MiCollab Audio, Web and Video Conferencing is packaged on the MiCollab server, which is connected to the IP network. The MiCollab server provides access to a Web-based administrator interface for configuring MiCollab Audio, Web and Video Conferencing , scheduling conferences, viewing conference calls, and administering collaboration controls. You can access all interfaces through either HTTP or HTTPS.

Note:
MiCollab Client v5.0 requires MiCollab Audio, Web and Video Conferencing 4.0 or later running on MiCollab v4.0 or later.

Select the Enterprise from the list box and the following information is displayed for the Enterprise's collaboration servers:

- **Description**: The short description configured for the collaboration server.
- **URL**: The Web address for the collaboration server.

You can complete the following tasks for collaboration servers:

- Sort the information in the table.
- Select one or more entries in the table.
- Click the Add Server link to add a collaboration server.
- Click the collaboration server link in the **Description** column to edit the collaboration server.
- Delete collaboration servers.

Note:
To clean up your database you can delete previously-used UCX/YA Collaboration servers.

To delete a collaboration server:

1. Select the server you want to delete from the table.
2. Click the **Delete Server** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the server, or click **Cancel** to cancel the deletion.

- Refresh the information on the page.

1.8.6.1 Adding and Editing Collaboration Servers

On this page, you can add and edit information for the MiCollab Audio, Web and Video Conferencing collaboration servers you configure for the Enterprise.

Note:
Some configuration fields are disabled if MiCollab Client is running in MiCollab - integrated mode.

To add or edit an MiCollab Audio, Web and Video Conferencing Collaboration server:

1. Type a **Description** (*Required*) for the MiCollab Audio, Web and Video Conferencing collaboration server. This field has a maximum length is 64 characters.
2. Type the **URL** (*Required*) for the MiCollab Audio, Web and Video Conferencing collaboration server. This field has a maximum length of 255 characters and must begin with " http://" or " https://."

3. Click **Sync Now**. The remaining fields are auto-populated by the collaboration server.

- **Dial-In phone number 1/2/3**: These fields have a maximum length of 32 digits (0-9), and correspond to the following fields as programmed on the MiCollab Audio, Web and Video Conferencing server:
  - The toll free number that user's can dial to join MiCollab Audio, Web and Video Conferencing audio conferences.
  - The public (non-toll free) number that user's can dial to join MiCollab Audio, Web and Video Conferencing audio conferences.
  - The extension number that user's can dial to join MiCollab Audio, Web and Video Conferencing audio conferences.
- Dial Out Allowed: When enabled under Default Account Settings in MiCollab Audio, Web and Video Conferencing , users can dial out to others using MiCollab Audio, Web and Video Conferencing (CO call). By default, this is enabled.

> **Note**:
> This option can also be enabled or disabled on a per-user basis in MiCollab Audio, Web and Video Conferencing.

- **Port Reservations Enabled**: When Port Reservations are enabled in MiCollab Audio, Web and Video Conferencing , the MiCollab Audio, Web and Video Conferencing server tracks how many audio and Web conferencing ports are scheduled for use at any given date and time.
- **Project Codes Required**: When this option is enabled in MiCollab Audio, Web and Video Conferencing , users must enter a project code when creating an MiCollab Audio, Web and Video Conferencing conference.
- Department Codes Required: When this option is enabled in MiCollab Audio, Web and Video Conferencing , users must enter a department code when creating an MiCollab Audio, Web and Video Conferencing conference.
- Project Codes: Provides a list of Project Codes configured for the MiCollab Audio, Web and Video Conferencing server.
- Department Codes: Provides a list of Department Codes configured for the MiCollab Audio, Web and Video Conferencing server.

Note:
Project and department codes are used to track conferences for billing purposes and to restrict conference usage.

- **MiCollab Audio, Web and Video Conferencing Internal Port**: Corresponds to the value for the Internal Port field (by default, port 4443) on the MiCollab Audio, Web and Video Conferencing Administrator Web Conferencing Settings page.
- MiCollab Audio, Web and Video Conferencing client version: Provides the current MiCollab Audio, Web and Video Conferencing Collaboration Client software version.
- **MiCollab Audio, Web and Video Conferencing server version**: Provides the current MiCollab Audio, Web and Video Conferencing server software version.
- **AWC External Port**: Corresponds to the value for the External Port field (by default, port 443) on the MiCollab Audio, Web and Video Conferencing Admin Web Conferencing Settings page.
- **Web Conferencing Name**: Corresponds to the value for the Web Conferencing Name field on the MiCollab Audio, Web and Video Conferencing Administrator Web Conferencing Settings page.

Note:
If you receive an IO Exception error message after you click **Sync Now**, refer to the Synchronization Error Messages topic.

4. Do one of the following:

- Click **Create** to create the MiCollab Audio, Web and Video Conferencing collaboration server.
- Click **Save** to save the updated information for the MiCollab Audio, Web and Video Conferencing collaboration server.
- Click **Cancel** to return to the Collaboration tab without making changes.

You are returned to the **Collaboration** tab.

1.8.7 Features Tab

The Features tab provides fields and options used to configure feature profiles for each Enterprise and view current Licensed Feature Usage. Using feature profiles, you can quickly provision users with MiCollab Client features.

Select the Enterprise from the list box and the following information is displayed:

- **Feature Profiles**: The **Add Profile** link in the Feature Profiles section allow you to configure feature profiles for the selected Enterprise. A feature profile consists of a profile name and description, a list of licensed features included in the profile, and a list of members (users) assigned to the profile. You can create feature profiles based on basic user types: Integrated User, Stand-alone Web Portal User, and Stand-alone Mobile Portal User.

> **Note**:
> The Federation and Peering licenses are server-level licenses and therefore will not be included in any Feature Profiles. If the UC Server is licensed for Federation and Peering, the Federation and Peering tabs will appear on the UC Server Administrator interface. The tabs will not appear if the server is not licensed for these features. See the About Licensed Features topic for details about MiCollab Client licensed features.

- **Licensed Feature Usage**: The Licensed Feature Usage section provides read-only information about the current licensed feature usage on the system.

You can complete the following tasks from the Features tab:

- Click the Add Profile link to add a feature profile.
- Click the feature profile link in the **Name** column to edit the feature profile.
- Click the  icon to add or edit feature profile members.
- Delete a feature profile. **To delete a feature profile:**

1. Select the feature profile you want to delete from the feature profile table.
2. Click the **Delete Profile** link. A dialog box appears prompting you to confirm the deletion.
3. Click **OK** to delete the feature profile, or click **Cancel** to cancel the deletion.

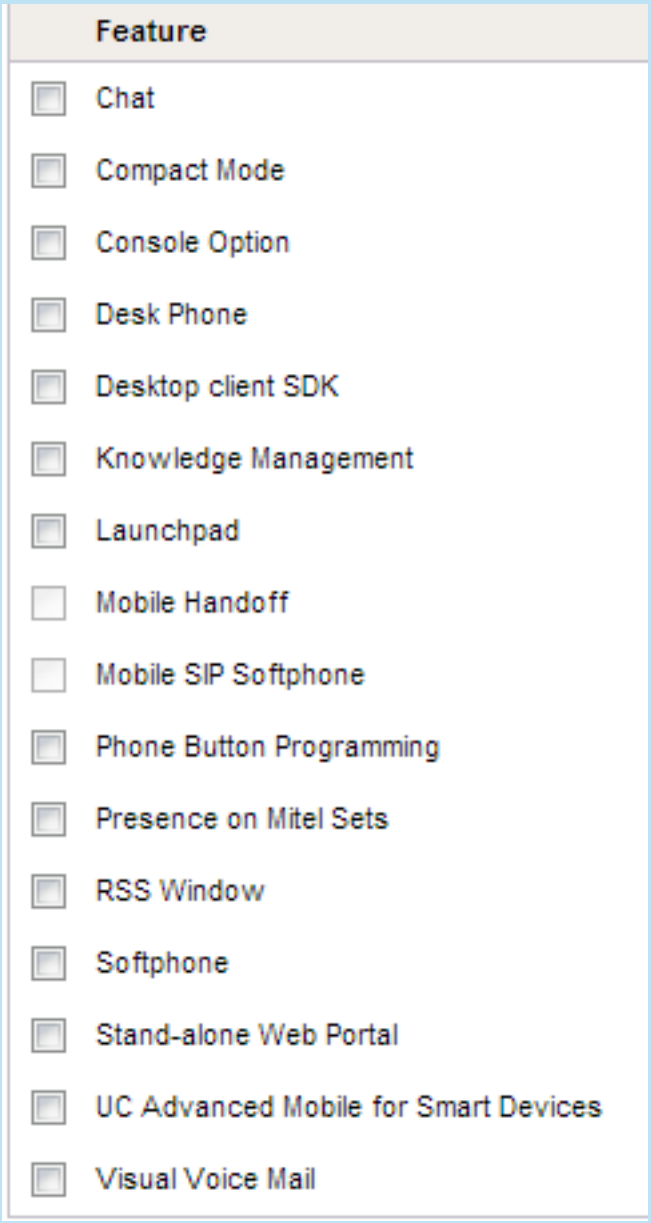
- View Licensed Feature Usage.

