A MITEL
PRODUCT
GUIDE

MiVoice Connect

System Administration Guide

Release 19.3

Document Version 1.0

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.

®,™ Trademark of Mitel Networks Corporation

Contents

What's New in this Document 1

This section describes changes in this document due to new and changed functionality in MiVoice Connect Release 19.3. The changes are summarized in the following table.

Table 1: Document Version 1.0

Feature	Update	Location	Publish Date
New option to enable or disable TLS1.0 and TLS1.1	Users can use the **Enable TLS1.0 and TLS 1.1** option in the **Additional Parameters** page in Connect Director to enable/disable TLS 1.0 and TLS 1.1 in all MiVoice Connect components.	Configuring Other System Parameters on page 53	July 2022
New option to enable or disable FTP anonymous server.	Users can use the **Enable FTP anonymous server** option in the **Additional Parameters** page in Connect Director to enable/disable anonymous FTP on the MiVoice Connect server.	Configuring Other System Parameters on page 53	July 2022
Teleworker support.	6900-Series IP phones have teleworker support.	Supported IP and DECT Phones on page 284	July 2022

Feature	Update	Location	Publish Date
Caller ID display for BCA calls.	Users can enable or disable the **Show caller ID** option. Depending on the BCA call state, the caller ID is displayed.	Configuring an IP Phone Button for a BCA Extension on page 368	July 2022
Enhancements for Allow Auto Answer for BCA calls.	Enhancements are made to the **Allow Auto Answer** option to work for BCA calls while using a headset with a 6900-Series IP phone.	Configuring an IP Phone Button for a BCA Extension on page 368	July 2022
Provision to add or update InGate server.	Users can either add or update InGate server by using the **Hardware type** field in the **Administration** > **Appliances/ Servers** > **Platform Equipment** page in Connect Director.	• Adding Ingate on page 136 • Editing InGate Parameters on page 137	July 2022
Provision to download the certificate for InGate server.	Users with administrative permissions can use the **Download** option in the **Administration** > **Appliances/ Servers** > **Platform Equipment** page in Connect Director to download the certificate for InGate server.	Adding Ingate on page 136	July 2022

Feature	Update	Location	Publish Date
Update to the **Email address** field.	Added a note about the **Email address** field stating that the email address must be in a standard format and must not be duplicate.	General Tab on page 490	July 2022
MySQL Community Edition version update.	Beginning with Release 19.3, the MySQL version is upgraded from 5.7.29 to 5.7.37 Community Edition.	• Installing and Upgrading MySQL Archive and ODBC Connector on Secondary Server on page 1036 • Installing MySQL on a Secondary Server on page 1037	July 2022
New option to enable GrandParent site for emergency calls.	Users can use the **Use GrandParent site for emergency calls and other calls when no local trunks are available** option in the **Administration** > **System** > **Sites** > **General** tab page in Connect Director to enable a child site to use the grandparent site trunk for non-routable calls if no trunks are available at the child site.	Creating a Site on page 102	July 2022

Feature	Update	Location	Publish Date
Update to **Enable to HELD** option.	The **Enable to HELD** option is updated to **Enable HELD for E911**.	Telephony Tab on page 504	July 2022
Command check box exclusion for Ingate.	The **Command** check box is not applicable for InGate.	Status and Maintenance > Appliances List Pane on page 766	July 2022
Update to the **Status**, **Performance**, and **Calls** tabs for Ingate.	The **Status**, **Performance**, and **Calls** tabs in the **Status and Maintenance** > **Appliances** page in Connect Director are disabled by default for InGate.	Status and Maintenance > Appliances Details Pane on page 774	July 2022
Update to the **Upload location for logs** field.	Added the conditions to be met for log upload.	Configuring Other System Parameters on page 53	July 2022
Update to the **Client Password** field.	Added the value range for the **Client Password** field in the **Administration** > **Users** > **Users** tab in Connect Director.	General Tab on page 490	July 2022

Feature	Update	Location	Publish Date
Update to the **All Previous Log Files** pane.	The **Captured Phone Logs** and the **Captured Switch Logs** tabs are added to the **All Previous Log Files** pane in the **Diagnostics** > **Remote Packet Capture** page in Connect Director.	• Viewing Remote Packet Capture Log Files on page 840 • Deleting Remote Packet Capture Log Files on page 842	July 2022
Added the conditions to consider while saving the Jack number information.	When you enter the jack number information in the **Jack #** field in the **Administration** > **Users** > **General** tab in Connect Director, it is not saved. The conditions to consider to fix this issue are added as part of the 19.3 Release.	General Tab on page 490	July 2022
Added information regarding remote packet capture for 6900-Series phones.	In Connect Director, remote packet capture for 6900-Series phones fails. To fix this issue, you must collect the remote packet capture data from the phone and upload it to the respective server.	Diagnosing Switch or Phone Problems through RPC on page 834	July 2022

Feature	Update	Location	Publish Date
Added information about how to fix issue if the remote packet capture upload from Teleworker phone to HQ server through FTP or HTTPS does not work.	The remote packet capture upload from Teleworker phone to HQ server through FTP or HTTPS does not work. To fix this issue, you must upload the pcap to the local FTP/TFTP server.	Diagnosing Switch or Phone Problems through RPC on page 834	July 2022

Preface 2

This chapter contains the following sections:

This preface provides information about the objectives, organization, and conventions of the *MiVoice Connect System Administration Guide*.

2.1 Objectives and Audience for this Book

ShoreTel is now part of Mitel. Together, we look forward to helping you power connections that are brilliantly simple.

This guide is written for the person who uses Connect Director to configure, administer, and maintain the MiVoice Connect system.

2.2 Organization of this Book

The content in this guide is organized to reflect the order of the MiVoice Connect system's initial configuration.

The *Getting Started* section in the next chapter provides an ordered checklist to use the first time you configure the system.

2.3 Documentation Overview

The MiVoice Connect system is documented as described in the following sections.

2.3.1 System Documentation

You can access the following system documents at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform, and Connect Director provides links to these documents:

- *MiVoice Connect Planning and Installation Guide*
- *MiVoice Connect System Administration Guide* (this guide)

- *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide*

If the system includes the Connect Contact Center, refer to the *MiVoice Connect Contact Center Administration Guide* and the *MiVoice Connect Contact Center Installation Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-contact-center.

2.3.2 Hardware Documentation

The following hardware installation documents are packaged with their associated voice switch, IP phone, or appliance:

- *Voice Switch Quick Install Guide*
- *IP Phone Quick Install Guide*

2.3.3 User Documentation

User guides for the Connect client and for IP phones and button boxes are available from the Mitel documentation website:

- For Connect Client: https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/connect-client
- For IP phones and button boxes: https://www.mitel.com/document-center/devices-and-accessories/ip-phones

2.3.4 Release Notes

The *MiVoice Connect Release Notes* provide information about new releases and new features as well as issues that relate to new installations and upgrades. You can access this document on the Mitel documentation website: https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform. Connect Director includes a link to this document.

2.3.5 Online Knowledge Base

To access additional information or to resolve issues on Connect Director, you can use the Mitel Technical Knowledgebase, accessible at https://www.mitel.com/.

2.4 Document Conventions

The following conventions are used in this guide:

- Data-entry fields, hypertext links, control buttons, keywords, and other items within the system management interface are in a **bold** font.

- Information that you enter in data fields are in a data_entry font.

Using Connect Director 3

This chapter contains the following sections:

This chapter describes how to use Connect Director.

3.1 Introduction to Connect Director

Connect Director is a web-based tool for managing a MiVoice Connect system from anywhere on an IP network. You use Connect Director to configure, manage, and maintain all aspects of the MiVoice Connect system. Connect Director also includes maintenance pages that let you view status and issue maintenance commands for system components, including remote servers.

The main server (Headquarters) hosts the Connect Director web application. When you launch a web browser and navigate to the Connect Director website, the server provides HTML web pages from which you can add to, delete from, and edit the configuration of the system. When you click **Save**, your change is sent to the server and saved in the Mitel database. All other system components are automatically and immediately notified and updated.

Connect Director allows simultaneous access to Connect Director by multiple users. To ensure data integrity, the database is locked during save transactions in Connect Director. If another user tries to save changes while the database is locked, Connect Director advises the user that the changes were not saved; the user simply needs to save the changes again. Most changes to the database are completed within one second, so the probability of attempting to save while the database is locked is low.

Through administrative permissions, the MiVoice Connect system allows various levels of access to Connect Director. By default, the initial system administrator has access to everything on the system. You can assign other users one of several built-in roles, or you can define roles for more limited purposes such as allowing site administrators, directory list managers, and read-only users to perform specific tasks. You can define roles to provide only as much system access as each user requires by assigning a role with an appropriate permission level.

3.2 Starting Connect Director

This section assumes that the system software has been installed as described in the *MiVoice Connect Planning and Installation Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

To use Connect Director, your system must meet the following requirements:

- JavaScript and cookies must be enabled.
- Minimum supported screen resolution is 1280 x 720.

Before starting Connect Director, you need the following information:

- The fully qualified domain name (FQDN) or IP address of your Headquarters server
- Your user ID
- Your password

To start Connect Director:

1. Launch a browser.
2. In the URL field, enter the following:

   ```
   http://<FQDN or IP address of Headquarters server>/dm/login
   ```
3. Press **Enter**.

   The login screen appears.

Note:
For information about configuring access through Active Directory, see Using Active Directory with a MiVoice Connect System on page 522.

4. In the **Username** field, type your user name or the default user name (“admin”).
5. In the **Password** field, type your password or the default password (“changeme”).

Note:
Mitel recommends that you create a new user with administrator privilege. After you assign the full System Administrator role to a user, the default user “admin” is disabled. For additional information about granting administrative permissions to users, see Administrative Permissions on page 68.

6. Click **Login**.

   The system displays one of the following pages:

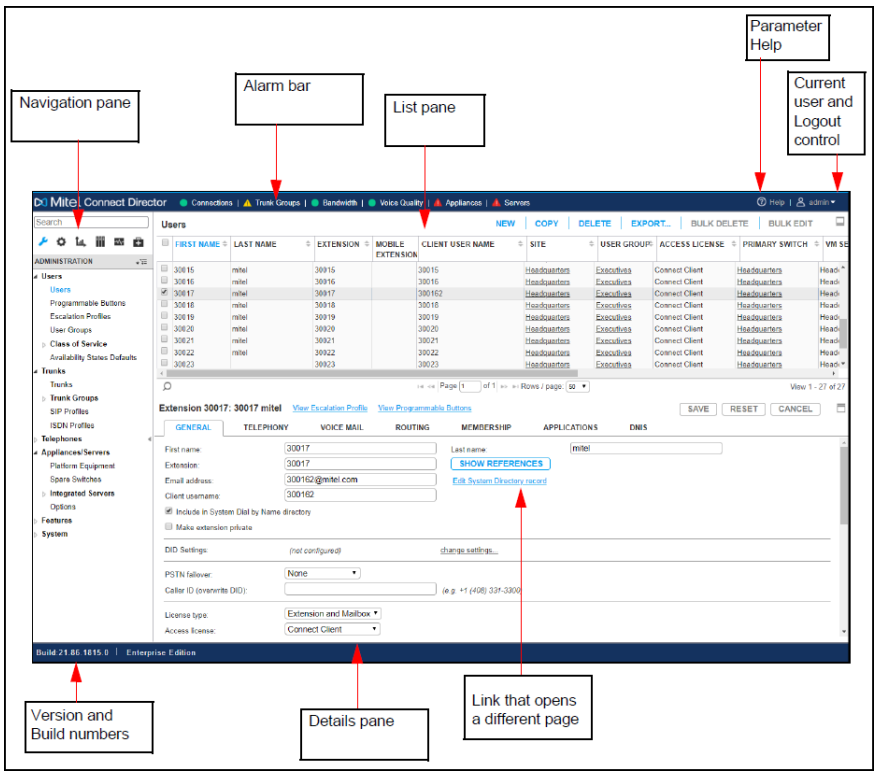
   - When you log in to a new system for the first time, the System Key Request page is displayed. For information about requesting the system key, see Installing a License Key on page 33.
   - Upon subsequent logins, if the system is not registered the License Requirements page is displayed. For information about registering the system, see Registering the MiVoice Connect Software on page 27.
   - If the system is registered, the Dashboard page in the Maintenance menu is displayed.

3.3 Understanding the Connect Director Interface

The Connect Director interface includes the following components, as illustrated in the figure below:

- The **alarm bar** shows at-a-glance status of system components.
- The **navigation pane** provides access to the menus in Connect Director.
- The **list pane** lists all particular objects of the type selected from the menu in the navigation pane.
- The **details pane** provides details for the object selected in the list pane.
- **Help** lets you access parameter descriptions for the current page.
- **Logout** lets you log out of Connect Director.
- **Build** indicates the build number of the MiVoice Connect system software that you are running.

Figure 1: Connect Director Interface



3.3.1 Navigation Pane

The navigation pane (see Navigation Pane figure below) is located on the left side of the Connect Director page and provides access to the menus described in Navigation Pane in Connect Director.

Table 2: Navigation Pane in Connect Director

Icon	Label	Description
	Search	Type a text string in the data-entry field to search the field labels on the Connect Director pages and the navigation menus. The search begins with the first letter you enter. The text you enter operates as if it begins and ends with a wild card. To dismiss the search window, press the **Esc** key or backspace to delete the text. **Note**: This search function is different from the filtering function available on the list panes in Connect Director. For more information about filtering on the list panes, see Filtering Information on page 20.
	Administration	Click this icon to open a menu that lets you configure users, trunks, telephones, appliances/servers, features, and other aspects of the MiVoice Connect system.
	System	Click this icon to open a menu that lets you configure licenses and administrative permissions.
	Reports	Click this icon to open a menu that lets you run reports on call details and web conferences.
	Documentation	Click this icon to open a menu that lets you link to Mitel product documentation.

Icon	Label	Description
	Maintenance	Click this icon to open a menu that lets you view status information about the components installed in your system. This menu also lets you access a system dashboard, system topology, alerts, call quality information, events, and event filters.
	Diagnostics	Click this icon to open a menu that lets you perform diagnostic tasks, such as running remote packet capture operations.