  The Licensed Feature Usage table provides the following information:

  - **Feature**: The name of the licensed feature. See the About Licensed Features topic for feature descriptions. Non-licensable features will not be visible in this list.
  - **Sys Allowed**: Indicates the total number of seats defined in the license for the entire system (all Enterprises combined).
  - **Sys Used**: Indicates the total number of seats in use for the entire system (all Enterprises combined).
  - **Allowed**: Indicates the number of seats defined in the license for the selected Enterprise.
  - **Used**: Indicates the number of seats in use for the selected Enterprise.
- Sort the information in the Licensed Feature Usage table.
- Refresh the information on the page.

Note:

The **Features Tab** - Licensed Feature Usage has been simplified in MiCollab Client 6.0 to only display the following Features .



Basic MiCollab Client: MiCollab Client 6.0 offers Desktop and Web clients the option to be configured as Basic MiCollab Client . The Basic UC Client is assigned the **default** feature profile which only provides access to the non-licensable features . Also see Licensed Features and Synchronization

Allowed Features	Desktop Client	Web Client
Blind Transfer	X	X
Call Forwarding	X	
Compact Mode	X	
Contact Groups	X	X
Corporate Contact	X	X
External Dial	X	
Missed Call Logs	X	X
Make and Receive Call	X	X
Office Communicator Integration	X	
Phone Button Programming	X	
RSS Window	X	
Visual Voice Mail	X	X
WLM Integration	X	

Teamwork mode: For accounts in Teamwork Mode, you can select any feature, however any phone or call control related features (such as Desk phone or Softphone) will be ignored. Licenses for individual features such as Chat, Visual Voicemail, etc… are still required.

1.8.7.1 Adding and Editing Feature Profiles

On the Feature Profile Details page, you can add new feature profiles and edit the features for existing feature profiles. See the About Licensed Features topic for feature descriptions.

Note:
Refer to the Licensed Features and Synchronization topic if you intend to create MiCollab Client accounts using a PBX Node or AD/LDAP synchronizer.

To add or edit a feature profile:

1. Configure the settings for the feature profile.

   - **Name:** (*Required*) Type a name for the feature profile. Maximum length is 64 characters, and the vertical bar character is not supported.
   - **Description**: (*Optional*)Type a description for the feature profile. Maximum length is 128 characters, and the vertical bar character is not supported.
   - **Member count**: This read-only field displays the number of members assigned to the feature profile.

2. *If you are creating a new feature profile,* click **Create**. The page expands to show the Features section.
3. Configure the features for the feature profile.

   The **Features** section shows a list of all the features that you can include in the feature profile. In addition, this section provides the following licensing information:

   - **Seats Available**: Displays how many licensed seats are available for each feature.
   - **Seats in Use**: Displays how many licensed seats are currently in use for each feature for the feature profile. The value displayed here corresponds with the number of members you have assigned to the feature profile. If you have not yet assigned members to the feature profile, the value will be 0.

   To add features to the feature profile, do one of the following:

   - Select the individual features you want to include in the feature profile.
   - Click **Select All** to include all features in the feature profile.

Note:
Both Web Portal features are set automatically when you select either one of them.

To remove features from the feature profile, do one of the following:

- Clear the feature check box for those individual features you want to remove.
- Click **Remove All** to remove all features from the feature profile.

Note the following if you are editing a feature profile with assigned members:

- When you select and deselect features, the **Seats Available** and **Seats In Use** columns are updated to show the effect of including or excluding the feature in the feature profile.
- If the number of available seats is less than the total number of profile members, the feature is disabled and displayed in *italic font*.

4. Click **Save** to save the feature profile. You are returned to the Features tab.

You can add members to the feature profile from the Features tab.

1.8.7.2 Adding and Editing Feature Profile Members

The Feature Profile Members page provides a table that lists all of the members for the feature profile. From this page you can add and remove members from a feature profile.

To add feature profile members:

1. Click the **Add Members** link. The Add Feature Profile Members page appears. Account names are presented alphabetically. Note the following:
   - Click the arrow buttons at the bottom of the page to scroll to a different page.
   - Use the Search function to quickly search for a name.
2. Select the accounts you want to add to the feature profile.
3. Click **Add to Profile**. The list of accounts you selected are added to the feature profile.
4. Click **Save**. The progress bar on the Feature Profile Member Update Status page indicates the progress of the operation.
5. Click **Done**. You are returned to the Features tab.

To remove feature profile members:

1. Select the members you want to remove from the feature profile.
2. Click the **Remove Members** link. The members are removed from the feature profile.
3. Click **Save**. The progress bar on the Feature Profile Member Update Status page indicates the progress of the operation.
4. Click **Done**. You are returned to the Features tab.

1.8.8 Peering Tab

Note:
Peering is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

Note:
The presence of the peered users with the login ID as UPN will be seen only when both the peered servers are on MiCollab version 9.4 and above.

The Peering tab allows you to configure peering for the Enterprise by adding MiCollab Client Services or external servers as peers. Peering between different enterprises on the same MiCollab Client server is supported.

Select the Enterprise from the list box and the following information is displayed in the Peer Server table for each peer server you have added:

- **Description**: The name that you have provided for the peer server.
- **Server**: The Fully Qualified Domain Name (FQDN) that you added for the peer MiCollab Client Service. N/A is displayed for external peer servers.
- **Peer Type**: The type of peer server (**MiCollab Client Service** or **External**).
- Peer Server Version: The MiCollab Client Service version which is installed on the peer server.
- **Status**: The status of the connection to the peer MiCollab Client Service. N/A is displayed for external peer servers.

You can complete the following tasks from the Peering tab:

- Click the Add Server link to add a peer server.
- Click the server link in the description, column to edit the peer server details.

- Delete a peer server. When you delete a peer server, all the information associated with the synchronizer is also deleted.
- Sort the information in the Peer Server table.
- Click  to open the peered MiCollab Client Service Administrator interface.

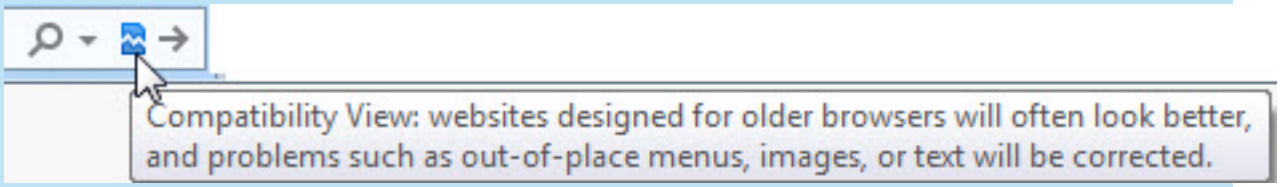
Note:

The following procedure must be done on MiCollab Client 5.1 to resolve peering on a server that had a changed IP address:

Go to the Enterprise Tab, expand Trusted Servers, select the peered server whose IP address changed, and in the Trusted Server Details page edit the field "IP address/ hostname" with the correct IP address.

Note:

Peering contacts not displayed for a corporate directory on IE9 or IE10, then enable compatibility view by clicking here (icon is displayed to the right of the URL address in the browser window):



Note:

Whenever the peered server address is changed, the server address must also be updated in the peer trusted servers list.

1.8.8.1 Adding and Editing Peer Servers

The Peer Server Details page allows you to add and edit MiCollab Client Service and external peer servers.

If you are adding an external server to enable federation, the customer must install the IM server and deploy the XMPP gateway provided with the server to federate with MiCollab Client Service. Refer to the IM server documentation for instructions about configuring federation.

To add or edit a peer server:

1. Configure the server **Settings**.

- Select the **Peer Type**. Options include **MiCollab Client Service** and **External**.
- Type a **Description** for the peer server. The Description is limited to 64 characters in length and must contain alpha-numeric characters, dashes, and/or spaces.
- (*MiCollab Client Services only*) Type the **hostname** for the MiCollab Client Service . The value entered in the hostname field must match the value used for generating the web server certificate on the MiCollab Client Service to which the MiCollab Client Service is being peered.
- (*MiCollab Client Services only*) The **Peer enterprise ID** field defines which enterprise from the peered MiCollab Client Service will be synchronized with the selected Enterprise on the local MiCollab Client Service . The Enterprise ID is configured on the Enterprise tab. Do one of the following to add the Enterprise ID:
- Click the **Select Enterprise** link, and then select the correct Enterprise from the list.
- Type the Enterprise ID in the box. The Enterprise ID:
- is limited to 4-32 characters in length.
- must contain alpha-numeric characters (dashes included).
- cannot contain spaces, vertical bars, commas, semicolons, or colons (| , ; :).

Note:
The Enterprise domain should be unique for each MiCollab Client Service peer. Mitel suggests using the site location or Enterprise ID (configured on the Enterprise Details page) as part of the Enterprise domain (for example, **Phoenix.xyzcompany.com**, where **Phoenix** is the Enterprise ID).

- (*MiCollab Client Service s only*) *If required*, type the **Peer Dialing Prefix** for the server. The Peer Dialing Prefix is only required for PBX-to-PBX calls where the networked PBXs are not configured for transparent extension dialing. The value you enter here corresponds with the dialing prefix (not including the outgoing call digit) that PBX users must press to dial an extension on the networked PBX. The Peer Dialing Prefix is limited to 20 characters in length.

  Note: No validation is performed on the characters entered for the Peer Dialing prefix. The administrator should enter what is set up in the PBXs for calling from one PBX to another. The Peer Dialing prefix can start with a hyphen (-) character.

Doing so informs the MiCollab Client Service to **not** append the outgoing prefix digit defined under the PBX node settings when making calls to extensions on the PBXs associated with the peered MiCollab Client Service .

2. *If you are adding a new peer server*, click **Create**.
3. (*External Servers only*) Configure the **Synchronization Settings** for the server

   a. (*Optional*) Schedule automatic synchronizations between MiCollab Client and the AD/LDAP databases by specifying the following:

      - The frequency (in days) the synchronization should occur.
      - The hour the synchronization should start.
      - The minute the synchronization should start.
      - Whether the synchronization should occur in the AM or PM.

   b. Click Add to add an AD/LDAP synchronizer and configure the settings.

   c. Click **Sync Now** to synchronize the AD/LDAP directory with the Unified Communications server. After you click **Sync Now**, the peer server contacts are imported to the MiCollab Client Service database (visible from the Corporate Directory Tab) and federation with these contacts is automatically enabled.
4. Click **Save**.

After you create peer servers, you can edit the associated fields at any time.

Peering between different enterprises on the same MiCollab Client Service is supported.

1.8.9 Federation Tab

Note:
Federation is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

The Federation tab allows you to configure IM and presence federation. IM and Presence Federation provides a communication path between a single MiCollab Client Service and one or more IM servers for the purpose of providing extended IM capabilities to MiCollab Client users. The communication path between the servers uses the Extensible Messaging and Presence Protocol (XMPP).

The customer must install the IM server and deploy the XMPP gateway provided with the server to federate with MiCollab Client Service. Refer to the IM server documentation for instructions about configuring federation.

Note:
You can also configure federation for an external IM server from the Peer Server Details page. After adding the server and performing a synchronization with the server's AD/LDAP database, the IM server contacts are imported to the MiCollab Client Service database (visible from the Corporate Directory tab) and federation is automatically enabled.

When a MiCollab Client Service and IM server are configured for federation, MiCollab Client users are provided with IM presence information and the ability to chat with IM contacts using the Desktop Client's Chat window.

When you configure federation from the Federation tab, instruct users to manually add federated contacts to the Desktop Client. Users should create a new personal contact, and then add the IM login information (for example, john_smith@ocs.com) for the contact using the MiCollab Client Login option.

Note:
For MiCollab Client v4.0, IM server support is limited to Microsoft Office Communicator Server (OCS) and IBM Lotus Sametime Server. For MiCollab Client v6.0, NextPlane Federation is supported.

In addition, for MiCollab Client v6.0, federation with MBG in the network path between MiCollab Client Service and the federated server (Skype for Business, IBM Sametime) is supported. This is accomplished by adding MBG connector for TCP port 5269 in MBG v8.0.

To configure federation with an external IM server:

1. Configure the external IM server for federation. Refer to the IM server documentation for instructions.
2. On the Federation tab, click **Enable Federation**. This configures the embedded XMPP MiCollab Client Service for federation.

3. Add the external IM server to the Federated Servers table.

   a. Click **Add Server**. A server entry is added to the Federated Servers table.
   b. Double-click **Enter domain**. An editable text box appears.
   c. Type the domain for the IM server (for example, ocs.com).

   Perform these additional steps if adding a NextPlane server:

   a. Select checkbox NextPlane.
   b. Double-click **Enter server**. An editable text box appears.
   c. Double-click **Port**. An editable text box appears.
4. Click **Apply** to save the information, or click **Reset** to clear your changes.

You can also complete the following tasks from the Federation tab:

- Click the **Disable Federation** button to disable federation on the MiCollab Client Service .
- Click the Delete Server link to delete an IM server from the Federated Servers table.

1.8.9.1 Federation Tab

Note:
Federation is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

The Federation tab allows you to configure IM and presence federation. IM and Presence Federation provides a communication path between a single MiCollab Client Service and one or more IM servers for the purpose of providing extended IM capabilities to MiCollab Client users. The communication path between the servers uses the Extensible Messaging and Presence Protocol (XMPP).

The customer must install the IM server and deploy the XMPP gateway provided with the server to federate with MiCollab Client Service. Refer to the IM server documentation for instructions about configuring federation.

Note:
You can also configure federation for an external IM server from the Peer Server Details page. After adding the server and performing a synchronization with the server's AD/LDAP database, the IM server contacts are imported to the MiCollab Client Service database (visible from the Corporate Directory tab) and federation is automatically enabled.

When a MiCollab Client Service and IM server are configured for federation, MiCollab Client users are provided with IM presence information and the ability to chat with IM contacts using the Desktop Client's Chat window.

When you configure federation from the Federation tab, instruct users to manually add federated contacts to the Desktop Client. Users should create a new personal contact, and then add the IM login information (for example, john_smith@ocs.com) for the contact using the MiCollab Client Login option.

Note:
For MiCollab Client v4.0, IM server support is limited to Microsoft Office Communicator Server (OCS) and IBM Lotus Sametime Server. For MiCollab Client v6.0, NextPlane Federation is supported.

In addition, for MiCollab Client v6.0, federation with MBG in the network path between MiCollab Client Service and the federated server (Skype for Business, IBM Sametime) is supported. This is accomplished by adding MBG connector for TCP port 5269 in MBG v8.0.

To configure federation with an external IM server:

1. Configure the external IM server for federation. Refer to the IM server documentation for instructions.
2. On the Federation tab, click **Enable Federation**. This configures the embedded XMPP MiCollab Client Service for federation.

3. Add the external IM server to the Federated Servers table.

   a. Click **Add Server**. A server entry is added to the Federated Servers table.
   b. Double-click **Enter domain**. An editable text box appears.
   c. Type the domain for the IM server (for example, ocs.com).