3.3.1.1 Viewing the Navigation Menu

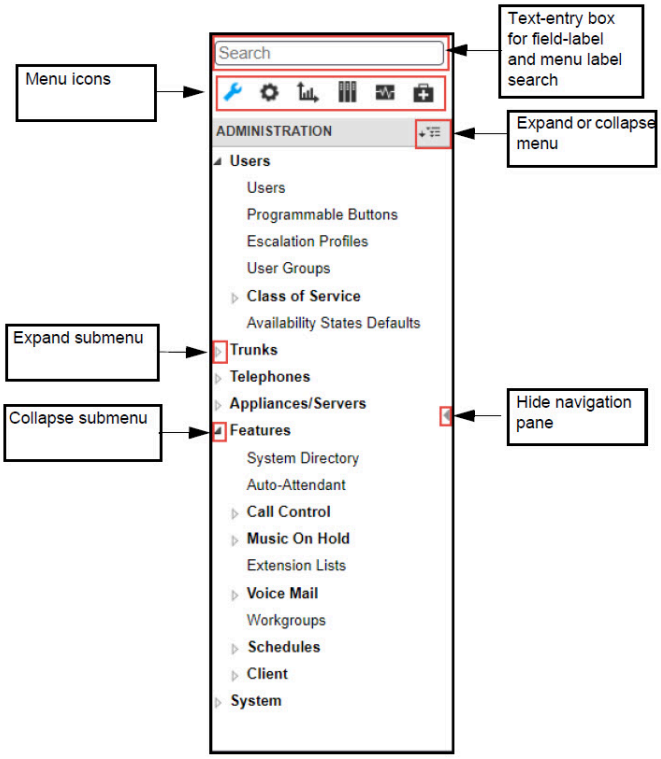
You can show or hide the Connect Director navigation pane as follows:

- To hide the navigation pane, click at the side of the pane.
- To show the navigation pane, click at the side of the minimized pane.

You can expand or collapse the navigation menu as follows:

- To expand the menu, click .
- To collapse the menu, click .

Figure 2: Navigation Pane



3.3.2 Alarm Bar

The alarm bar displayed at the top of the Connect Director interface shows alert status for the following major components and functions in the MiVoice Connect system:

- Connections alerts reflect issues with physical connections between devices such as servers and devices within the MiVoice Connect system or logical connections between MiVoice Connect software components, such as TMS, DRS, and voice mail services.
- Trunk Groups alerts involve issues with the trunks on a switch, which are used to route inbound and outbound calls.
- Bandwidth alerts reflect poor throughput in network bandwidth.
- Voice Quality alerts reflect issues involving poor voice quality in calls monitored by the MiVoice Connect system.
- Appliances alerts involve general switch and appliance issues that could affect the functionality or quality of MiVoice Connect services.
- Servers alerts involve general server issues that could affect the functionality or quality of MiVoice Connect services.
- Hybrid alerts involve issues related to hybrid applications such as Connect HYBRID Fax and Connect HYBRID Scribe. This category is displayed only if MiVoice Connect HYBRID services are enabled.

Alerts are issued to flag critical, warning, or informational situations. The color of a button indicates the highest alert severity for components or functions, as follows:

- (red) indicates at least one critical (error) alert. You can hover over the button to see how many warning and error alerts are in effect for that component type.
- (yellow) indicates at least one warning alert and no critical (error) alerts. You can hover over the button to see how many warning and error alerts are in effect for that component type.
- (green) indicates no critical (error) or warning alerts, but any number of informational alerts might have been issued.

The information displayed in the alarm bar is automatically refreshed every 30 seconds.

To view active alerts with the alarm bar:

1. Hover over a yellow or red button.

   The number of active error and warning alerts for that category are displayed in a pop-up window.
2. Click a button on the alarm bar.

The Alerts page opens, and it displays a list of all active alerts filtered by category, severity, and time interval. For detailed information about Alerts, see Monitoring Alerts on page 822.

3.3.3 Using List Panes and Details Panes

On Connect Director pages, you can:

- edit, add, delete, or copy configuration parameters
- view status
- issue commands

Most pages in Connect Director are divided into a top pane and a bottom pane:

- The top pane (the “list pane”) displays objects in the category that you have selected from the navigation menu. (For an example of a list pane, see List Pane Example.) List panes generally provide categorical information about the objects.
- The bottom pane (the “details pane”) displays detailed information about the object selected in the list pane. (For an example of a details pane, see Details Pane Example.) Where appropriate, the details pane also includes additional tabs and subtabs for more parameters. On Maintenance status pages, the details panes often provide additional tabs that display information such as detailed status, performance, and related calls.

When you click a particular category in the navigation menu, by default the first item in the list pane is selected and that item’s detailed information is displayed in the details pane. To display the details for a different object, click that object in the list pane. Specific

data-entry fields, drop-down lists, and option buttons are described in the appropriate sections throughout the subsequent chapters of this book.

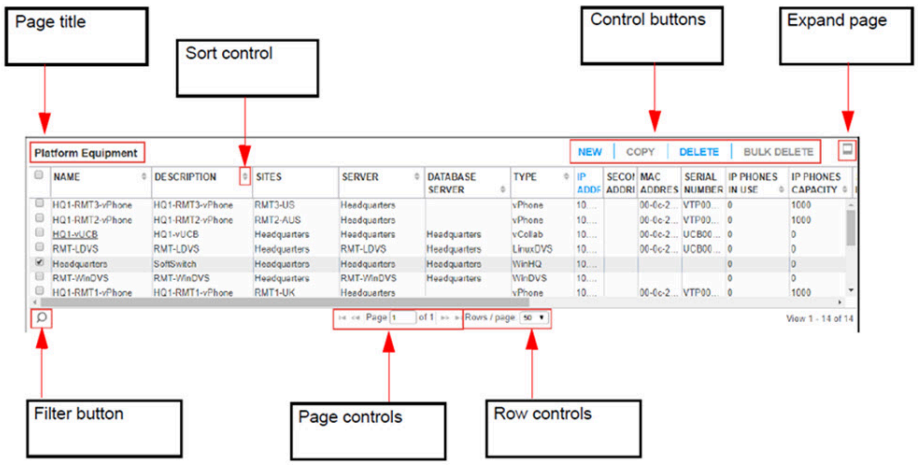
The details pane is where you specify parameters for new objects or edit parameters for existing objects. Fields marked with an asterisk (*) are mandatory fields and require that you enter a value or make a selection. When creating a new object, you must supply information in these fields. The pencil icon ( ) indicates that you have changed a value. After you add or change a parameter value, you must click **Save** to save the changes. The pencil icon is no longer displayed after your changes are saved.

In a list pane, you can adjust column widths, but you cannot rearrange columns or pick which columns to display.

In many of the Connect Director pages, you can control which page displays and the number of rows displayed by using controls on the bottom of the list pane, as shown in List Pane Example.

- You can navigate among the pages of information as follows:
  - For list panes you reach through the Administration menu, type a page number in the box or use the arrow keys.
  - For list panes you reach through the Maintenance menu, click a page number or click **First, Previous, Next,** or **Last**.
- You can change the number of rows in a list pane as follows:
  - For list panes you reach through the Administration menu, select the number of rows to show per pane by clicking the **Rows/page** drop-down list at the bottom of the pane and selecting a number.
  - For list panes you reach through the Maintenance menu, select the number of rows to show per pane by clicking the **Show *n* entries** drop-down list at the bottom of the pane and selecting a number.
- You can adjust the size of the panes as follows:
  - To expand the list pane (top pane) to a full page, click .
  - To expand the details pane (bottom pane) to a full page, click .
  - To show both the list pane and the details pane, click .

Figure 3: List Pane Example

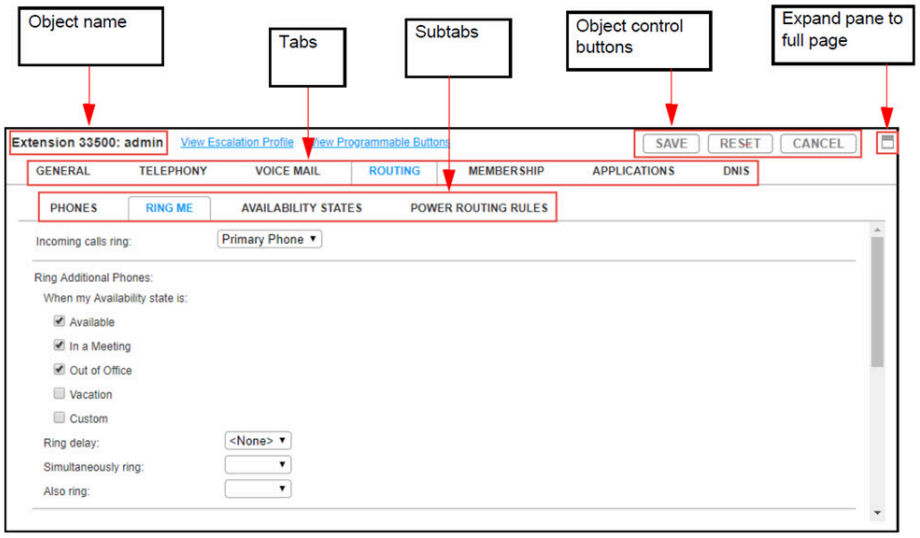


The control buttons that you can use to add, copy, delete, or export objects are described in Control Buttons in Connect Director. Specific data-entry fields, drop-down lists, and option buttons are described in the appropriate sections throughout each chapter.

Table 3: Control Buttons in Connect Director

Button	Function
New	Creates a new object profile by using default values.
Copy	Creates a copy of the current object profile that you can use to create a new ob ject profile. Some values, such as extension numbers, are automatically gene rated for the new profile.
Delete	Removes the current object from the system.
Export	Allows you to export the selected objects in comma-separated variable format.
Bulk Edit	Allows you to edit certain fields for multiple items at once. For an example of how to use the bulk edit functionality, see Copying Programmable Button Configurations on page 334.
Bulk Delete	Allows you to delete certain fields for multiple items at once.
Move	For telephones, this option allows you to move the selected telephones to a diff erent switch.
Save	Saves the changes you make to the profile.
Reset	Reverts to the last saved profile.
Cancel	Cancels the changes you make to the profile.

Figure 4: Details Pane Example

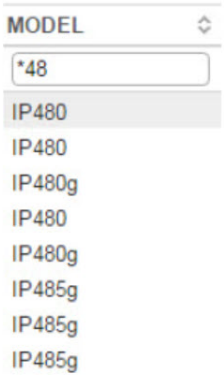


3.3.4 Filtering Information

To find information quickly, you can filter the data displayed in many of the Connect Director pages.

When you enter text for a filter, the system filters for items that begin with those letters. The filter is not case sensitive. You can include a wild card in the text string. For example, if you type “*48” in the filter for the Model column on the IP Phones status page, you see all phone models that contain “48”. The Filter Example figure illustrates this example.

Figure 5: Filter Example



To filter information displayed on a page in Connect Director:

1. On any list pane in Connect Director, click

   Text boxes and drop-down lists are displayed under the column headings for the fields you can use as filters.

2. To define a filter, do any of the following:

   - Enter text in one or more text boxes.
   - Select an item from one or more drop-down lists.
   - For date and time columns:

   a. Click in the first text box for the column, and select a day from the calendar and use the slider bars to specify the hour and minute.
   b. Click in the second text box for the column, and then do one of the following:

      - Select a day from the calendar and use the slider bars to specify the hour and minute.
      - Click **Now**.

   c. Click **Done**.

Note:
At least one date and time field must be entered to filter on a date and time range. If the start time is left blank, the earliest possible date and time are used. If the end time is left blank, the latest possible date and time are used.

3. To apply the filter, click  .

   The rows are filtered to display information that matches the filter you entered.

4. If you want to close the filter box but retain the filtered results, click  .
5. To clear the filter, click  .

   All rows are again displayed.

3.3.5 Sorting Displayed Information

The records on each list pane are presented in a default sort order. You can change the sort order to ascending or descending order by clicking a column heading. When you sort a column in a list pane, the icon next to the column heading changes from  to or , which indicates whether the sort is ascending or descending.

Note:
You can apply a filter to sorted data, or you can sort filtered data.

1. Launch Connect Director.
2. In the navigation menu, click the page you want to use.

   The page launches.
3. In the list pane, click the column heading you want to sort by.

   The rows are sorted accordingly.

3.3.6 Getting Help

To get help for the parameters on the Connect Director page that you are viewing, click **Help**.

You can access documentation for MiVoice Connect through the Documentation menu in Connect Director. In the navigation menu, click Documentation and then the particular document or category of documents you want to view.

You can also access the full set of product documentation for MiVoice Connect from Mitel Doc Center located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

3.4 Getting Started with System Configuration

This section summarizes the tasks necessary to configure your system for the first time. This list also follows the order in which this guide is organized. Before you begin configuring the system, ensure that the system has been properly installed as described in the MiVoice Connect Planning and Installation Guide.

You must download Mitel's Windows PowerShell script utility, "TacTools", to help verify server prerequisites, validate certificates, check system load balancing, and other useful functions for migration preparation and system administration. TacTools is available as a free download from the partner knowledgebase at the following location:

- For Partners: https://mitelcommunity.force.com/partner/s/article/TAC-Tools-Powershell-Scripts
- For Customers: https://mitelcommunity.force.com/customer/s/article/TAC-Tools-Powershell-Scripts

Disclaimer:

The TacTools script was written and provided by TAC. It is provided on a "best effort" basis and is not guaranteed to function properly in your environment. TAC will not troubleshoot the script in a customer's environment. Many modules are written to be "read only" to minimize any potential impact on the customer's server. Running any modules that will make any changes to your server will prompt you for confirmation. It

is recommended that if you run a module that can make changes to your server, then you must run the script as part of a maintenance window, and must accept any potential service impact caused by the changes made to your server.

- Launch Connect Director as described in Starting Connect Director on page 11.
- Register the Mitel software and request a license key or keys. For more information, see Managing License Keys on page 32.

  Prompt registration in Connect Director is encouraged to ensure that Mitel staff has current information about your Mitel products and installation.
- Install your license key or license keys if you have them. Until you have updated all required licenses, Connect Director will continue to open to the License Requirements page after login. **You have up to 45 days to install the licenses. If the licenses are not installed during that time, you cannot continue to use the MiVoice Connect software.** For information about installing license keys, see Managing License Keys on page 32.
- Configure system parameters as follows:

  1. Specify the dialing conventions to use throughout the system. The dialing conventions include extension length as well as the dialing plan reservations for extensions and trunk access codes. For more information about dialing plans, see Setting Dial Plan Parameters on page 41.
  2. Configure the system's extensions from the System Extensions page. Review the default system extensions and, if necessary, change them if the system must use these defaults for other purposes. For more information about system extensions, see Configuring System Extensions on page 49.
  3. Specify the languages you want to make available for the system. (ensure you have appropriate licenses for the languages).
  4. Review the password and log file settings on the Additional Parameters page. See Configuring Other System Parameters on page 53for more information about other configurable parameters. Mitel created the defaults to apply widely, so they can probably remain at their current values.
- If you want to ensure secure client access, install a certificate from a Certification Authority on your Headquarters server. For more information, see Certificates on page 81. Otherwise, you can use the default certificates pre-installed on your MiVoice Connect system.
- Create and configure the sites that you want your MiVoice Connect system to include. For more information, see Overview on page 100.

Note:
The **Night bell switch** and **Paging extension** parameters are included on the Sites page, but you cannot configure these parameters until the proper switch is configured. In addition, before you can configure **Operator extension** or **Fax redirect extension**, you must configure the proper users. For more information, see Overview on page 460.

- Set the IP address range for the IP phones at any remote sites. On the IP Phone Address map page, you define IP address ranges so that IP phones are assigned to the correct site. IP phones not assigned to a remote site are associated with Headquarters.
- Configure additional sites if desired. For more information, see Overview on page 100.
- Configure MiVoice Connect servers, voice switches, and other appliances using the Platform Equipment page.
  - For information about how to configure additional Mitel application servers, see Overview on page 115. For each additional server, do the following:

    1. Name the server and assign it to a site.
    2. Create the new server and configure it.
    3. Set the voice mail and auto-attendant extensions.
    4. Assign a user group to the server.
  - For information about how to configure voice switches and other appliances, see Switch Types on page 150. For each switch or appliance, do the following:

    1. Select the role (primary or spare) that you want the switch to perform for the site.
    2. Identify the site where you want to use the switch or appliance.
    3. Select the appliance type you want to use.
    4. Create the appliance profile.
    5. Provide a name and description for the appliance, and use the Find switches button to discover each voice switch or appliance on the network.
    6. For each switch, specify the server that you want to manage the switch.
    7. Each voice switch must have a valid IP address from a DHCP server or an address statically configured from the serial port.
- Configure IP phones. For more information, see Overview on page 284.

  1. Add IP phone ports to your voice switches as necessary to support your IP phones. Each switch port that is assigned to IP phones supports five IP phones.
  2. Set the boot parameters for the IP phones. IP phones are set to find boot information from a DHCP server. If your installation has other requirements, use the

set-up menu on the IP phone to set server and boot configuration parameters. For more information, see the MiVoice Connect Planning and Installation Guide.

You can speed up the installation by using the Extension Assignment feature. For more information, see Configuring Extension Assignment on page 549.

- Configure the following users in the following order before you add general users to the system:

  1. During installation, a system administrator is set up. Assign a person at your site to this role. When you assign a system administrator, the default user ID and password must be changed. Make a note of the new user ID and password, because the default user ID (“admin”) and the default password (“changeme”) will no longer be available.
  2. Configure an operator for each site. See Administrative Permissions on page 68for more information. This is the extension reached when 0 is dialed from the telephone. Note that operators can span sites.
  3. Configure a “user” as the Fax Redirect extension for each site.
  4. Configure a user as the default Personal Assistant for all other users. This is the user that callers are routed to when they dial “0” in a user’s mailbox. It is important that you configure the default Personal Assistant before adding the bulk of the users so that appropriate defaults can be assigned. If you omit this step, you may have to spend time reconfiguring the users later.
  5. Configure the Availability states and assign the Personal Assistant.
- Complete configuration of sites as follows:

  1. Return to the Sites page and complete the configuration for Night Bell, Paging, Operator, and Fax Redirect.
  2. If you have added additional servers, review the details for each site and reconfigure as appropriate.
- Configure all trunk groups and trunks as follows:

  1. Configure trunk groups from the Trunk Groups page. You can modify the default trunk groups and add new trunk groups.
  2. Depending on the trunk type, configure individual trunks from either the Trunks page or the Platform Equipment page. For example, SIP trunks are best configured on the Trunks page, but trunks on a voice switch-T1 can quickly be configured using the **Fill Down** button on the Platform Equipment page.
- Configure user groups (including Class of Service permissions) and users. For details, see Overview on page 460.
- Configure call control parameters, and set up hunt groups and paging groups as needed. For details, see Configuring Account Codes on page 352.
- Configure voice mail parameters and system distribution lists as described in Configuring Voice Mail Options on page 587.

- Configure the auto-attendant parameters and menus as described in Overview on page 611.
- Set schedules to be used by the auto-attendant or paging groups. For more information about schedules, see Overview on page 621.
- Configure workgroups, including schedules and the queue, as described in Overview on page 628.
- Configure the system directory as described in Overview on page 667. If you use Microsoft Exchange and Microsoft Outlook, you can leverage Contacts on the Exchange Server for common contact information.
- If using Connect Contact Center, you must configure it. Refer to the *MiVoice Connect Contact Center Administration Guide* and the *Mitel Contact Center Installation Guide* for information.

Registering and Licensing the MiVoice Connect Software

4

This chapter contains the following sections:

This chapter describes how to register your MiVoice Connect software and manage licensing.

4.1 Registering the MiVoice Connect Software

After installing or upgrading, you must register the new MiVoice Connect software. **If registration is not received by Mitel within 45 days of installation, access to Connect Director is denied**.

For upgrades, if you have previously submitted your contact information to Mitel and your system is connected to the Internet, your contact information is automatically submitted during subsequent upgrades.

4.1.1 Information Collected through Product Registration

When you install or upgrade a system and request license keys, the following information is collected through product registration:

- Contact information
- License key list:
  - current license keys
  - features activated
  - features available for activation for each licensed feature
- Server MAC address
- Sales Order Number (for initial installations only)
- Switch inventory:
  - switch types
  - MAC addresses
  - serial numbers

- Installed software version information:
  - product name
  - build number
  - install timestamp

All this information is included in the End User License Agreement (EULA) provided for an installation or upgrade.

4.1.2 Registration Process

To receive unlimited access to Connect Director, you must complete the product registration process.

The MiVoice Connect system software can be registered automatically, over the Internet, or through email. These methods are described in the following sections. When registering automatically or over the Internet, registration data is transmitted to Mitel over a secure connection to ensure integrity and privacy.

For upgrades that meet the following prerequisites, the software is registered automatically:

- Contact Information is saved in Connect Director before starting the upgrade process.
- A valid system license key is installed before starting the upgrade process.
- Your system can connect through the Internet to the Mitel Support web site https://www.mitel.com/support.

For new installations or upgrades that do not meet these prerequisites, you are prompted to register the software the first time you launch Connect Director after installing or upgrading. You can choose to register the software over the Internet or through email, but registration over the Internet is completed more quickly than through email.

If your installation does not have adequate or current licenses, Connect Director displays the License Preview page when you have completed or skipped registration. For more information about licenses, see Managing License Keys on page 32.

4.1.2.1 Registering Automatically

1. Install or upgrade the Mitel software.
2. Start the Headquarters server, and then log in to Connect Director.

Registration information is sent over the Internet to Mitel. Upon receipt, Mitel sends a response. When the response is received, a compliance token is created on the Headquarters server, and Connect Director is unlocked.

Note:
Until registration is completed, a Reminder Notification (“out-of-date” message) in red letters is displayed on the **Contact Information** page.

4.1.2.2 Registering over the Internet

1. Upgrade or install the Mitel software.
2. Start the Connect Headquarters server, and then log in to Connect Director.
3. Do one of the following to display the **Contact Information** page:
   - When prompted to register, click **Now**.
   - In the navigation pane, click **System** > **Contact Information**.
4. On the **Contact Information** page, enter information in the fields, as described in Fields on the Contact Information Page.
5. Click **Save**.
6. Click **Now**.

Note:
The **License Preview** page is displayed. For more information about licensing, see Managing License Keys on page 32.

7. On the **License Preview** page, click **Submit**.

Note:
Registration information is sent over the Internet to Mitel. Upon receipt, Mitel sends a response. When the response is received, a compliance token is created on the Headquarters server, and Connect Director is unlocked.

Note:
Until registration is completed, a Reminder Notification (“out-of-date” message) is displayed on the **Contact Information** page.

Table 4: Fields on the Contact Information Page

Field Name	Description
Register and request system key	Select either of the following options to register and request a system key: • Now • Print
Partner name	Name of the partner or reseller from whom the system was purchased. This field is required.
Company name	Name of the customer's company. This field is required.
Address	Address of the company. This field is required.
City	City where the company is located. This field is required.
State/Province	State or province where the company is located.
Postal code	Postal code for the company.
Country	Country where the company is located.
Main phone	Main telephone number of the company. This field is required.
Main email	Main email address of the company.
Server MAC address	MAC address of the server where the Headquarters server is installed. This field is automatically populated with information from the server. Change this information only if you want a license for a server other than the one to which you are currently connected. If you have changed this information but want to revert to the defaults, click **Reset**.
Sales order number	The Sales order number, which you can find on the Mitel Sales packing sl ip. This number is required only if license keys have not been entered in Connect Director. For system upgrades, the sales order number is optio nal.
Primary contact	
Name	Name of the administrator responsible for the MiVoice Connect system. This field is required.
Title	Job title of the administrator responsible for the MiVoice Connect system.
Phone	Phone number of the administrator responsible for the MiVoice Connect system. This field is required.
Pager	Pager number of the administrator responsible for the MiVoice Connect system.
Email	E-mail address of the administrator responsible for the MiVoice Connect system.

Field Name	Description
Secondary contact (recommended)	
Name	Name of the back up administrator Mitel can contact regarding the MiVoic e Connect system.
Title	Job title of the back up administrator Mitel can contact regarding the M iVoice Connect system.
Phone	Phone number of the back up administrator Mitel can contact regarding the MiVoice Connect system.
Pager	Pager number of the back up administrator Mitel can contact regarding th e MiVoice Connect system.
Email	Email address of the back up administrator Mitel can contact regarding t he MiVoice Connect system.

4.1.2.3 Registering by Email

1. Upgrade or install the Mitel software, and then launch Connect Director.
2. Do one of the following to display the **Contact Information** page:

   - When prompted to register, click **Now**.
   - In the navigation pane, click **System** > **Contact Information**.

   The **Contact Information** page is displayed.
3. On the **Contact Information** page, enter information in the fields, as described in the Fields on the Contact Information Page.
4. Click **Save**.
5. Click **Now**.

Note:
The **License Preview** page is displayed. For more information about licenses, see Managing License Keys on page 32.

6. On the **License Preview** page, click **Save to File**.

   The `LicenseRequest.slr` file is produced.
7. Save the `LicenseRequest.slr` file to your desktop or another location so that you can easily locate it.
8. Email the `LicenseRequest.slr` file to license.support@mitel.com.

Note:
Upon receipt, Mitel sends a response containing a compliance token that grants access to Connect Director. This token (license key) is associated with the Server MAC address and a system build number.

9. Verify the compliance token.

   a. Click **Administration** > **System Parameters** > **Product Verification**.

      The **Product Verification** page is displayed.

   b. Enter the Compliance Token and click **Verify**.

4.1.2.4 If Registration Is Not Received by Mitel

When your Mitel software is registered automatically or over the Internet, if registration information is not received by Mitel (for any reason), Connect Director submits the information every hour for seven days after installing or upgrading.

If the process is unsuccessful, you must submit the Contact Information again (over the Internet or through email) as often as necessary until registration is completed.

After you register and apply for licenses, Mitel acknowledges your submission in an email message and mails your system key within 3-5 days. Until the license key arrives, when you want to use Connect Director you can click **Later** in the Connect Director Welcome screen to enter Connect Director. You have up to 45 days to install the license key.

If registration is not completed in 45 days, Connect Director is locked.

4.2 Managing License Keys

The subsequent sections describe license compliance, how to view licenses and install license keys, and license types.

4.2.1 Compliance

If your system does not comply with Mitel's license requirements, Connect Director offers 45 days to comply with the license requirements. To comply, you can remove unneeded configurations, order additional licenses, or do both. The 45-day grace period allows you to make ad hoc, unplanned changes that could temporarily exceed your license limits, but it gives you time to get back into compliance.

You can easily print or send the license status page via e-mail for purposes of license compliance verification. License status is never transmitted without explicit action by a Mitel administrator.

Note:
Do not upgrade unless your installation complies with your current license requirements. If you upgrade your system while it is out of compliance, you have only 45 days before you are locked out of Connect Director. If you have license issues, contact your Mitel Partner or Mitel Installed Base Business Services Team at micare_admin@mitel.com.

4.2.2 Viewing Licenses in Connect Director

The License Requirements page lists licenses that are available for the MiVoice Connect system and the quantity of configured and purchased licenses for each type of license. You can use this page to track and manage all licenses. Details about licenses are provided in License Types on page 34.

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Licenses** > **License Requirements**. The **License Requirements** page is displayed.

4.2.3 Installing a License Key

1. View the license packet that you received from Mitel.
2. Launch Connect Director.
3. In the navigation pane, click **System** > **Licenses** > **License Keys**. The **License Keys** page is displayed.
4. Click **New** at the top of the page.

Note:
The **General** tab is displayed in the details pane at the bottom of the page.

5. On the **General** tab, enter the following information:
   - In the **Key** field, copy and paste all license keys that you received from Mitel. (You can paste in multiple license keys at once.)
   - In the **Comment** field, enter a description of the licenses.
6. Click **Save**.

4.2.4 License Types

Mitel licenses are categorized as either self-audited or keyed licenses.

4.2.4.1 Self-Audited Licenses

Self-audited licenses do not have a key associated with them. They are tracked on the License Requirements page to assist system administrators in tracking the number of required licenses based on the current configuration versus the number that have been purchased, which they enter manually.

For the following types of self-audited licenses, if the usage exceeds the current number of licenses, you are notified until licensed capacities meet or exceed usage:

- **Phone Only Access License:** This count includes the number of desk phones.
- **Remote Server Software:** This count includes licenses that correspond to the number of distributed voice servers. Up to 20 remote servers can be configured in addition to the Headquarters server.
- **TAPI Application Server:** This count includes licenses for remote TAPI Application Servers that have the “Allow Voice Mailboxes” check box deselected. The number purchased should match the number of deprioritized servers that exist at a particular site.
- **Phone API License:** This count includes licenses for the Phone API. (For more information, contact Mitel Professional Services for the appropriate SDK document).

4.2.4.2 Keyed Licenses

You add keyed licenses by entering a license key string obtained from Mitel or a partner. Embedded in the license key are the type and number of licenses associated with that key. When a valid key is entered, the system decodes it and details the type and number of licenses added. Keyed licenses are additive, and more than one can be entered into Connect Director over time.

These licenses are tracked in the Keyed Licenses section on the License Requirements page in Connect Director. The types of keyed licenses are as follows:

- **System License:** This count includes licenses required on a per-system basis.
- **Additional Site License:** This count includes licenses required for each site beyond the main headquarter location. For installed base customers, when you upgrade and request your new system key, you will automatically receive additional site licenses for all configured sites.
- **Extension License:** This count includes all extensions licensed by both Extension Only and Extension and Mailbox licenses. For more information about this license type, see Extension and Mailbox Licenses on page 36.

- **Mailbox License:** This count includes all mailboxes licensed by both Mailbox Only and Extension and Mailbox licenses. For more information about this license type, see Extension and Mailbox Licenses on page 36.
- **SoftPhone License:** This count includes SoftPhone licenses, which are issued on a per-user basis. Obtain and install one license for each SoftPhone user.
- **Additional Language License:** This count includes licenses if more than one language is enabled.
- **Mobile Access License** is required for each client that is enabled for Mobility.
- **SIP Phone License** is a keyed license that enables the system to support one SIP device through a SIP proxy.

Note:

400-Series IP phones and 6900-Series (6910, 6920, 6930, and 6940) phones do not require such a license.