   Perform these additional steps if adding a NextPlane server:

   a. Select checkbox NextPlane.
   b. Double-click **Enter server**. An editable text box appears.
   c. Double-click **Port**. An editable text box appears.
4. Click **Apply** to save the information, or click **Reset** to clear your changes.

You can also complete the following tasks from the Federation tab:

- Click the **Disable Federation** button to disable federation on the MiCollab Client Service .
- Click the Delete Server link to delete an IM server from the Federated Servers table.

1.8.10 User Profile Tab

The User Profile tab allows an administrator to set or configure user profiles for MiCollab Client Service.

With Centralized Client Management, the administrator can control/manage the Dynamic status, Auto Start settings for Windows PC clients, Calendar Integration and Set Advisory, and the Call Through functionality for the Mobile Clients. This gives the administrator the ability to add, delete or update the user profiles created from the MiCollab Client Service Admin portal.

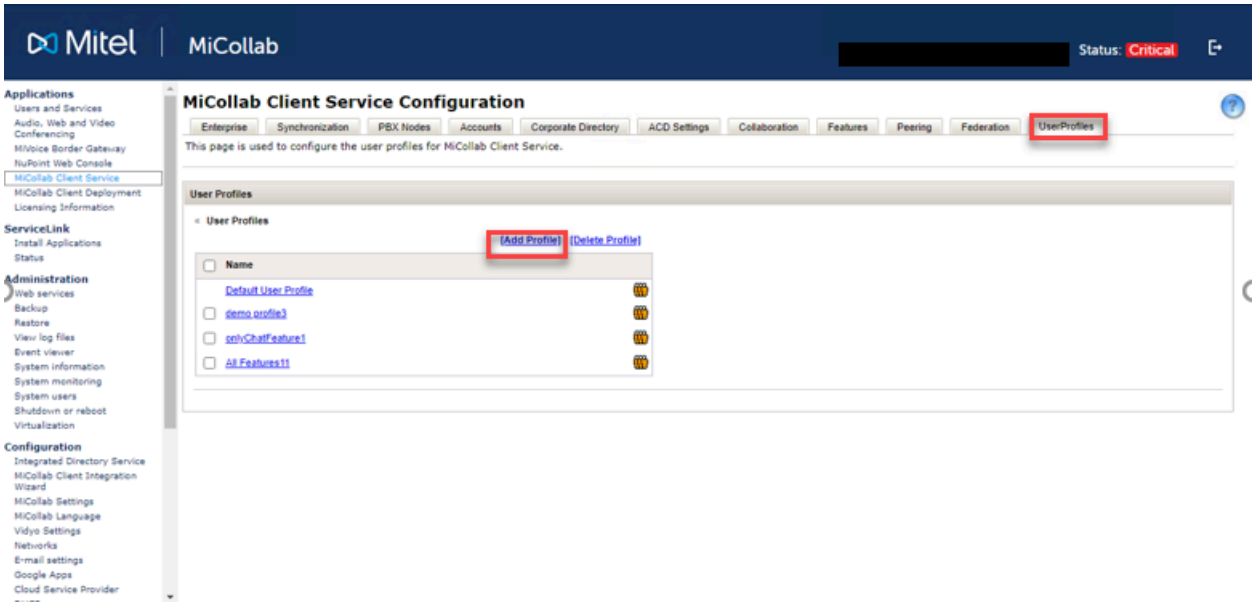
With Release 9.3 onwards, when the system migrates with this feature, all the existing users will be moved or assigned under the default user profile. This will ensure that all the existing users/features will work as they were previous to Release 9.3 with no change. These default user profiles cannot be controlled by the administrator.

The administrator can control only the user profiles that are newly created from the MiCollab Client Service via the User Profile tab

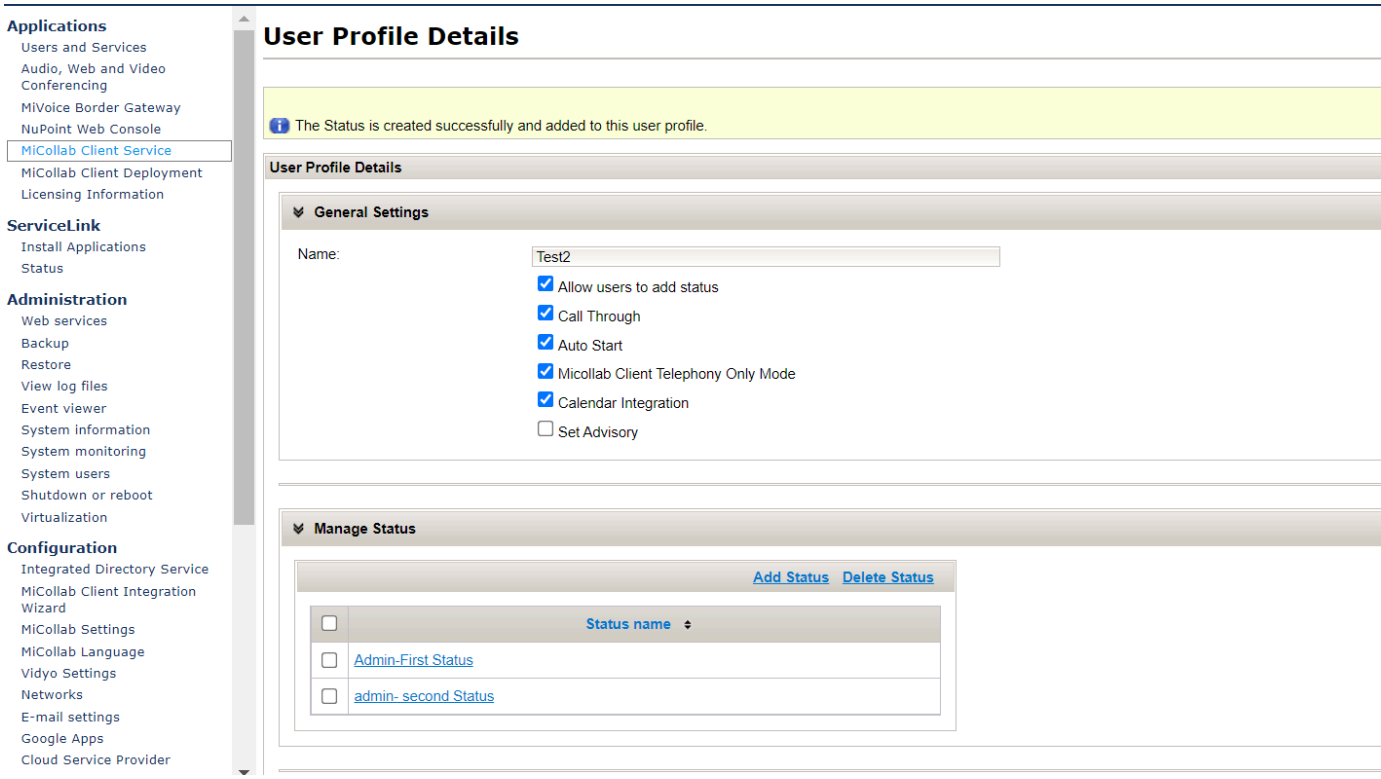
To add a user profile:

1. Navigate to **Applications > MiCollab Client Service > User Profiles.**

2. Under User Profiles, click on **Add Profiles.**



3. Enter the **Name** of the profile under **General Settings**.



4. Select the following options:

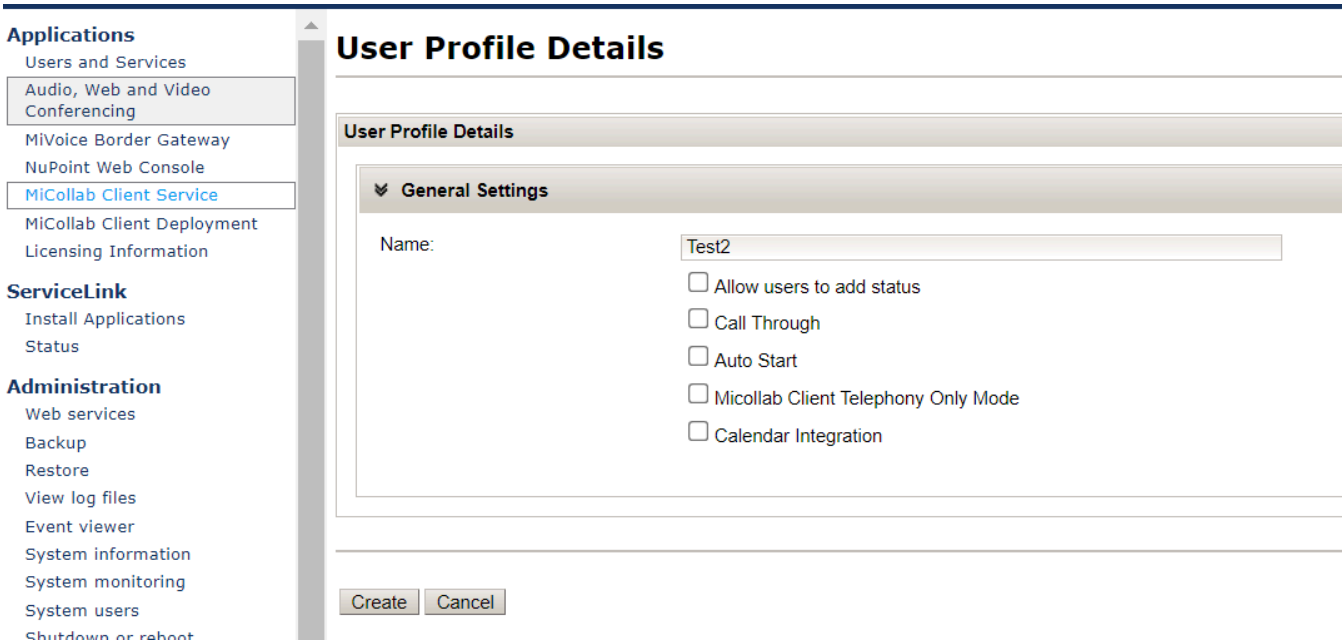
- **Allow the users to add status**
- **Call Through**
- **Auto Start**
- **MiCollab Client Telephony Only Mode**
- **Calendar Integration**
- **Set Advisory**

Note:

The **Allow users to add status** option enables the user to add any user-defined dynamic status from the client-side. If this option is left unchecked, then the user cannot add a status by themselves.

Note:

Calendar Integration and Set Advisory will appear when the Calendar Integration is enabled at Enterprise.



5. Click **Save.**

To manage dynamic status:

The option **Allow users to add status**, under General settings, enables the user to add any user-defined dynamic status from the client-side. If this option is left unchecked in the MiCollab server, by the administrator, then the user cannot add a status by themselves. The dynamic statuses, if selected to be managed by the administrator, can be managed using the following procedure.

Note:

The Flexible CLI option will be editable by the end-users for the administrator provisioned dynamic statuses.

Note:

The Remote extension drop-down option will be editable for all the administrator provisioned dynamic statuses with MiVoice MX-One.

Note:

For MX-One diversions to work, the administrator needs to explicitly create a status with a name, **In the office,** under the dynamic status option.

Once a user profile is added, the next steps to manage a status can be performed using the following steps:

1. Navigate to **Applications > MiCollab Client Service > User Profiles.**
2. Then go to, **User Profiles > Manage Status > Add Status.**
3. Enter the **Status Name** under **General Settings**.
4. Next, check the following check-boxes based on how the profile should be set:

   - **Enable Do Not Disturb**
   - **Accept Video Calls**
   - **Accept Messages**

5. Under **Audio Call Settings**, select the following fields:

   - Call Using –the default setting is **Use Current Settings**
   - Outgoing Number - the default setting is **Default**
   - Send my calls to - the default setting is **PBX Default**
   - When I am on the phone - the default setting is **PBX Default**
   - If I do not answer - the default setting is **PBX Default**

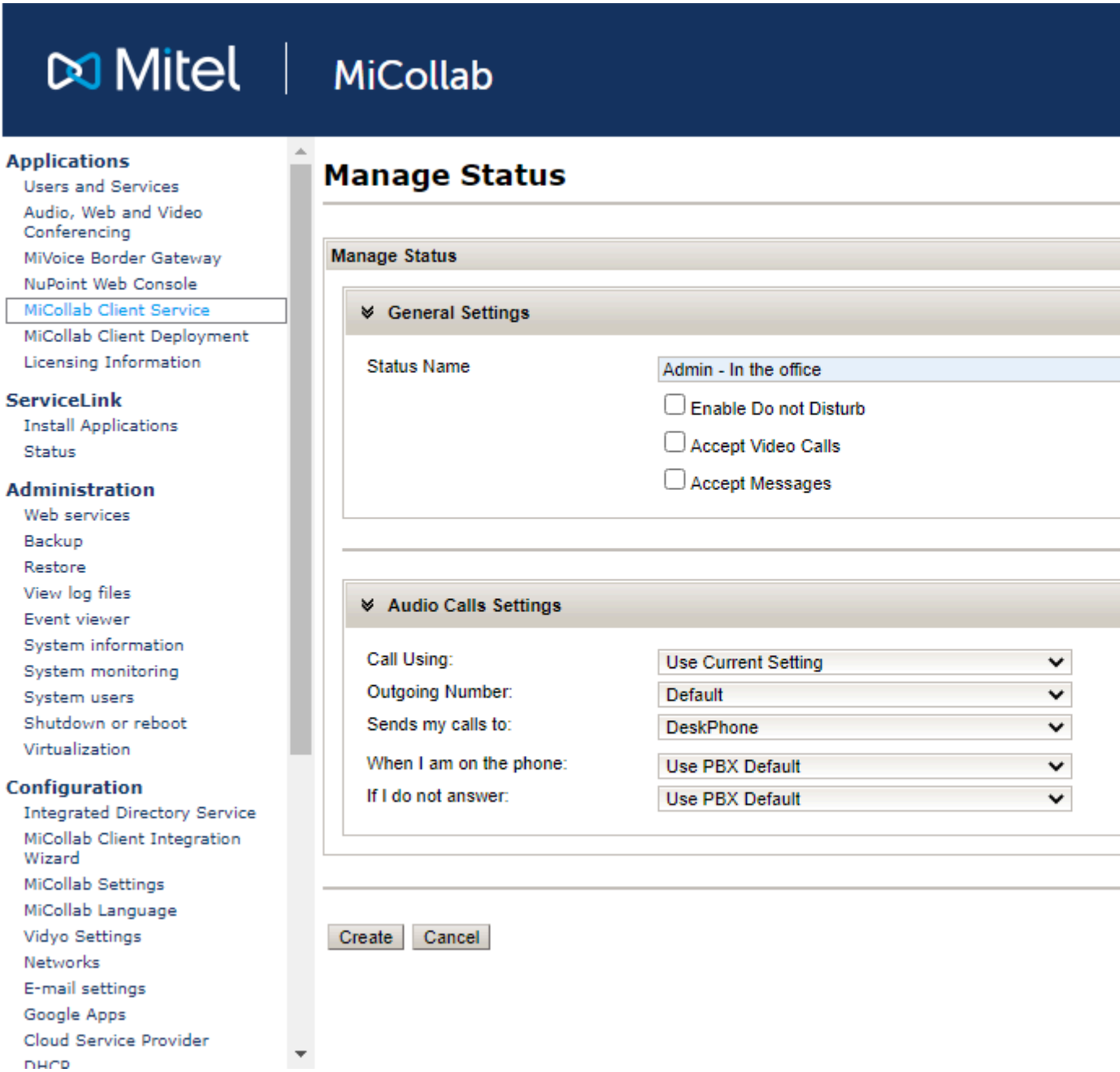
   If the device selected by the administrator is not available for the user, then that field will be set to default device.

   Also, if some device is added to a user after the creation of the admin status, then the admin should reset all the status assigned to that user which will delete all the existing statuses of the user and create new ones.