- **SIP Trunk License** is a keyed license required to enable one physical SIP trunk.
- **Standard Resolution Video License** is a keyed license that enables the Connect client to support one point-to-point video session at VGA resolution (640x480).
- **High Resolution Video License** is a keyed license that enables the Connect client to support one point-to-point video session at XGA resolution (1024x768).
- **Connect Client Access License** is a keyed license that provides access to the following capabilities:
  - All functions available through the Phone Only Access License
  - Instant Messaging Presence
  - Contact Viewer
  - Call recording
- **Workgroup Agent Access License** is a keyed license that provides access to the following:
  - All functions available through Connect Client Access License
  - Ability to transfer calls by dragging and dropping call cells into the buddy list
  - Workgroup access utilities, including log in and log out
  - Workgroup Queue Monitor

- **Workgroup Supervisor Access License** is a keyed license that provides access to the following:
  - All functions available through Workgroup Agent Access License
  - Workgroup access utilities, including log in, log out, and wrap up
  - Workgroup Agent Monitor

Note:
This license allows you to change the mode of another user.

- **Operator Access License** is a keyed license that provides access to the following:
  - All functions available through Workgroup Supervisor Access License
  - Access to XGA video
  - Extension Monitor

Note:
This license allows you to change the mode of another user.

- **External Unified Messaging SIP Link** is a keyed license that is required for each Unified Messaging (SIP) server.
- **Audio Conference License** is a keyed license that is necessary for each audio port that you want to use in conferences managed by a Service Appliance.
- **Web Conference License** is a keyed license that enables web ports for use in conferences managed by a Service Appliance.
- **Virtual Switch IP Phone License** is a keyed license that supports devices connected to virtual phone switches. The system requires one license for each device connected to a virtual phone switch. In addition, Extension or Extension and Mailbox licenses are required to enable users on a virtual IP Phone switch.
- **Virtual Switch SIP Trunk License** is a keyed license that is required to enable one SIP trunk on a virtual SIP trunk switch. No additional SIP trunk license is required.
- **Remote Phone License** is a keyed license that allows access for VPN phones. This applies to softphones or desk phones that you want to deploy remotely.
- **Virtual Edge Gateway License** is a keyed license that provides access to the virtual Edge Gateway appliance.

4.2.4.3 Extension and Mailbox Licenses

Systems require one extension license for each configured extension-only user. If more than one key is installed, the number of licenses purchased is the sum of licenses for all valid keys. Extension-only users have an extension but no Mitel voice mailbox. They

may have external mailboxes they can access using Simplified Message Desk Interface (SMDI), QSIG, or SIP Unified Messaging.

Systems require one Mailbox license for each configured Mailbox-only user. If more than one key is installed, the number of licenses purchased is the sum of licenses for all valid keys. Mailbox-only users are only those users with Mitel mailboxes that may use SMDI.

Systems require one Combo license for each user configured for Extensions and Mailboxes. If more than one key is installed, the number of licenses purchased is the sum of licenses for all valid keys.

Features Available with Extension, Mailbox, and Combo Licenses lists the features available through Extension, Mailbox, and Combo licenses.

Table 5: Features Available with Extension, Mailbox, and Combo Licenses

Feature	Combo	Extension Only Includes 3rd-party SMDI-based voice mail to Mitel PBX	Mailbox Only Includes Mitel SMDI-based voice mail to 3rd-party PBX
PBX features			
Use SoftPhone (requires SoftPhone license)	Yes	Yes	No
Make calls, take calls, etc.	Yes	Yes	No
Voicemail features			
Configure availability states	Yes	Yes	Yes
Forward calls to configured destination	Yes	Yes	No
Create and play greetings	Yes	No	Yes

Feature	Combo	Extension Only	Mailbox Only
		Includes 3rd-party SMDI-based voice mail to Mitel PBX	Includes Mitel S MDI-based voice mail to 3rd-party PBX
Use the Personal Assistant	Yes	No	Yes
Notification escalation	Yes	No	Yes
Configure Find Me	Yes	No	Yes
System call routing schedule	Yes	No	Yes
Create call routing notes	Yes	Yes	Yes
Assign extension	Yes	No	Yes
Record name	Yes	No	Yes
Automated attendant features			
Dial by number, name	Yes	Yes	Yes
Transfer to / Go to extension	Yes	Yes	Yes
Message by number, name	Yes	Yes	Yes
Advanced features			

Feature	Combo	Extension Only	Mailbox Only
		Includes 3rd-party SMDI-based voice mail to Mitel PBX	Includes Mitel S MDI-based voice mail to 3rd-party PBX
Extension assignment	Yes	Yes	No
Member of a hunt group	Yes	Yes	No
Member of a workgroup	Yes	Yes	No
Connect client features			
Connect client: Phone Only, Connect Client, Workgroup Agent, Workgroup Supervisor, Operator	Yes	No mailbox features	No extension features
Extension monitor	Yes	Operator-only features	No
Agent monitor	Yes	No mailbox features	No
Queue monitor	Yes	No mailbox features	No
Voice mail viewer	Yes	No	Yes
Call history	Yes	Yes	No
System directory	Yes	No mailbox features	No extension features

Feature	Combo	Extension Only Includes 3rd-party SMDI-based voice mail to Mitel PBX	Mailbox Only Includes Mitel S MDI-based voice mail to 3rd-party PBX
Outlook features			
Forward voice mail as .wav attachment	Yes	No	Yes
Voice mail form integration	Yes	No	Yes
Outlook Contact/ Quick Dialer	Yes	Yes	No
Outlook Contact/ Screen Pop	Yes	Yes	No
Outlook Calendar integration	Yes	Yes	Yes

Note:

- Although call forwarding is handled by the third-party PBX, calls arriving at the Connect voice mail system are routed as specified by Connect voice mail forwarding conditions
- Calls will be directed to mailbox only.
- Calls will be directed to mailbox only.

Setting Up System Parameters 5

This chapter contains the following sections:

This chapter describes how to specify system-wide parameters in Connect Director.

5.1 Setting Dial Plan Parameters

The dial plan defines the numbering convention your MiVoice Connect system uses to route calls. The system uses the dial plan to parse dialed numbers—whether from internal users or the Public Switched Telephone Network (PSTN)—and to direct calls appropriately. The dial plan can include extensions, site codes (pre-extensions), access codes for trunks, and account codes.

This section describes how to set the parameters for creating number strings in a dial plan. These parameters are set using the Dial Plan page in Connect Director. On the Dial Plan page, you can:

- Specify the lead digit used in a string.
- Specify how you want the MiVoice Connect system to interpret each leading digit.
- Specify the number of digits included in an extension.

Note:

- You cannot reduce the number of digits included in an extension after the parameter is set.
- Mitel strongly recommends that administrators configure dial plans using Connect Director. Because dial plan entries can consume a large amount of switch resources, Mitel also recommends that administrators closely monitor switch CPU and memory usage. Monitoring the switch usage helps administrators determine when it is necessary to reduce the number of stored entries after adding a large number of DNIS or Prefix entries.
- The default and custom plan combined length for Site Dialing Rules and Trunk Dialing Rules should not exceed 2000 characters.

Manipulation of Mitel databases can cause undesired results. In the event that manual or 3rd party database changes cause undesired results, Mitel Support may require that those database changes be reversed to resolve the issue

Before beginning, for each Mitel site review the MiVoice Connect system deployment and topology and the local telephone company dial plan and dial rules.

5.1.1 Setting the String Parameters Used in Your Dial Plan

All available digits are pre-configured as lead dial strings. Reconfigure only those dial strings that you want to use for special purposes.

Note:
Because the MiVoice Connect system allows users to dial emergency numbers with or without a trunk access code, extensions must not conflict with the leading digits of emergency telephone numbers. If you deploy a global voice network, you must consider the leading digits of emergency numbers for all the international locations in your system.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Dialing Plan** > **Dial Plan**. The **Dial Plan** page is displayed.
3. In the drop-down list for a digit, select the parameter that you want to assign to that leading digit. See the table below for descriptions of available parameters.
4. Repeat Step 3 for every digit you want to assign.
5. When you are finished entering values, click **Save**.

Note:

After you set and save a leading digit parameter, you cannot change it in the following situations:

- The leading digit is an extension prefix. In addition, be aware that setting extension prefixes is a one-time activity. If you leave any extension prefixes unused, you cannot assign them later.
- The leading digit is an extension digit that already has extensions configured starting with that digit.
- The leading digit is configured as the leading digit of a trunk access code for a trunk group.

In these cases, after the change is saved the field is unselectable.

Table 6: Dial Plan Page: Digit Reservation Parameters on the General Tab

Option	Description
Extensions	Reserves this digit as the leading digit in an extension.
Trunk Access Codes (1 Digit)	Reserves this digit for use as a one-digit trunk access code. When you assign a number as the leading digit in a trunk access code, using the same number as the leading digit in extensions can cause the system to misroute calls.
Trunk Access Codes (2 Digit)	Reserves this digit as the lead digit in two-digit trunk access codes. When you assign a number as the leading digit in a trunk access code, using the same number as the leading digit in extensions can cause the system to misroute calls.

Option	Description
Trunk Access Codes (3 Digit)	Reserves this digit as the lead digit in three-digit trunk access codes. When you assign a number as the leading digit in a trunk access code, using the same number as the leading digit in extensions can cause the system to misroute calls.
Not Used	Specifies that this digit cannot be used as a lead digit.
Operator	Reserves this digit for use as the extension used to access the Mitel operator. The default value is zero (0). In international applications, zero is often used as the access code for trunks. This sets a potential for conflict. Mitel recommends that international customers standardize globally on a single trunk access code for the purposes of network call routing (for example, use “9” for all trunk groups).
Extension Prefix (n Digit)	Lets you specify the number of digits used in extension prefixes that have this leading digit. Extension prefixes can be up to seven digits. The Configure Extension Prefix Warning section appears with a list of each of the sites in your system. Next to the list of sites you will find a blank field that requires you to enter the desired extension prefix. This prefix will be appended to every dialed number at that particular site. Make sure to back up the system before clicking **Save**.

5.1.2 Increasing the Extension Length

You can increase the number of digits for phone extensions from the three-digit default to up to seven digits. When you increase the number of extension digits, to match the new number you must also add one or more numbers to the beginning of extensions for existing numbers, including mailboxes, menus, and distribution lists. Be sure that the added number or numbers do not conflict with other access codes in the system’s dial plan.

You can change the parameters listed in Dial Plan Page: Extension Length Tab:

Note:
You cannot reduce the number of digits included in an extension after setting this parameter.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Dialing Plan** > **Dial Plan**, and then click the **Extension Length** tab. The **Extension Length** tab is displayed.
3. In the drop-down list for the **New extension length** field, select a value for the new extension length.

   A confirmation dialog is displayed.
4. Click **OK** to increase the extension length.
5. If you want to add one or more numbers at the beginning of all extensions in the MiVoice Connect system, enter this number or these numbers in the **Pre-pend current extensions with number(s)** field.

Note:
Ensure the numbers that you pre-pend to the extension do not conflict with other numeric strings in the dial plan. For example, the pre-pended numbers should not conflict with trunk access codes, the operator extension, emergency numbers, and so on.

6. After completing all changes to the dial plan, click **Save**.

Table 7: Dial Plan Page: Extension Length Tab

Option	Description
Current	
Number of extension digits	Shows the number of digits currently used in Mitel extensions. The default is 3 digits.
New	
Increase extension length (irreversible)	Allows you to increase the number of digits that cannot be reversed.

Option	Description
New extension length	Allows you to increase the number of digits used in Mitel extensions up to 7 digits.
Pre-pend current extensions with number(s)	Allows you to specify the number or numbers to appear at the beginning of extensions.

5.2 Configuring Digit Translation Tables

This section provides an overview of digit translation tables and describes how to create and delete them.

A digit translation table is a remedial solution for an environment with overlapping or conflicting dial plans on different (but connected) phone systems. A digit translation table resolves differences in the numbers of digits in the dial plans.

A digit translation table converts numbers between either of the following:

- The dial plan of a non-Mitel system and the dial plan of a MiVoice Connect system
- Different dial plans on separate Mitel networks

Through the digit translation table, you can adjust the extension format of a MiVoice Connect dial plan to the format of the dial plan in another phone system. You can specify:

- The number of digits
- The lead digit for numbers in each system

Note:
The use of a digit translation table requires careful planning. For guidance on how to plan for digit translation tables, refer to the *MiVoice Connect Planning and Installation Guide*.

After a digit translation table exists, it is applied (as needed) to application servers, trunks, and SIP trunks. Details are provided in the following chapters:

- Configuring Application Servers on page 118 explains how to apply translation tables to servers.
- Configuring Trunk Groups on page 219 explains how to apply translation tables to ISDN trunk groups.

- Digit Translation Across SIP Trunks on page 679 explains how to apply translation tables to SIP trunk groups.

When the MiVoice Connect system applies a digit translation table, the direction of the routed call determines whether digits are added or deleted.

When resolving possible differences between dial plans, the system administrator should specify number translation so that its operation is invisible to users. Methods for achieving smooth operation for dial plans are described in the *MiVoice Connect Planning and Installation Guide*.

In general, a system translates the numbers of digits when it passes calls to another phone system. However, the particular system that performs the translation is the choice of the system administrator. One of multiple MiVoice Connect systems or the system from another manufacturer can perform the translation. The decision can be based on which system provides the most convenient or efficient point of translation.

You can associate the digit translation table with:

- A trunk that bridges systems
- The Simplified Message Desk Interface (SMDI) module in an application server so that users can access legacy voice mailboxes

In either case, users do not have to change their dialing habits.

When SMDI is selected as the voice mail interface, translation table lists appear in profiles for trunk groups and application servers.

5.2.1 Creating Digit Translation Tables

Note:
The maximum number of rows allowed when creating a digit translation table is 128. If you add more than 128 entries, an error occurs when you click **Save**.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Digit Translation Tables**. The **Digit Translation Tables** page is displayed.
3. Click **New**.

Note:

The **General** tab is displayed. For details about the parameters on the General tab, see Digit Translation Tables: General Tab.

4. In the **Name** field, type a name for this digit translation profile.
5. In the **Original** field, enter the string to translate.
6. In the **Replacement** field, enter the replacement string.
7. To add more rows to the digit translation table, click **Add**. (The maximum number of rows allowed is 128).
8. To remove a row, click **Remove** next to the row you want to remove.
9. When you are finished making changes, click **Save**.

Table 8: Digit Translation Tables: General Tab

Parameter	Description
Name	Specify the name of the digit translation table
Add	Click **Add** to add a row to the current digit translation table
Original	Specify the digit that you want to replace with a new digit
Replacement	Specify the new digit that should replace the original digit
Remove	Click **Remove** to remove a row of the digit translation table

5.2.2 Deleting Digit Translation Tables

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Digit Translation Tables**. The **Digit Translation Tables** page is displayed.
3. Select the check box next to the digit translation table you want to delete.

4. Click **Delete**.

   A confirmation dialog is displayed.
5. Click **OK** to delete the digit translation table.

5.3 Configuring System Extensions

Services such as voice mail, account codes, auto-attendant, music on hold, Make Me conferences, and Mitel conferences associated with the Headquarters site have system-wide application. These services, when enabled on the Headquarters site, are each automatically assigned an extension on the Headquarters server. Each extension can be used by any user anywhere on the system to access the service, though the service may be executed at the server site that is local for the user.

You can view and modify extensions assigned to these system-wide services using the System Extensions page. Parameters on the System Extensions Page describes the parameters on the System Extensions page.