   The settings defined by the end-user in the MiCollab Next-Gen Client under **Settings > Call Settings > Call Using** dropdown will have a priority over the **Call using** setting which is defined by the administrator in the dynamic status of User Profile. So whatever option the user selects in the MiCollab client's **Call Using** dropdown, that is either **Softphone, Deskphone, Prompt,** or **Managed by status,** these options would take precedence over the settings defined by the administrator in the Admin Portal in the dynamic status' **Call Using** option.

Note:

For any dynamic status that is created by the administrator in the user profile, enabling or disabling the option **Accept Messages** would work only in case of Legacy chat. This will have no effect on the end-user clients in case of CloudLink chat.



6. Click **Create.**

   Once the status is created, assign a user profile to the user, and then the same can be viewed under **MiCollab client > Settings> Manage Status.**

> **Note**:
>
> The status that are created via the admin- defined user profile cannot be edited or deleted by the end-user.

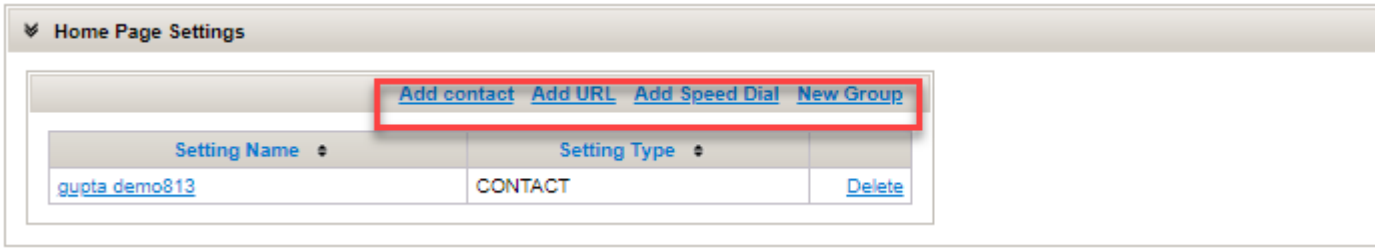
Managing Shortcuts

> **Note**:
> The administrator can add up to a maximum of 50 items in the Homepage settings.

Perform the following steps to manage the shortcuts from the User Profile:

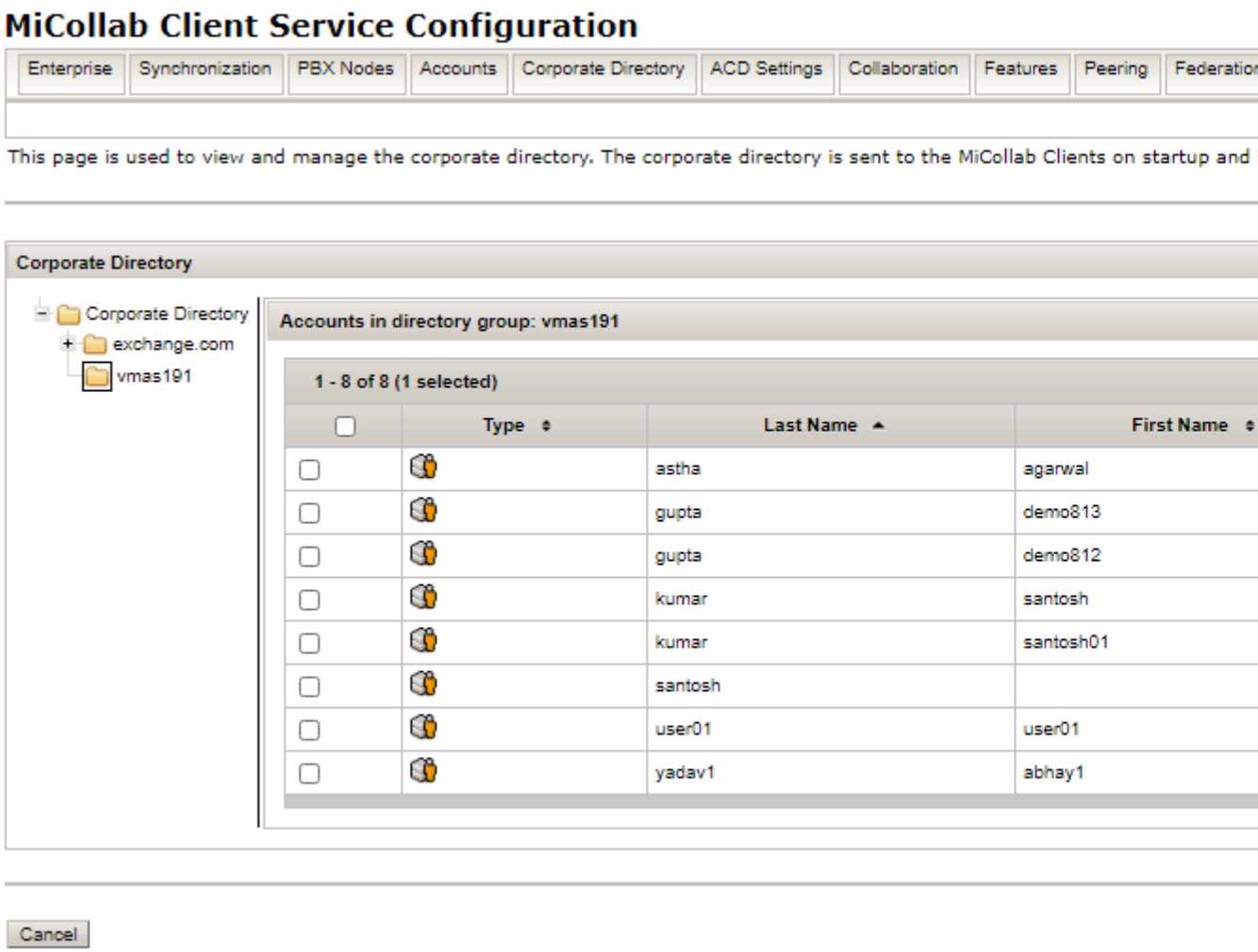
1. Navigate to **Applications> MiCollab Client Service > User Profiles.**
2. Under **User Profile Details > Home Page Settings,** you can control/manage the following shortcuts:

   - Add Contact
   - Add URL
   - Add Speed Dial
   - New Group



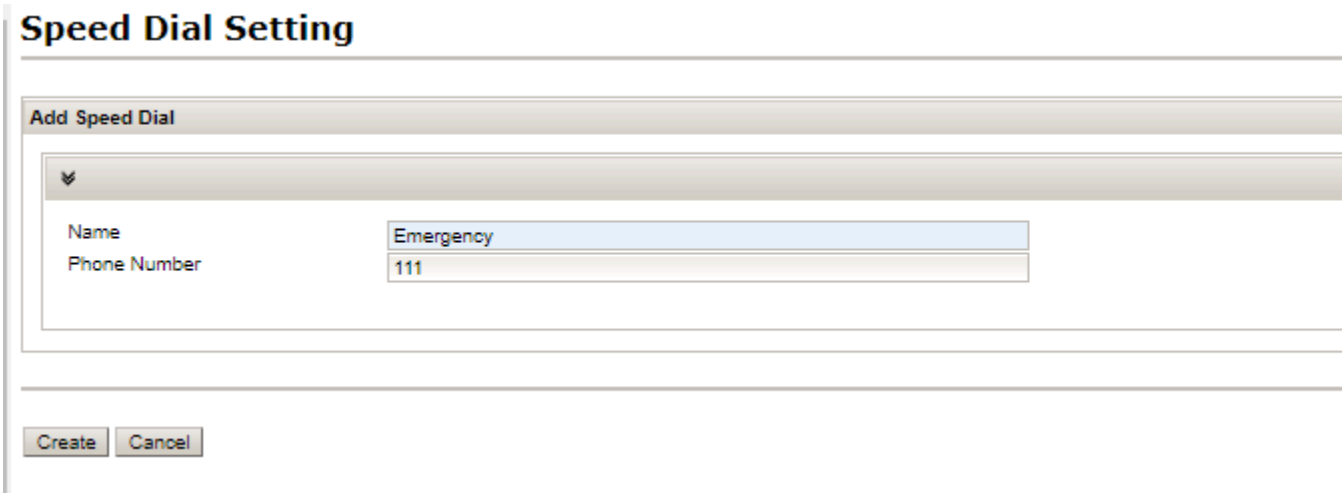
3. Click on each of the options to create the shortcuts:

- Add Contact



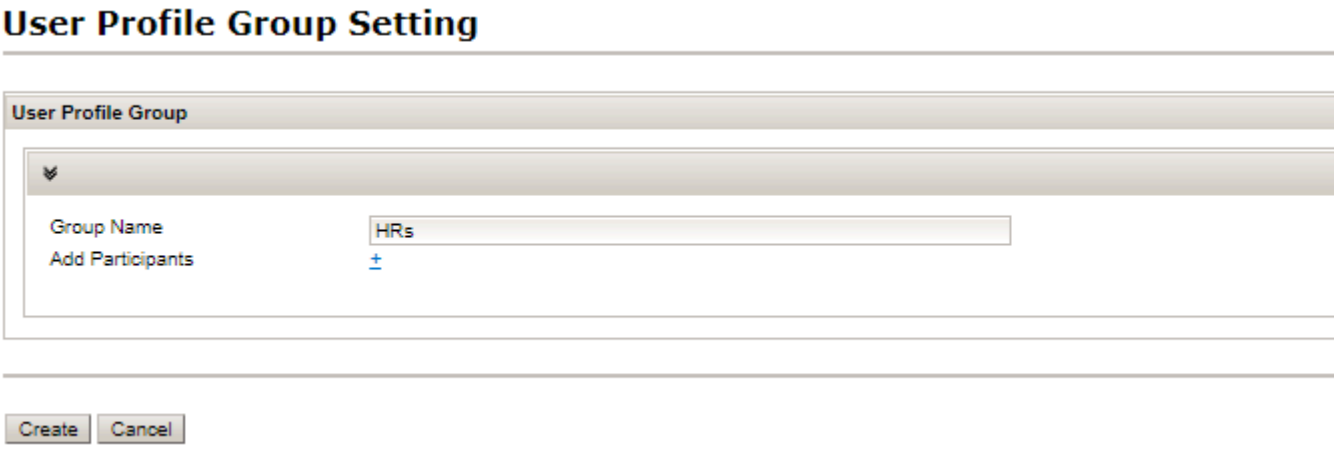
- Add URL

- Add Speed Dial



- Add Group

Note:
The administrator can add any number of participants within a group. There is no limit on the number of participants.



Note:

These shortcuts cannot be edited or deleted by the end-user from the MiCollab Client side once they are managed by the administrator from the MiCollab Client side.

Bulk User Provisioning from the Admin Portal:

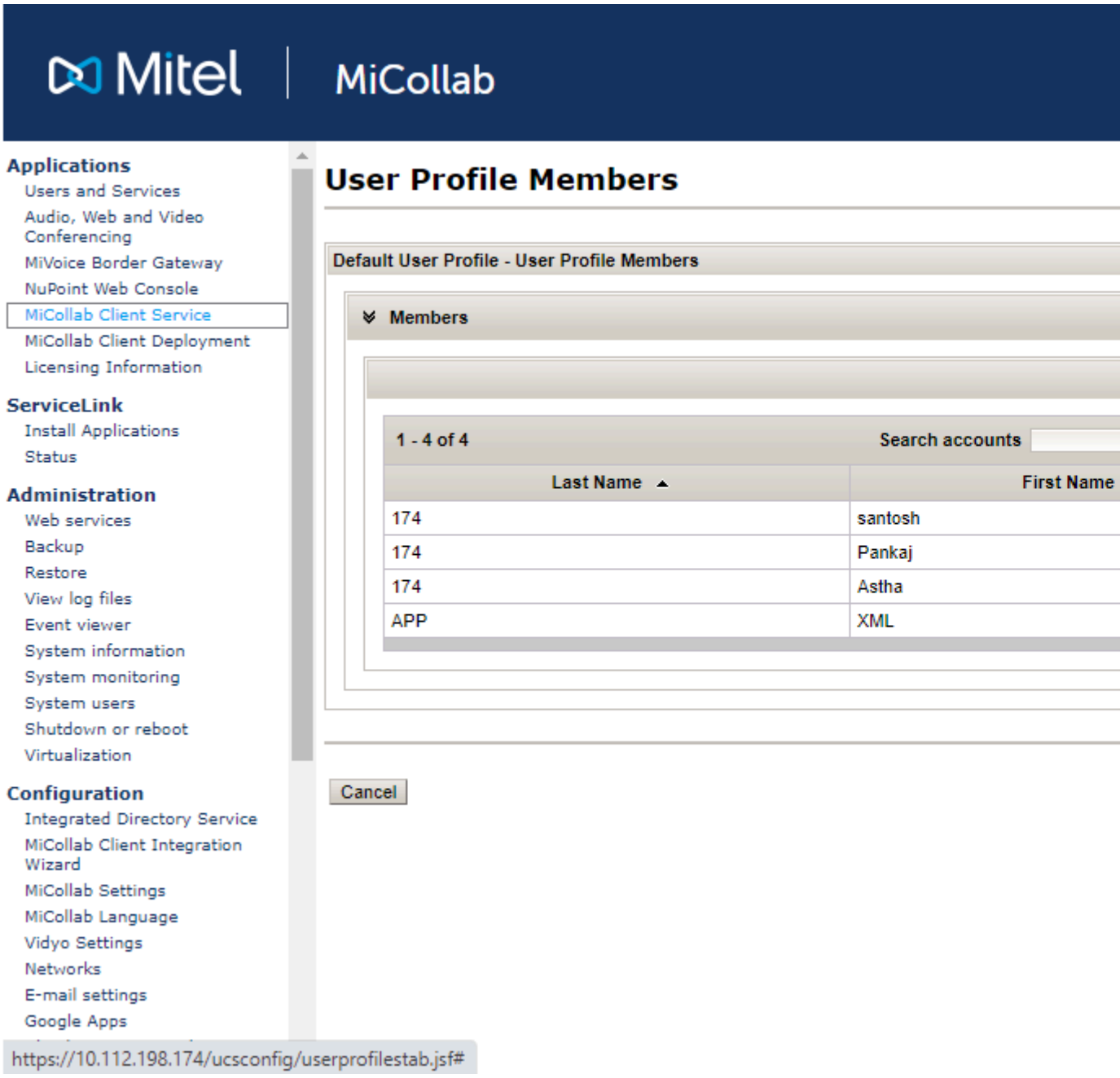
1. Navigate to **Applications > MiCollab Client Service > User Profiles.**

2. Under User Profiles, all the user profiles are listed. Click on the orange icon against each profile.

A warning message is displayed. Click **OK** to proceed. This will list the members to whom the profile is already assigned.