5.3.1 Viewing System Extensions

1. Launch Connect Director.
2. In the navigation pane, click **Administrator** > **System** > **Dialing Plan** > **System Extensions**.

Note:
The **System Extensions** page displays the system extensions currently configured.

5.3.2 Modifying System Extensions

Note:
After modifying system extensions, a TMS restart is required on all servers in order for the changes to take effect. Perform the TMS restart during off hours as it may drop calls in the system. A system restart is not required.

1. Launch Connect Director.

2. In the navigation pane, click **Administrator** > **System** > **Dialing Plan** > **System Extensions**. The **System Extensions** page appears.
3. Enter or edit extensions for your system. (For details about the parameters on the System Extensions page, see Parameters on the System Extensions Page).
4. Click **Save**.
5. Perform a TMS restart on all servers during off hours. A system restart is not required.

Table 9: Parameters on the System Extensions Page

Field	Description
Voice mail	
Extension	The extension the system uses for forwarding calls to voice mail.
Show References	Click to display a list of everywhere this extension is used.
Login extension	The extension that users use to log into their voice mailbox. Mitel recommends that users be allowed to dial in from outside the company to retrieve voice mail. Typically, you direct this number to an auto-attendant menu and configure the menu with a single-digit action of “Go to Menu” using the Voice mail **Login extension** parameter.
Show References	Click to display a list of everywhere this extension is used.
Broadcast mailbox	The extension users use to broadcast a voice mail message to all users.
Account codes	
Extension	The extension on the Headquarters SoftSwitch associated with the account codes application. When account code collection is optional or forced, calls are routed to this extension for an account code prompt. For more information, see Configuring Account Codes on page 352.

Field	Description
Music On Hold	
Extension	The extension for system-wide file-based music on hold. This extension is created during system installation.
Auto-attendant	
Extension	The extension for the system-wide auto-attendant.
Show References	Click to display a list of everywhere this extension is used.
Backup extension	The extension you want to use as an auto-attendant backup in case the Headquarters server fails. The backup auto-attendant (BAA) provides basic inbound call routing in case the auto-attendant on the server is unavailable. In addition, it answers calls routed to voice mail in case voice mail on the server is unavailable. The BAA is also used when extensions are unreachable during a network or switch outage and the Admissions Control Bandwidth is exceeded. Callers who access the MiVoice Connect system over a SIP trunk can access the BAA in the same manner as users who access the system via all other trunk types. Mitel supports RFC2833 (DTMF), so if the voice-mail server is down, external callers can enter an extension by using DTMF to ring the extension of the user they are trying to reach.
Make Me conference	
Extension	This extension lets users create conferences with up to eight participants on a voice switch if the conference capability is so configured. The default is three.
Conference	

Field	Description
Extension	The system-wide extension internal users dial to initiate a conference enabled by a Service Appliance.
Show References	Click to display a list of everywhere this extension is used.
External number	The main external telephone number users dial to access a conference enabled by a Service Appliance.
Additional calling information	Allows you to specify other external telephone numbers users can use to access conferences enabled by a Service Appliance. These numbers can be local to remote sites. The D2 administrator should format the text in the “Additional calling information” field so that the information appears in the suitable format in the email invitation.

5.4 Enabling SNMP

Mitel voice switches support Simple Network Management Protocol (SNMP) agents for the Ethernet interface. These agents provide Management Information Base II (MIB-II) statistics and allow voice switches to be integrated into standard network management applications. Details about the SNMP parameters you can configure in Connect Director are described in Fields on the SNMP Page.

Mitel has tested and supports the HP OpenCall network management console.

Mitel recommends that you configure your SNMP management station to launch Connect Director automatically when you click a Mitel device.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **SNMP**. The **SNMP** page opens.
3. Enter or edit values for the fields on the **SNMP** page, as described in Fields on the SNMP Page.
4. Click **Save**.

Table 10: Fields on the SNMP Page

Field	Description
Community strings	
Read-Only (Get)	Do not enter any values in these fields.
Read/Write (Get/Set)	**Note**: Mitel devices do not support active scans such as SNMP GET request. Mitel hardware or software does not respond to an active SNMP GET request so as to avoid impact on the voice solution. However, Mitel supports SNMP traps that allow the switches to communicate with the monitoring solution for network monitoring.
IP address of trap receivers: One Two Three Four Five	The IP address of up to five destinations that should receive SNMP traps. The destination IP address must have an installed SNMP trap listener (on UDP Port 162).

5.5 Configuring Other System Parameters

You can configure a variety of system-wide parameters on the Additional Parameters page. Fields on the Additional Parameters Page describes these parameters.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Additional Parameters**. The **Additional Parameters** page opens.
3. Enter or edit values for the fields on the **Additional Parameters** page, as described in Fields on the Additional Parameters Page.
4. Click **Save**.

Table 11: Fields on the Additional Parameters Page

Field	Description
General	
Upload location for logs	Specify an FTP or HTTPS server for Device Log Upload. Devices support log upload using FTP or HTTPS only. • The allowed format for the FTP server is: `ftp://ftp_server_ip -or- ftp_server_ip -or-ftp://ftp_server_FQDN`. • The allowed format for the HTTPS server is: `https://HQ_server_ip or https://HQ_server_fqdn`. **Note**: • For HTTPS option, the log upload location is supported only with the HQ server. • For FQDN-based certificates, provide the HQ FQDN in the **Upload location for logs** field. • Log upload to LDVS server is not supported. • For teleworker phones, only the HTTPS option is support for log uploads.

Field	Description

Upload location for logs (Continued)	Following are the conditions that apply for upload location for logs for the phones:
	• For teleworker phones:
	  • If the upload location for logs is set to either `https://server_ip` or `https://fqdn`, then the default upload location for logs will be used.
	  • If the upload location for logs is set to FTP or server IP address, then the upload location for logs will be `https://HQ_server_ip`.
	• For non-teleworker phones, if the upload location for logs is left blank and:
	  • If the **Enable FTP anonymous server** option is enabled, then the upload location for logs will be `ftp://HQ_server_ip`.
	  • If the **Enable FTP anonymous server** option is disabled, then the upload location for logs will be `https://HQ_server_ip`.
	• For non-teleworker phones, if the upload location for logs is set to server IP address and:
	  • If the server IP address is not managed by MiVoice Connect or if the **Enable FTP anonymous server** option is enabled, then the upload location for logs will be `ftp://server_ip`.
	  • If the **Enable FTP anonymous server** option is disabled, then the upload location for logs will be `https://HQ_server_ip`.

Field	Description

Upload location for logs (Continued)	• For non-teleworker phones, if the upload location for logs is either `https://server_ip` or `https://fqdn`, then the default upload location for logs will be used.
	• For non-teleworker phones, if the upload location for logs is either `ftp://server_ip` or `ftp:/fqdn` and:
	  • If the server IP address or FQDN is not managed by MiVoice Connect or if the **Enable FTP anonymous server** option is enabled, then the default upload location for logs will be used.
	  • If the **Enable FTP anonymous server** option is disabled, then the upload location for logs will be `https://HQ_server_ip`.
	
	Note:
	• The FTP path is `C:\inetpub\ftproot`.
	• The HTTPS path is `C:\inetpub\ftproot\uploads\phone`.

Min client/admin password length	The minimum number of characters for the password that a user enters to log into the Connect client or Connect Director. Valid values are 4–26.
Max client/admin password length	The maximum number of characters for the password that a user enters to log into the Connect client or Connect Director. Valid values are 4–26.
Phone help button destination	If you want the IP480, IP480g, or IP485g phones to include a Help soft key that is configured to dial an internal support or Help Desk group, specify the destination number, which must be a valid dial string, including a trunk access code and country code if needed.

Field	Description
Enable TLS1.0 and TLS 1.1	This option allows you to enable/disable TLS 1.0 and TLS 1.1 in all MiVoice Connect components including HQ server, appliances, and other DVS servers (the exception is SG switches, which do not support TLS1.2). **Note**: • When you enable/disable the **Enable TLS1.0 and TLS 1.1** option, all the switches and appliances will restart. The restart takes 2 to 4 minutes. • If the MiVoice Connect system comprises SG voice switches, ensure that the **Enable TLS1.0 and TLS 1.1** option is enabled. • Even if you disable the **Enable TLS1.0 and TLS 1.1** option in Connect Director, the MiVoice Connect HQ server, though it prefers TLS 1.2, allows both TLS 1.0 and TLS 1.1. To enforce TLS1.2 on all clients and terminate any TLS 1.0 and TLS 1.1 requests from client, set the following registry entries value to **1**: • `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]"DisabledByDefault"=1` • `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.1\Server]"DisabledByDefault"=1` • After the MiVoice Connect system is upgraded, these manual settings will revert. You must manually enforce TLS1.2 as mentioned here.

Field	Description
Enable FTP anonymous server	This option allows you to enable/disable anonymous FTP on the MiVoice Connect server. If you disable this option, you must use HTTPS for file operations. **Note**: • This option is enabled by default. • If you are using the FTP boot feature for the switches, then you must enable the **Enable FTP anonymous server** option. • If MGCP phones are used in the system, you must not disable the **Enable FTP anonymous server** option. This is because MGCP phones require FTP during bootup to download files from the HQ server and will not register if the **Enable FTP anonymous server** option is disabled. • You must enable the **Enable FTP anonymous server** option during the MiVoice Connect version upgrade. After all the appliances and devices are upgraded successfully, the administrator can decide whether to keep this option enabled or to disable it. • If the MiVoice Connect system comprises SG voice switches, ensure that the **Enable FTP anonymous server** option is enabled. • Ensure that **Enable FTP anonymous server** option is enabled while using `Record2File2`.
HQ / DVS log file storage	
Max days	The number of days that the headquarters server keeps a log file entry for a server event before deleting it. Valid values are 1–30.
Max size	The maximum megabytes in the server's log file. Valid values are 10–250000 MB.

Field	Description
Voice mail log file storage	
Max days	The number of days that the server keeps a voice mail log file entry on the Headquarters server for a voice switch before deleting it. Valid values are 1-30.
Max size	The maximum number of megabytes in a voice mail log file on the Headquarters server for a voice switch. Valid values are 10-500 MB.
Service Appliance (Collaboration)	
Service appliance Exchange server	The fully-qualified domain name (FQDN) or IP address of the Microsoft Exchange server to which a service appliance connects for Exchange synchronization. If you install a certificate from a public Certificate Authority, to avoid warnings in the Connect client you must specify the FQDN that matches the Common Name of the certificate. In this case, do not specify the IP address of the server in this field.
Log file storage	
Max days	The number of days that the Headquarters server keeps an entry in the log files for service appliances. Valid values are 1-30.
Max Size	The maximum size in megabytes for the log file of a service appliance. Valid values are 10-60000.
Conferencing	

Field	Description
Global conferencing URL	The optional system-wide conferencing URL, which corresponds to an FQDN designated for the first service appliance installed in the system. Users who enter this global conferencing URL are automatically redirected to the preferred service appliance, if one is designated. For example, if you assign an FQDN of “conference.acme.com” to the first service appliance you install, specify that FQDN in this field.
Instant messaging	
Domain name	The domain name for instant messaging, for example, greatcompany.com.
Session timeout	The number of minutes the system lets an instant message stay open without a response from the recipient. Valid values are 10-600.
Enable offline messaging	Select this check box to store messages for users who are off-line. Users can see these IM messages when they go on-line. If this option is not enabled, the system drops instant messages sent to users who are off-line.
Enable TLS for IM	Select this check box to allow encryption through transport layer security (TLS).

Field	Description
Client history retention period	The number of days worth of instant messages that will be saved for users to be able to retrieve in the Connect client. Valid values are 3-549 days. The default value is 249 days. **Note**: If you set high values for the retention period and the number of chats for this period, there will be a delay in loading IM messages after you start Connect client because of large amount of data being loaded.
Client compatibility and upgrade	
Require secure client access (https)	Select this check box if you want secure connectivity for the Connect client and Connect Director. If this setting is enabled, certificates are required for the system. For more information about certificates, see Certificates on page 81.
Suppress client upgrade notifications	Select this check box to prevent client upgrade notifications. We recommend enabling this parameter when you use the Silent Client Upgrade feature in connection with Active Directory to install client software on remote machines.
Minimum allowed client version	The earliest version number of the Connect client available to users. **If Suppress client upgrade notifications** is not enabled, users receive a notice when the Connect client needs to be upgraded. The default value is the earliest version of the Connect client that the system software accepts.

Field	Description
Current version for the build	The most recent version number of the Connect client for users. **If Suppress client upgrade notifications** is not enabled, users receive a notice when the Connect client software is out of date, but the value of this parameter does not force a software upgrade.
Active directory (AD) integration	
Enable AD integration (changing AD integration flag will impact all AD users)	Select this check box to enable the system to use Active Directory for authentication.
AD path	Enter the path that the system uses for Active Directory. **Note**: The AD path must be as follows: **LDAP:// DomainNm:port/ou=US,dc=company,dc=com**. If the specified port number does not exist, the LDAP request will direct you to port 389. For secure LDAPs, use port 636.
Gmail configuration	
Client Email	Enter the OAuth client email provided in the file that was downloaded when you created the service account. See Voice Mail Synchronization with Gmail for Business on page 604 for more information.
Private Key	Enter the private key provided in the file that was downloaded when you created the service account.
Domain Name	Enter the premier or educational Gmail account domain name.

Field	Description
Configure user email structure	
Pick first part	From the drop-down list, pick the first part of the email address.
Spacer	Type the character, if any, that you want to use to separate the first and last parts of the user name in email addresses. Examples are a period (.), underscore (_), hyphen, or any other character.
Pick last part	From the drop-down list, pick the last part of the user name email address.
Example	Displays a preview of the email structure that reflects the format selections you specified in the previous fields.
Client third party integration	
Enable LinkedIn	Select this checkbox to enable LinkedIn as client third-party integration.
Enable Dropbox	Select this checkbox to enable Dropbox as client third-party integration.

You can also configure system-wide file-based music on hold. Following are the steps to do this:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Music On Hold** > **System Defaults**. The **System Defaults** page opens.
3. Enter or edit values for the fields on the **System Defaults** page, as described in the following table.
4. Click **Save**.

Table 12: Fields in the System Defaults Page

Field	Description
Music on Hold System Defaults	

Field	Description
Internal calls	Select the default music on hold (MOH) source used for internal calls.
File based system default	Select the default MOH source.

5.6 Implementing Client Compatibility

The Client Compatibility feature provides greater control to organizations over which versions of the Connect client they deploy during a MiVoice Connect system upgrade. This feature is designed to reduce the impact of system upgrades. Because you can upgrade the servers first and then the clients later, you can spread the upgrade over time, which is less demanding for the IT staff and allows users to upgrade at their own convenience.

The Client Compatibility feature lets you specify the earliest version of the Connect client that the system supports and suggests an earliest version that clients can use without upgrading.

When a user's version of the Connect client falls below the minimum suggested version but is later than the minimum allowed version, the system sends an upgrade notification that lets the user upgrade immediately. A user who chooses to upgrade later must use the Upgrade function in the Connect client menu.