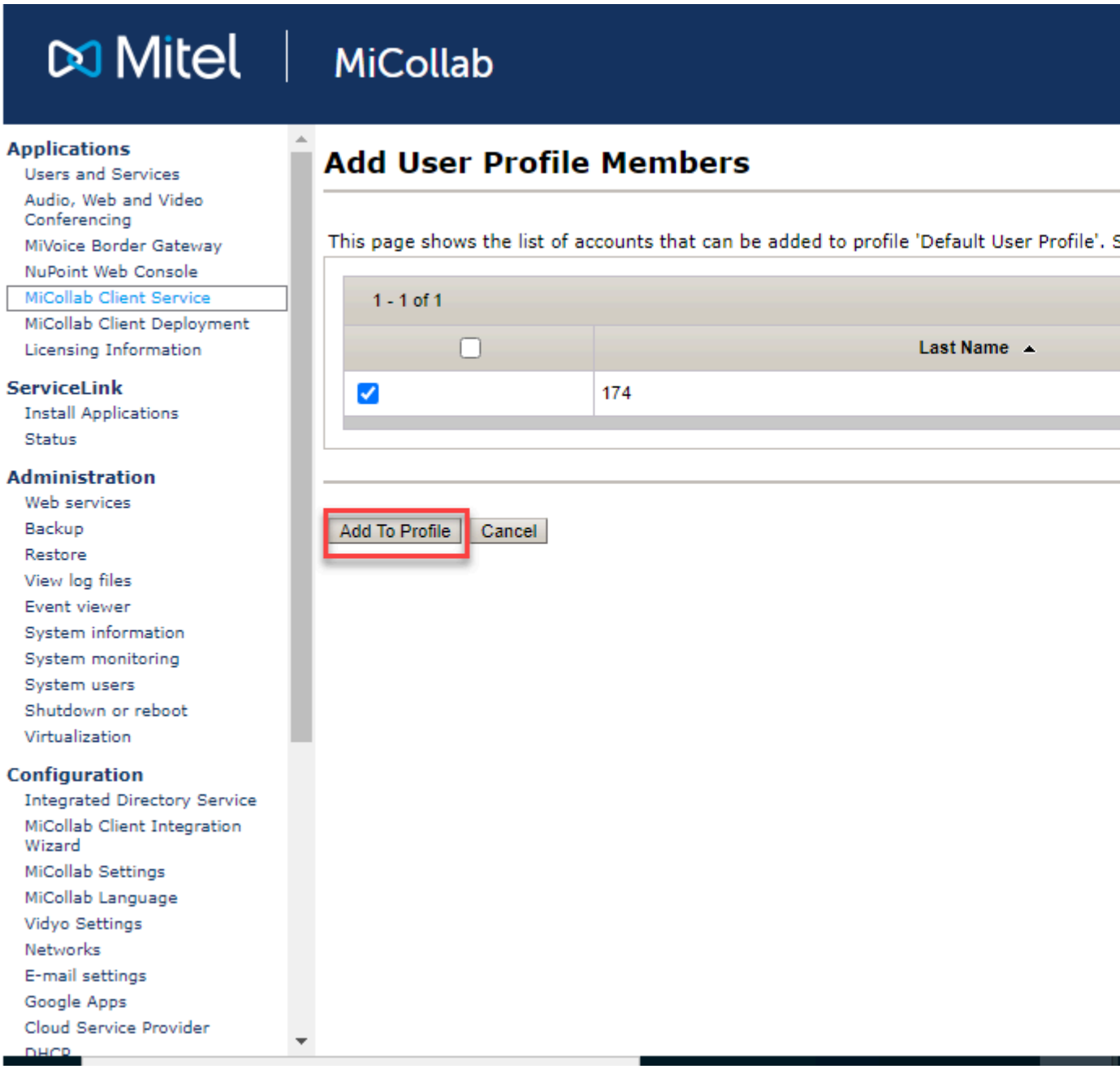

Mitel
MiCollab
Applications
Users and Services
Audio, Web and Video Conferencing
MiVoice Border Gateway
NuPoint Web Console
MiCollab Client Service
MiCollab Client Deployment
Licensing Information
ServiceLink
Install Applications
Status
Administration
Web services
Backup
Restore
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reboot
Virtualization
Configuration
Integrated Directory Service
MiCollab Client Integration Wizard
MiCollab Settings
MiCollab Language
Vidyo Settings
Networks
E-mail settings
Google Apps
Cloud Service Provider
MiCollab Client Service Co
Enterprise
Synchronization
PBX Nodes
This page is used to configure the user profiles
10.112.198.174 says
All the logged in users whose profile
and all on going calls would be impac
consuming, it would impact the syste
should be performed after office hou
Do you want to proceed?
User Profiles
User Profiles
[Add Profile]
[Delete Pro
Name
Default User Profile
Test2
Test

3. Click on **Add Members** and select one or more members against whom the profile needs to be assigned



4. Once all the members are selected, click on **Add to Profile**.

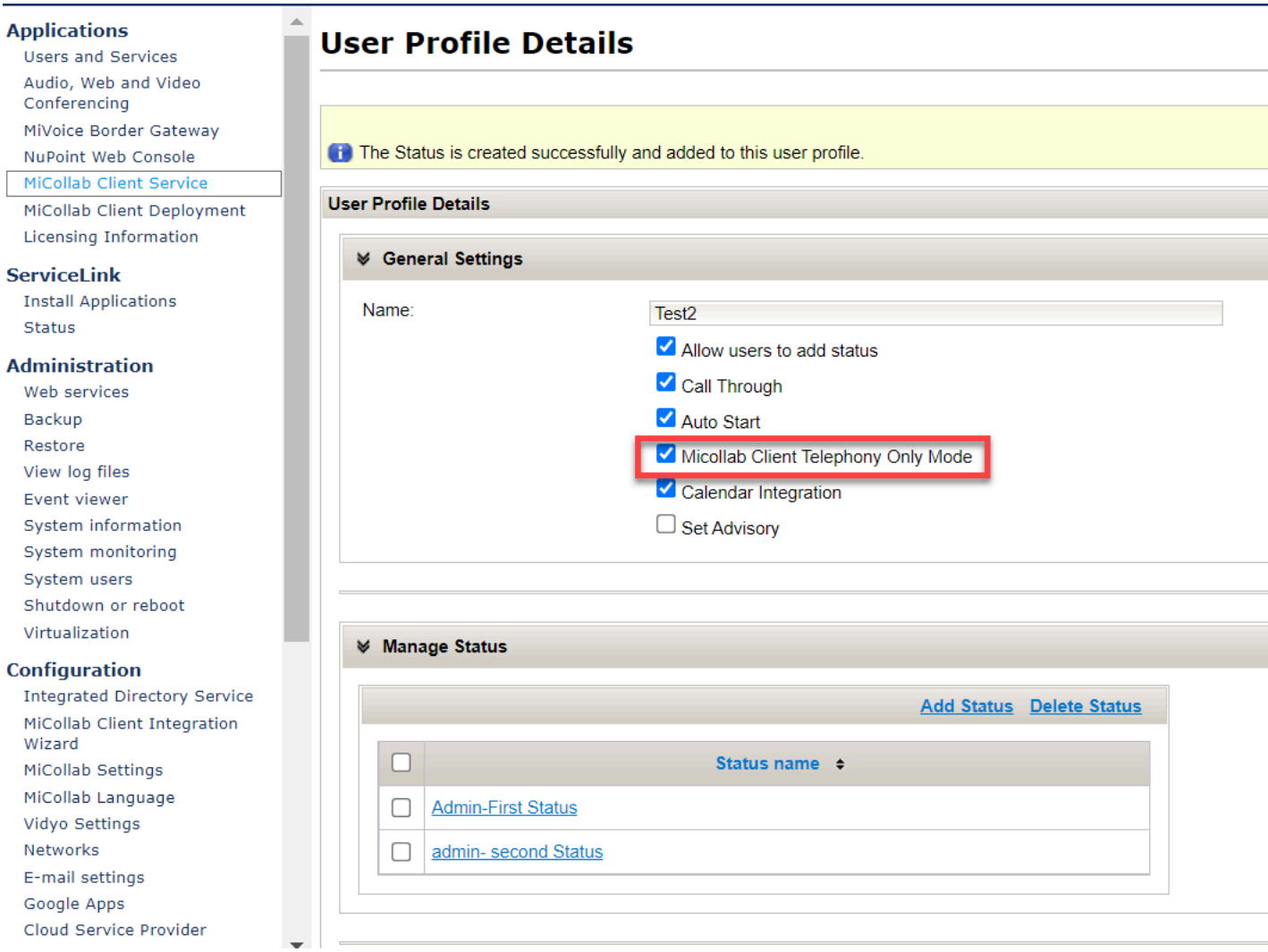
   The members will be assigned to that profile.



Enabling MiCollab Client Telephony Only Mode

The **MiCollab Client Telephony Only Mode** enhances the end-user experience while placing calls with a Mitel application (e.g. Mitel Assistant), using the MiCollab Client as the telephony endpoint. This mode is only applicable to MiCollab PC Clients and it provides the end-users with the required telephony features while being integrated with other Mitel applications. Mitel applications can cross-launch the MiCollab PC Client using

the Tel URI protocol. The administrator can enable/disable this mode from the MiCollab Client Service Administrator portal under the **User Profiles** tab for all or for selected group of users. This mode remains disabled for default user profile.



.