To implement client compatibility:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Additional Parameters**. The **Additional Parameters** page opens.
3. Scroll to the **Client compatibility and upgrade** section and do the following:

   - Select the **Require secure client access (https)** option if you want the Connect client to be accessed securely. Certificates are required if you select this option. For information about importing certificates, see Certificates on page 81.
   - Select the **Suppress client upgrade notifications** option to hide the client upgrade option in the Connect client. With this setting, users can upgrade only after they receive a notification.
   - In the **Minimum allowed client version** field, enter the number of the earliest version of the Connect client that users can use. The default value is the earliest client version the system software supports.
   - In the **Current version for the build** field, enter the current version of the Connect client that clients can use. Clients receive an upgrade message if the Connect client

version goes out of compliance. However, with this parameter, the system does not require a software upgrade. (If the **Suppress client upgrade notifications** option is selected, this parameter is disabled because users don't have permission to initiate upgrades).

Note:
The earliest and latest versions of the Connect client that the MiVoice Connect system software supports are displayed to the right of the field.

4. Click **Save**.

Client compatibility is configured for the Connect client.

5.7 Configuring Languages

A MiVoice Connect system can support more than one language at a time. To add one or more languages beyond the default (free) language of the customer's choice, the customer must buy a license for each additional language. For example, if two languages are enabled, then the customer buys one license. Furthermore, when a customer buys a keyed license for each additional language, up to 10 additional licenses can be associated with one key. For more than 10 additional language licenses, an additional key is needed.

5.7.1 Specifying Which Languages Are Available to the System

1. Launch Connect Director.
2. Click **Administration** > **System** > **Languages**.

Note:
The **Languages** page opens indicating the languages that are enabled languages with a check mark.

3. For each language that the MiVoice Connect system must support, select the check box in the **Enable** column.
4. Click **Save**.

Table 13: Languages Page

Column Name	Description
Enable	Select the check box to enable use of the language.
Name	The name of the language.
Locale	The abbreviation for the locale.
Used	Shows whether or not the language is used.

5.7.2 Supported Languages

The supported languages in the current release are as follows:

- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- Dutch
- English (Australia)
- English (UK)
- English (US)
- French
- French (Canada)
- German
- Hebrew
- Italian
- Japanese
- Korean
- Norwegian
- Portuguese (Brazil)
- Portuguese (Portugal)
- Spanish (CALA)
- Spanish (Spain)
- Swedish

Note:

The 6900-Series (6910, 6920, 6930, 6940, and 6970) phones, support the following languages:

- English
- French
- German
- Spanish

The functional areas for which a specific language can be configured are as follows:

- Sites
- Auto-Attendant Menus
- Users
- Workgroups
- Route Points
- Trunk Groups

5.8 Using Hybrid Services

If you are interested in using hybrid services, such as Connect HYBRID Scribe and Connect HYBRID Fax, see the articles about these topics on the Mitel Support website.

5.9 System Information

The System Information page displays various details about your system, such as directory paths and when the server was installed.

Setting Up Security Parameters 6

This chapter contains the following sections:

This chapter describes system-wide parameters for security in Connect Director.

6.1 Security Overview

MiVoice Connect provides the following methods for ensuring the security of the system and hardware:

- Administrative permissions
- Certificates
- Trusted server applications
- Password policy
- Other security-related parameters

The following sections provide more information about these security topics.

6.2 Administrative Permissions

Administrative permissions in Connect Director involve assigning roles that carry various permissions to individual users.

Roles are sets of permissions that enable users to perform various tasks in Connect Director. System administrators who have the Administrative permission management permission may grant one or more roles to users for various purposes. Users who have been granted permissions are called administrators. To log in to Connect Director, a user must have been assigned an administrative role with at least one permission.

The administrative permissions are described in Roles Page: General Tab, Roles Page: Users Tab, Roles Page: User Groups Tab, Roles Page: Distribution Lists Tab, Roles Page: Workgroups Tab, Roles Page: Sites Tab, Roles Page: Maintenance Tab.

The default roles and their permissions are shown in Default Roles and Their Default Administrative Permissions - Part 1 and Default Roles and Their Default Administrative Permissions - Part 2.

System administrators with the proper permission level can define new roles and assign these new roles or the default roles to users at one or more sites.

The initial administrator set up during installation has full permissions. Users assigned the Technical Support role have no permission to change parameters, but they are allowed to read all pages.

Permissions are additive; that is, the more selections, the greater the permissions. When defining a new role, you can select as many or as few permissions as are needed for that particular role. For example:

- In a company with one Mitel system administrator, that administrator would have all permissions.
- An administrative assistant may have permission to change Distribution Lists at one site.

Table 14: Roles Page: General Tab

Field	Description
Name	The name of the administrative role.
Administrative permission management	This permission allows the user to create new administrative roles and assign them to a user of any level. Because this is a powerful permission, it should be granted only to lead administrators.
Account code management	This permission allows the user to add, change, and delete Account Codes. This permission is granted for all sites. You might want to use this permission if a department other than Information Technology wants to manage account codes and needs no other permissions.
Report generation management	This permission allows the user to generate Call Detail Record (CDR) reports through Connect Director from a local host or a remote server.

Field	Description
System directory management	This permission allows the user to add, change, and delete entries in the System Directory. This permission is granted for all sites.
All other system management	This permission allows the user to set dialing plans, system-wide extensions (including route point and workgroup extensions), sites, IP phone options, digit translation tables, voice mail options, auto-attendant options and schedules, user groups, trunk groups, local prefixes, DNIS digit maps, classes of service, call control, system parameters such as password length, AMIS options, call-handling defaults, event filters, licenses, extension lists, hunt groups, paging groups, and contact information. This permission is granted for all sites.

Table 15: Roles Page: Users Tab

Field	Description
User management	Designate the level of permissions for user settings by selecting one of the following options: • To provide the fullest level of permissions for changing users, select **Add/delete/modify user**. • To provide a limited set of permissions that allows the user to modify settings for existing users, select **Modify user settings only**. The User management permission does not allow changes to a user's administrative role, because only the Administrative Permission Management permission gives administrators permission to change administrative roles.

Field	Description
Manage users on the following sites	The selected user management permission may be granted for no sites, all sites, or a set of selected sites by selecting one of the following options: • To deny permission to manage users, select **None**. • To grant permission for the selected level of user management system-wide, select **All sites**. • To limit the selected level of user management to specific sites, select **Selected sites**, and then in the Available list highlight the sites to include and click  to move them to the Selected list.

Table 16: Roles Page: User Groups Tab

Field	Description
User group and license type assignment	This permission allows the user to add users to or move users between user groups; it can be granted for all sites or for a set of selected sites. Select one of the following options. • To grant permission system wide, click **All user groups**. Selecting this option applies to all current user groups as well as those created after permission is first granted. • To grant permission to manage only specific user groups, click **Selected user groups**, and then in the Available list highlight the user groups to include and click  to move them to the Selected list. • To deny permission to manage user groups, select **None**. Permission is not extended to adding, changing, or deleting User Group options and Class of Service settings. (To make these changes, an administrator needs the **All other system management** permission.)

Table 17: Roles Page: Distribution Lists Tab

Field	Description
Distribution list membership management	This permission allows the user to add or remove users in existing distribution lists. Select one of the following options: • To grant permission to manage distribution lists system wide, click **All distribution lists**. • To grant permission to manage only specific distribution lists, click **Selected distribution lists**, and then in the Available list highlight the distribution lists to include and click  to move them to the Selected list. • To deny permission to manage distribution lists, select **None**. Note that this permission does not include the capability to create or delete distribution lists. (To make these changes, an administrator needs the **All other system managemen**t permission.)

Table 18: Roles Page: Workgroups Tab

Field	Description
Basic workgroup management	This permission allows the user to add or change options for workgroups. Select one of the following options: • To grant permission to manage workgroups system wide, click **All workgroups**. Selecting this option applies to options for all current workgroups as well as workgroups created after permission is granted. • To grant permission to manage workgroup options for only specific workgroups, click **Selected workgroups**, and then in the Available list highlight the workgroups to include and click  to move them to the Selected list. • To deny permission to change workgroup options, select **None**. Workgroup attributes that cannot be changed with this permission include Workgroup Name, Extension, Backup Extension, DID, DNIS, User Group, Mailbox, Accept Broadcast Messages, Include in Dial By Name, and Make Number Private. (To make these changes, an administrator needs the **All other system management** permission.)

Table 19: Roles Page: Sites Tab

Field	Description
Site (switches, trunks, IP phones, servers) management	This permission allows the user to add and alter sites and their related switches, trunks, IP phones, and servers. This permission includes adding and deleting anonymous phones at permitted sites. Select one of the following options: • To grant permission to make changes at all sites in the system, click **All sites**. • To grant permission to make changes only at particular sites, click **Selected sites**, and then in the Available list highlight the sites to include and click  to move them to the Selected list. • To deny permission to change sites, click **None**. Trunk groups are excluded from this permission. (To make trunk group changes, an administrator needs the **All other system management** permission.).

Table 20: Roles Page: Maintenance Tab

Field	Description

Allow execution of system-wide Maintenance and Diagnostics commands	Select any of the following options:
	• **Core system and server components** includes all commands available on the following pages:
	  • **Maintenance** > **Status and Maintenance** > **System** page
	  • **Maintenance** > **Status and Maintenance** > **Servers** page (start or stop application services)
	  • **Maintenance** > **Status and Maintenance** > **Trunk Groups** page
	  • **Maintenance** > **Status and Maintenance** > **IM** page
	• **Maintenance and Diagnostics configuration settings** includes all commands available on the pages under **Maintenance** > **Configuration**. In addition, settings related to event filters are included.
	• **Diagnostics** includes all commands available on the pages under the Diagnostics menu of Connect Director.
	• **Clear alerts** includes all commands available on the **Maintenance** > **Alerts** page.

Site and Appliance Status and Maintenance commands	Use one of the following options to specify whether this role can apply maintenance commands for sites and appliances. This includes all commands available on the **Status and Maintenance** > **Sites** page and on the **Status and Maintenance** > **Appliances** page. • To deny permission to execute maintenance commands at any site, select **None**. • To grant permission to execute maintenance commands at all sites, select **All sites**. • To limit permission to execute maintenance commands to specific sites, select **Selected sites**, and then in the Available list highlight the sites to include and click › to move them to the Selected list.

Field	Description
IP Phone Status and Maintenance commands	Use one of the following options to specify whether this role can apply maintenance commands for IP phones. This includes all commands available on the Status and Maintenance > Phones page. • To deny permission to execute maintenance commands on phones at any site, select **None**. • To grant permission to execute maintenance commands on phones at all sites, select **All sites**. • To limit permission to execute maintenance commands on phones at specific sites, select **Selected sites**, and then in the Available list highlight the sites to include and click › to move them to the Selected list.
Allow execution of Site, Appliance and IP Phone commands on the following sites:	
Available	Displays the available list of Site, Appliance, and IP Phone commands at specific a site.
Selected	Displays the selected list of Site, Appliance, and IP Phone commands at a specific site.

Table 21: Default Roles and Their Default Administrative Permissions - Part 1

Name	Administrative Permission	Account Code	System Directory	Report Generation	Other System
Accounts and Directories		Yes	Yes		
Call Center		Yes	Yes		
Everything Except Roles		Yes	Yes	Yes	Yes
HQ Site					
Maintenance					
Reporting				Yes	

Name	Administ rative P ermission	Account Code	System D irectory	Report G eneration	Other Sy stem
System Administrator	Yes	Yes	Yes	Yes	Yes
Technical Support					

Table 22: Default Roles and Their Default Administrative Permissions - Part 2

Name	User	User Gro up	Distribu tion List	Work group	Site	Maintena nce
Accounts and Directories	All	All	All	None	None	
Call Center	None	None	None	All	None	
Everything Except Roles	All	All	All	All	All	
HQ Site	Selected	None	None	None	Selected	
Maintenance	None	None	None	None	None	All
Reporting	None	None	None	None	None	
System Administrator	All	All	All	All	All	
Technical Support	None	None	None	None	None	

6.2.1 Configuring Roles

The Roles page shows the default and added roles available in the system. You can add, edit, copy, or delete roles on this page.

6.2.1.1 Adding a Role

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Administrative Permissions** > **Roles**. The **Roles** page is displayed.
3. Click **New**.

   The **General** tab is displayed.
4. In the **Name** field, type a name for the new role.
5. Select the check boxes or radio buttons for the permissions you want to include.
6. Click **Save**.

6.2.1.2 Editing a Role

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Administrative Permissions** > **Roles**. The **Roles** page is displayed.
3. Click the name of the role that you want to edit.

> **Note**:
> The details for that role are displayed on the **General** tab.

4. If you want to change the role's name, in the **Name** field type a new name for the role.
5. Modify other parameters on the **General** tab as needed to indicate the permissions you want to include for the role.
6. Click **Save**.

6.2.1.3 Deleting a Role

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Administrative Permissions** > **Roles**. The **Roles** page is displayed.
3. Click the name of the role that you want to delete.

> **Note**:
> The details for that role are displayed on the **General** tab.

4. Click **Delete**.
5. In the confirmation dialog, click **OK**. The role is deleted.

> **Note**:
> If the last role with the Administrative Permission Management permission enabled is removed, the default **admin** account (as created during initial installation) is reactivated and includes the full set of administrative permissions.

6.2.2 Configuring Administrators

The Administrator List page shows users who have been assigned a role with administrative permissions of some kind. A user may have only one administrative role. New users are created with no administrative role assigned to them.

At least one user must remain on the list to prevent the problem of no one being left to administer the system.

6.2.2.1 Adding an Administrator

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Administrative Permissions** > **Administrators**. The **Administrators** page opens.
3. Click **New**. The **General** tab is displayed.
4. In the **User extension** field, type the extension for the user to whom you want to assign as an administrator.
5. In the **Role** drop-down list, select the role you want to assign to the user.
6. Click **Save**.

6.2.2.2 Deleting an Administrator

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Administrative Permissions** > **Administrators**. The **Administrators** page opens.
3. Click the name of the administrator that you want to delete.

Note:
The details for that role are displayed on the **General** tab.

4. Click **Delete**.
5. In the confirmation dialog, click **OK**. The administrator is deleted.

6.2.3 Monitoring User Logins

A list of all users who are logged in to Connect Director is displayed in the list pane on the **User Logins** page. This information can be helpful if you notice slower performance when using Connect Director. As an administrator, you can log out any users who have been logged in for some period of time but who haven't actually looked at Connect Director recently. Details about the fields on the **User Logins** page are shown in User Logins Page: List Pane.

To log off a user:

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Administrative Permissions** > **User Logins**. The **User Logins** page opens.
3. Click the name of the user that you want to log off.

Note:
The details for that role are displayed on the **General** tab. For details, see User Logins Page: General Tab

4. Click **Delete**.
5. In the confirmation dialog, click **OK**. The user is logged off from Connect Director.

Table 23: User Logins Page: List Pane

Field	Description
Login Name	Displays the user name of the logged in user.
Login Time	Displays the amount of time that has passed since the user logged in to Connect Director.

Field	Description
Last Seen	Displays the amount of time since the logged-in user has looked at Connect Director.

Table 24: User Logins Page: General Tab

Field	Description
Login Name	Displays the user name of the logged in user.
Login Time	Displays the amount of time that has passed since the user logged in to Connect Director.
Last Seen	Displays the amount of time since the logged-in user has looked at Connect Director.
Session ID	Displays the session ID for the logged-in user's session in Connect Director.

6.3 Certificates

This section covers the following topics:

6.3.1 Conceptual Overview of Public Key Infrastructure Certificates

To ensure data integrity, Mitel relies on the X.509 standard for public key infrastructure (PKI). To understand PKI, you need to know the following terms:

- Certificate Authority (CA) – An entity that issues X.509 certificates. Public certificate authorities that are well known and trusted are included in the trust store of most

operating systems and browsers. To ensure secure transactions, these public CAs must be used to issue certificates for Transport Layer Security (TLS) services that will be accessed by browsers or other third-party software and devices.

- Certificate – A digital certificate issued by a certificate authority for a particular FQDN. If you specify a wild card in the certificate signing request, the certificate can apply to more than one server (for example, *.shoretel.com). Another type of certificate, the Subject Alternative Name certificate, can support multiple domain names.
- Trust Store (sometimes referred to as a CA bundle) – A collection of CA certificates that is used when making a TLS connection.
- Root CA Certificate – A CA certificate that is self-signed. Well known Certificate Authorities (for example, VeriSign, GoDaddy, and GeoTrust) have their Root CA certificates in the trust store for operating systems and browsers, or they can be downloaded from the Web.
- Intermediate CA Certificate – A CA certificate signed by another (often Root) CA. Intermediate CA certificates are not commonly part of the trust store shipped with operating systems and browsers.
- Public key – a cryptographic key available to all parties in a group (for example, Mitel customers). A public key is typically embedded in a certificate.
- Private key – a cryptographic key available only to the owner. The private key is not to be shared and is only to be used by the owner.

Certificate Authorities are the foundation for PKI, because the digital certificates they create provide authentication for transactions. The CA is the party that both the owner of the certificate and the party using the certificate trusts. You can purchase a certificate from a widely known Certificate Authority vendor, which provides certificates for multiple organizations and the general public.

To ensure the integrity of transactions, digital certificates can be used to prove the identities of both machines involved in the transaction. If the certificate was issued by a source that the server knows and trusts, then the server will accept the machine's certificate as proof of its identity. In this way, a secure session can be established because the two machines are able to present each other with certificates.

For more information, see *RFC 2459 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile)*. You can also find numerous explanations of PKI certificates by doing an Internet search.

You might find the XCA tool for managing certificates helpful when working with certificates. You can access it here: http://sourceforge.net/projects/xca/

6.3.2 MiVoice Connect's Implementation of PKI

Upon start up, each server and appliance creates a Mitel self-signed certificate. The details about how MiVoice Connect implements PKI are as follows:

- **HW Root CA:** Mitel maintains a CA for the purposes of manufacturing hardware with built-in certificates. The 400-Series IP phones and 6900-Series (6910, 6920, 6930, and 6940) phones contain a unique certificate signed by this CA and also an encrypted private key. The Headquarters server stores the certificate in the file system and in the database.
- UC Certificate Authority (also known as the HQ CA): The Headquarters server functions as a X.509 Certificate Authority for the system's PKI. Each Mitel MiVoice Connect Headquarters server creates its own root CA certificate for internal use. The MiVoice Connect server software installation process generates its own signed Certificate Authority certificate when it first boots up. This root certificate uses a 2048-bit RSA key-pair and is valid for 20 years.The Certificate Authority on the Connect Headquarters server issues certificates for Secure Session Initiation Protocol (SIPS) and HTTPS that are used in Transport Layer Security. Every server has a certificate for HTTPS, and every switch has a certificate for SIPS.

  The UC Certificate Authority root CA is uniquely generated for every installation. The ability to replace this CA with an alternate is not supported.
- **Service Appliances:** To provide HTTPS security to conference users, you must upload certificates to each service appliance for which you want to provide secure access. The service appliances include an administrative interface, accessible from Connect Director, that allows you to create and export a certificate signing request and import a certificate, along with any intermediate CA. Optionally, you can also import a private key if the certificate was not generated from the CSR. When the CSR is created, a self-signed certificate is created. If a wild-card certificate is installed, you can propagate the certificate and keys to all service appliances in the system. For more information on certificates for service appliances, see the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide*.
- **Mobility Router (SMR) CA:**The SMR creates its own CA for issuing client certificates to devices after they have authenticated with username and password. The SMR also uses this CA to create initial HTTPS server certificates, but these can be replaced by certificates from a Public Certificate Authority. For details about certificates for the Mobility Router, see the *MiVoice Connect Mobility Router Administration Guide*.
- **Edge Gateway CA:** The Edge Gateway creates its own self-signed certificates, which are used if no other certificates are installed. Because the Edge Gateway supports VPN access for IP400- Series phones (through RAST), it trusts the HW Root CA as a means to authenticate phones. For details about certificates for the Edge Gateway virtual appliance, see the *MiVoice Connect Edge Gateway Administration Guide*.

For MiVoice Connect, encryption is provided for all end-user communication, including all protocols to and from the IP400-series phones (with the exception of a few downloaded configuration files), and all protocols to and from the Connect client.

To ensure secure (HTTPS) access for Connect Director and the Connect client, you must enable the **Require secure client access (https)** option on the Additional Parameters page and install a custom certificate purchased from a public certificate vendor. This is the only method for ensuring that the Connect client and Connect Director are secure.

The Connect client falls back to HTTP if certificates are not installed to enable HTTPS. Connecting securely requires trusted certificates to be deployed on all platforms where the client connects. Furthermore, if you install a certificate from a public Certificate Authority and you enable the Exchange connector (on the Additional Parameters page in Connect Director), be sure that the FQDN that you specify in the Exchange server matches the FQDN included in the certificate. Otherwise, connecting to the client generates warning messages.

If ensuring secure client access is not a requirement, you can opt to use the default certificates signed by the UC Certificate Authority that are created during installation.

In the most typical Transport Layer Security (TLS) handshake, the server presents a certificate, possibly including one or more Intermediate CA certificates, and the client validates that certificate based on its trust store, which contains the appropriate Root CA. This is how the client authenticates the server. In this case, the server has not authenticated the client. In MiVoice Connect, client authentication through certificates applies to 400-Series IP phones and 6900-Series (6910, 6920, 6930, and 6940) phones and to Trusted Server Applications.

6.3.2.1 Security Pages in Connect Director

You must have the Administrative Permission to access the pages that pertain to certificates in Connect Director. These pages are accessible in the **System** > **Security** menu.

Connect Director includes a page that lets you generate a certificate signing request, which you can use to purchase a PKI certificate from a widely known and trusted certificate vendor. For instructions, see Generating a Certificate Signing Request on page 85.

For servers, including Windows and Linux distributed voice servers, you can upload and manage certificates for your MiVoice Connect system in Connect Director through the Certificates tab on the Platform Equipment page. For details, see Importing Certificates for Headquarters, Windows DVS, and Linux DVSs on page 87.

6.3.2.2 Back Up the Keystore Folder

All certificate files, including private and public keys, are stored in the following path:

```
<drive>:/Shoreline Data/keystore
```

Mitel recommends that you keep a backup copy of the `/keystore` folder in a secure offline location so that your certificates can be recovered in case of hardware failure.

Mitel recommends that you not delete the `/keystore` folder. If you delete this folder, you will need to reboot all voice switches and clear each phone's configuration by using MUTE CLEAR# on each phone.

6.3.3 Generating a Certificate Signing Request

Connect Director includes an interface you can use to generate a certificate signing request that you can send to a third-party Certificate Authority to purchase a certificate.

1. Launch Connect Director.
2. On the navigation pane, click **System** > **Security** > **Certificate Signing Request**. The **Generate Certificate Signing Request (CSR)** page opens.
3. To generate a CSR with a Subject Alternative Name for Trusted root certification, go to the **Add alternative common names if needed** field and enter the Subject Alternative Name in the **Alternative common name 1** field.
4. Complete all fields on the page, as described in Certificate Signing Request Page (Some fields are automatically populated with information from the Contact Information page. You can edit this information as necessary).
5. Click **Generate**.

> **Note**:
> The CSR is generated, and the Private key is also generated if the **Create a new private key** option was selected.

6. Create a staging folder (for example, `<drive>:\CertStaging`), and save the following text files there:
   - Copy and paste the generated CSR into a text file (for example, `server01.csr`), and save the file in the staging folder.
   - If generated, copy and paste the generated private key into a text file (for example, server01.key), and save the file in the staging folder. (Retain the private key for local use. Do not share it with the vendor. Later, when you import the certificate files that you receive from the CA vendor, you will include this private key file that you have retained locally).
7. Send the Certificate Signing Request file that you created to a Certificate Authority vendor to purchase a certificate.
8. When you receive the certificate files from the CA vendor, save them to the staging folder that you created in Step 5.
9. Proceed with the steps outlined in Importing Certificates for Headquarters, Windows DVS, and Linux DVSs on page 87.

Table 25: Certificate Signing Request Page

Parameter	Description
Server	The name of the server for which the certificate is being requested. Select a server from the drop-down list. You can select **None** if you want to generate a certificate signing request for a generic server.
Create a new private key	When you select a specific Mitel server in the Server field, by default this option is not enabled because you can use the existing private key on the server. If you select **None** in the **Server** field, this option is enabled by default.
Common name	Specify the name of the server for which you are requesting the certificate. You can specify a fully qualified domain name (FQDN) or a hostname. If you specify an FQDN in this field, it must match the actual FQDN name exactly. If you selected a specific server in the Server drop-down list, this field is automatically populated. If you create a CSR for a wildcard certificate (for example, *.shoretel.com), the domain name portion you specify in this field must match the actual domain name.
Add alternative common names if needed	Click **Add** if you want to specify additional server names to be included in the certificate signing request.
Organization	The full name of the company that is requesting the certificate.

Parameter	Description
Organizational unit	The department or branch of the company that is requesting the certificate.
City	The name of the city where the organization is located.
State	The full name of the state where the organization is located. This field is automatically populated with information from the Contact Information page. If a two-letter state postal abbreviation code was used there, it is displayed here. Change it to the full spelled-out name (for example, “California”).
Country	A two-letter abbreviation for the country where the certificate will be installed.

6.3.4 Importing Certificates for Headquarters, Windows DVS, and Linux DVSs

This process assumes that you have purchased a signed certificate from a trusted Certificate Authority vendor.

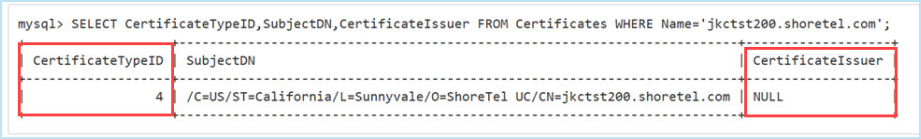
Note:
Because importing a certificate involves uploading multiple files, use a browser that supports selecting multiple files.

1. After purchasing a signed certificate from a CA vendor, store all the files received from the vendor, which should include the SSL certificate and the intermediate CA certificates, into a staging folder that you can access later for the upload. If a private key was created during the generation of the CSR, the private key must also be placed into the staging folder and imported later.

Note:

- Vendors could return certificate files in various formats and file types and might return a password along with the files. Not all file types returned from vendors can be imported as is. For example, a PKCS12 file can be imported as is, but a PKCS7 file cannot be imported without first running an OpenSSL command to extract individual certificates. These certificates then must be staged for import.
- If you are running Connect Contact Center, in addition to the Intermediate CA certificates, the Root CA certificate is required. If the Root CA certificate is not among the files returned from the vendor, you must download it, place it into the staging folder, and import it later.
- Before you import a certificate, you must verify that there is a current running ShoreTel self-signed certificate in the *Certificates* table in the Shoreware Database. For the ShoreTel self-signed certificate, the **CertificateIssuer** column will be **NULL** and the existing **CertificateTypeID** column will be **4**.

Figure 6: Certificate Verification



2. Launch Connect Director.
3. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
4. On the list pane, click the name of the device on which you want to install the certificate.

   The details for that device are displayed in the details pane.
5. Click the **Certificate** tab on the details pane.

   The **Certificates** tab is displayed, and it shows the details for the currently installed Mitel self-signed certificate or any previously imported certificate. The name (FQDN name) of the currently installed certificate should be identical to the Common name of the certificate that you are ready to import.
6. On the **Certificates** tab for the selected server, click **Delete Current Certificate**, and then click **OK** in the confirmation dialog.

Note:

Mitel does not recommend importing new certificates and changing a fully qualified domain name at the same time. If you would like to import a certificate that has a new FQDN, follow these steps on the Platform Equipment page in Connect Director after deleting the existing certificate:

a. On the **General** tab, change the value in the **Fully qualified domain name** field, and click **Save**.

Note:
This generates a self-signed certificate with the new FQDN.

b. Proceed with Step 7.

7. If provided by the vendor, in the **Certificate password** field enter the password for the certificate.

Note:
If your certificate has a password, you must enter the password before clicking the button to browse for the certificate files, which is described in the next step.

8. Upload the certificate and other relevant files from your system by clicking **Choose Files** or **Browse** in the **Certificate files** field and then selecting all the files provided by the Certificate Authority vendor. (These files include the SSL certificate and any intermediate CA certificates. There is typically one CA intermediate file, but there might be more than one.) In addition, include the private key if one was created when the certificate signing request was generated.

   Connect Director validates the uploaded files and confirms the validity with a check mark. After the import is complete, refresh your browser to see the new “Issuer” information.

Note:
If you do not include the proper intermediate CA certificates, the Directory, History, and Options features on the phones will not work.

9. Click **Save** to install the certificate on the server or appliance.

   The certificate you uploaded is installed for the selected device. The deployment of the imported certificates restarts some Windows services.

Note:

- If Connect Director cannot access the Root CA certificate, a warning message is displayed, but the import is still triggered by clicking **Save**.
- If the Appliance/Server is the HQ server, Connect Director restarts the *ShoreTel-WebFrameworkSvc* automatically to deploy the newly imported certificates.
- If the Appliance/Server is a Windows DVS, Connect Director restarts the *ShoreTel-WebFrameworkSvc* service remotely.
- If the Appliance/Server is a Linux DVS, Connect Director restarts the Connect Director Service remotely.
- The deployment of the imported certificates will take a few minutes.

6.3.5 Replacing an Imported Certificate with Self-Signed Certificate

1. Launch Connect Director.
2. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. On the **List** pane, click the name of the appliance or server for which you want to delete or revoke the existing certificate and replace it with a self-signed certificate.

   The details for that appliance or server are displayed in the **Details** pane.
4. Click the **Certificate** tab on the **Details** pane.

   The **Certificate** tab is displayed, and it shows the **Name** and **Domain** for the currently installed Mitel self-signed certificate or any previously imported certificate.
5. Click **Delete Current Certificate**.
6. In the confirmation dialog, click **OK**.
7. Optional: If you need to change the FQDN, click the **General** tab and provide the new FQDN in the **Fully qualified domain name** field.
8. Click **Save**.

6.3.6 Regenerating Certificates to Update Subject Alternative Name

When you update MiVoice Connect running on your system from an earlier version to the current version, (for example, from 19.1 to 19.2), the certificates are not automatically updated. Due to this, the Subject Alternative Name is not updated automatically. To resolve this issue, you must regenerate the certificate for self-signed certificates and third-party Certificate Authority.

To regenerate the certificate for self-signed certificates, follow these steps:

1. Launch Connect Director.
2. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
3. On the **List** pane, click the name of the appliance or server for which you want to delete or revoke the existing certificate and replace it with a self-signed certificate.

   The details for that appliance or server are displayed in the **Details** pane.
4. Click the **Certificate** tab on the **Details** pane.

   The **Certificate** tab is displayed. It shows the **Name** and **Domain** for the currently installed Mitel self-signed certificate or any previously imported certificate.
5. Click **Delete Current Certificate**.
6. In the confirmation dialog, click **OK**.
7. Click **Save** to regenerate the self-signed certificate.

Note:
After you delete the self-signed certificate and click **Save** to regenerate the self-signed certificate, wait for 5 minutes and check whether the certificate is generated. If not, restart the *ShoreTel-WebFrameworkSvc* service.

To regenerate the certificate for third-party Certificate Authority, follow these steps:

1. Generate a Certificate Signing Request. To generate a Certificate Signing Request, follow the instructions provided in Generating a Certificate Signing Request on page 85.
2. Import the certificate. To import the certificate, follow the instructions provided in Importing Certificates for Headquarters, Windows DVS, and Linux DVSs on page 87.

6.4 Configuring a Trusted Server Application

Through Connect Director, you can provide support for a trusted server for which you want to allow secure access to the Headquarters server such as the Mobility Router. Documentation for those components describes how to create the certificates that are uploaded through the **Trusted Server Application** page.

6.4.1 Viewing Trusted Server Applications

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Security** > **Trusted Server Application**.

> **Note**:
> The **Trusted Server Application** page is displayed. Details about the columns in the list pane are provided in Trusted Server Application Page: List Pane.

3. Click the name of a trusted account to see its details in the details pane.

Table 26: Trusted Server Application Page: List Pane

Column	Description
Trusted Account Name	The name you specify for the configured trusted server application.
Property Type	The property type associated with the trusted server.
Subject	Information about the certificate
Valid From	The first date the certificate is valid
Valid To	The date that the certificate expires
Enabled	Whether the specified truster server application is enabled

6.4.2 Creating a Trusted Server Application

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Security** > **Trusted Server Application**. The **Trusted Server Application** page is opens.
3. Click **New**.
4. On the **General** tab, specify the details for the trusted server account you want to create. For details, see Trusted Server Application Page: General Tab.

> **Note**:
> After you select a certificate, the **Subject, Valid from**, and **Valid to** fields are populated.

5. Click **Save**.

Table 27: Trusted Server Application Page: General Tab

Column	Description
Trusted account name	Specify the name of the trusted server application
Certificate	Click **Choose File** to browse for and select a certificate to upload to the Headquarters server.
Subject	Information about the certificate
Valid from	The beginning of the period for which the certificate is valid
Valid to	The end of the period for which the certificate is valid
Application type	The type of application you use to authenticate the server. Select **Client Application Service (CAS)** from the drop-down list.
Enable	Select this option to enable CAS.

Column	Description
Property Type	Select the property type to be associated with the trusted server. You can select from the following two options: • **admin-ro** This allows read-only access. • **admin-cas** This allows changes from the trusted server application to be made on the server.

6.5 Configuring the Password Policy

You can specify settings related to the password used for Connect Director.

1. Launch Connect Director.
2. In the navigation pane, click **System** > **Security** > **Password Policy**. The **Password Policy** page is displayed.
3. Specify the values for the parameters. (For details, see Password Policy Page).
4. Click **Save**.

Table 28: Password Policy Page

Parameter	Description
Minimum password strength	A number that reflects the complexity of the password based on an algorithm that factors in the following items: • password length • number of letters in the password • number of numbers in the password • number of special characters in the password • combined items from the items listed above Possible values range from 1-100, with 25 indicating a weak password and 90 a very secure password. The default is 66. The algorithm calculates points as follows: • **Password Length:** 5 Points: Less than 4 characters 10 Points: 5 to 7 characters 25 Points: 8 or more • **Letters:** 0 Points: No letters 10 Points: Letters are all lower case 20 Points: Letters are upper case and lower case

Parameter	Description
Minimum password strength (continued)	• **Numbers:** 0 Points: No numbers 10 Points: 1 number 20 Points: 3 or more numbers • **Special Characters:** 0 Points: No special characters 10 Points: 1 special character 25 Points: More than 1 special character • **Combined Items:** 2 Points: Letters and numbers 3 Points: Letters, numbers, and special characters 5 Points: Mixed case letters, numbers, and special characters
Reuse limit	The number of previous passwords that cannot be used. The range of possible values is 0-30. The default is 1.
Expiry days	The number of days before the password expires. The range of possible values is 10-365. The default is 90.
Number of failed attempts before lock-out	The number of times a user can provide the wrong password before being locked out. The range of possible values is 1-10. The default is 3.

Parameter	Description
Lock-out time	The amount of time in minutes that a user is locked out of logging back into the MiVoice Connect system after reaching the threshold number of failed attempts. (This lockout applies to any application or feature in MiVoice Connect that requires a password. Examples are Connect Director and the Connect client.) The range of possible values is 3-360. The default is 10.
Sync	Select this option to force a re-synch of bootstrapper d ata. Note that this will interfere with pending request so only do this when you know the system is not used.

6.6 Understanding Other Security-Related Parameters

This section describes three security-related configurations for a Mitel network:

- A port range that can be used for audio and video traffic throughout the network.
- Using trusted IP address ranges for service appliances (such as the SA-100 and SA-400) in the DMZ.

This section provides no guidance for choosing the IP address ranges to specify. This choice should have been made in advance, as a part of planning the network and formulating the network's security policy.

Note:
Unless Mitel's default port range conflicts with ports in the network, you can keep the defaults. Only the low-end port number is configurable, as this section describes.

6.6.1 Specifying the Port Range

Ports in the configured range are available to all Mitel applications and devices, such as voice switches, servers, IP phones, the Connect client, and Softphone.

When you specify the first port number, the system automatically adjusts the value of the last port to provide the maximum number of supported ports.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Port Configuration**. The **Port Configuration** page is displayed.
3. In the **First UDP port** field, enter a port number in the range of 1024–61034.

Note:
The value for the **Last UDP port** is automatically adjusted based on the value you entered.

4. Click **Save**.

6.6.2 Ranges of Trusted IP Addresses

Configuring trusted IP address ranges provides choices among the private IP address ranges. For this configuration task, specify one or more ranges of trusted IP addresses.

Note:
The default state of the private IP addresses includes the entirety of each range. Therefore, the IP ranges are completely open and insecure. After you specify a trusted IP address range, we strongly recommend that you delete the other ranges, as the configuration steps describe. If necessary, you can re-create these ranges.

6.6.2.1 Creating a Range of Trusted IP Addresses

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Trusted IP Ranges**. The **Trusted IP Ranges** page is displayed.
3. Click **New**. The **General** tab is displayed.
4. In the **Name** field, type a name for the trusted IP range.
5. In the **Low IP address** field, type an IP address for the low end.
6. In the **High IP address** field, type an IP address for the high end.
7. Click **Save**.

6.6.2.2 Deleting a Range of Trusted IP Addresses

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **System** > **Trusted IP Ranges**. The **Trusted IP Ranges** page is displayed.
3. Select the check box next to the name of the IP range you want to delete.
4. Click **Delete**. A confirmation dialog is displayed.
5. Click **OK** to delete the IP range.

6.6.2.3 Copying a Range of Trusted IP Addresses

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Trusted IP Ranges**. The **Trusted IP Ranges** page is displayed.
3. Select the check box next to the name of the IP range you want to copy.
4. Click **Copy**.

> **Note**:
> The **General** tab displays the details for the copied IP range.

5. Edit the details as necessary for the new trusted IP range.
6. Click **Save**.

Configuring Sites 7

This chapter contains the following sections:

This chapter explains how to configure MiVoice Connect sites.

7.1 Overview

The Mitel site is a logical concept designed to help system administrators organize the telephony environment. Sites can accommodate geographical requirements, such as where the external environment affects outbound calls, or logical requirements, such as a need to separate users who have advanced functions from standard users. After you create a site, you can assign servers, switches, appliances, users, other sites, and so on, to it.

You assign features to a site. For example, a site definition includes the following aspects: country, local area code, site operator, and admission control setting.

The MiVoice Connect system has a default site named “Headquarters”.

7.2 Viewing Configured Sites

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**.

The **Sites** page is displayed, and details about the columns on the Sites list pane are provided in Sites Page: List Pane.

Table 29: Sites Page: List Pane

Column Name	Description
Site	The name of the site

Column Name	Description
Country	The country in which the site is located. The information you specify here impacts the **Hardware type** you select for the site in the **Administration** > **Appliances/Servers** > **Platform Equipment** page when you are configuring switches for the site. For example, if your site is located in the UK, BRI switches will be available in the **Hardware type** drop down, but if your site is located in the US, BRI switches are not available in the **Hardware type** drop down.
Site Prefix	The prefix for the site, if one is configured. **Note**: This parameter allows you to add special characters. It is recommended that you do not add special characters (for example, !, #, $, %, & and so on) because this will restrict the calls you can make. **Note**: You can modify (that is, increase or decrease) the prefix length configured in the user extension. However, it is recommended that you do not modify the prefix length. This is because the prefix length configured in the user extension must match the prefix length configured in the dial plan.
Parent	The parent server for the site
Area Code	The area code associated with the site
Bandwidth	The bandwidth for the site
Switches	The number of switches installed at the site

7.3 Creating a Site

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. Click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays empty fields and default values.

4. Provide values for the parameters on the **General** tab, as described in Sites Page: Parameters on the General Tab.
5. Click **Save**.

Table 30: Sites Page: Parameters on the General Tab

Parameter	Description
Name	The name of a new or existing site. It must be unique.
Service Appliance Conference backup site	This option allows you designate a backup site for conferences initiated through a service appliance. If your MiVoice Connect system has service appliances assigned to sites other than Headquarters, you must select a remote site that has a service appliance installed to ensure that users will be able to reach a system conference extension.
Language	The default language for the site. You must obtain a license to enable more than one language. For more information about supported languages, see Configuring Languages on page 65.
Country / area	The name of the country in which the site is located.

Parameter	Description
Time zone	The time zone for the site, which is associated with the switches. This time zone determines the time and date provided for IP phones.
Parent	The parent site for the site. Sites other than Headquarters must select a parent. Only valid parent sites appear in the drop-down list. The default parent site is Headquarters. This server is used for two purposes: • By Connect Director to provide a default server when new users are added • By the call control software in voice switches so that calls that request voice mail service can be routed properly
Use parent site for emergency calls and other calls when no local trunks are available	Select this option to enable a child site to use the parent site trunk for non-routable calls (such as 911, 611, or 011) if no trunks are available at the child site. The parent site must be in the same country as the child site.
Use GrandParent site for emergency calls and other calls when no local trunks are available:	Select this option to enable a child site to use the grandparent site trunk for non-routable calls (such as 911, 611, or 011) if no trunks are available at the child site. The grandparent site must be in the same country as the child site.
Extension Prefix	Allows you to specify the number of digits used in extension prefixes that have this leading digit. Extension prefixes can be up to seven digits. The Configure Extension Prefix Warning section appears with a list of each of the sites in your system. Next to the list of sites you will find a blank field that requires you to enter the desired extension prefix. This prefix will be appended to every dialed number at thatparticular site. Ensure to back up the system before clicking **Save**.

Parameter	Description
Local area code	The local area code of the site, which enables users to dial local numbers without an area code. In the United States, this is the area code used for seven-digit dialing. For example, when the user dials an access code followed by seven digits at the site, this is the area code they are dialing. This also defines the area code that is considered local from a call permissions perspective.
Additional local area codes	In the United States, this defines area codes that can be dialed using 10-digit dialing instead of 1+10-digit dialing. For example, if the site is in an overlay area with multiple local area codes that require 10-digit dialing, you can be consistent with the dialing plan in your region by entering the additional area codes in this parameter. This also defines additional area codes that are considered local from a call-permissions perspective. • For each additional local area code that you want to add, click **Add** to create a data entry field for entering the additional area code. • Click **Remove** to remove a local area code.

Parameter	Description
Emergency number list	This is the list of numbers that can be dialed at the site (with or without a trunk access code) for emergency services. This number must not conflict with any extensions. • Click **Add** to create a data-entry field for entering an additional emergency number. (To accommodate locations where multiple emergency service numbers are required, each site is permitted to have a maximum of ten emergency numbers.) In each data-entry field, enter the exact emergency number required to contact the associated Emergency Service Provider. If **Trunk access code required**is selected, you can also enter a number in canonical format. • Click **Remove** to remove an emergency number.
Trunk access code required	Select this check box if you want a caller to dial the Trunk Access Code before dialing the specified emergency number. If this check box is not selected, entering the Trunk Access Code before the emergency number is permitted, but not required, to complete the call.

Parameter	Description
Enable RAY BAUM	Select this check box to enable RAY BAUM for emergency calls. **Note**: • This option is applicable only for US customers. • A reboot of the servers and switches will be required if the **Enable RAY BAUM** option is disabled. • After you clear the **Enable RAY BAUM** option, a reboot of the servers and switches will be required for the change to take effect.
Caller's emergency service identification (CESID)	Enter the Caller's emergency Service ID to be used. For example, enter **+14085555555.** For more information, see Configuring a System for Emergency Calls on page 983. **Note**: • Whenever you enter the CESID, it will be saved in the database as entered and will not be formatted as per the Country-specific numbering plan. • (For US customers) If the third-party vendor trunks are not used for RAY BAUM conformance, then the CESID will be the telephone number that will identify the location and the callback number.

Parameter	Description
Operator extension	This is the extension to which the user is transferred when he or she presses the operator digit for the site (typically “0”). You must configure the appropriate user before assigning the operator extension. This extension is different from the extension specified for the **When caller presses ‘0,’ transfer to** parameter on the **Users** > **Routing** > **Availability States** tab.
Fax redirect extension	When a fax tone is detected in an incoming call, the system automatically transfers the fax call to the fax redirect extension. Each site can have its own fax redirection number. The choice of the fax redirection number to use depends on whether the user or voice mail answers the call, as follows. • If the user answers the fax call, the system uses the fax redirection extension at the user’s site. • If the call is answered by voice mail, the Auto-Attendant or other menu, or a workgroup’s queue step menu, the fax redirection extension at the site where the call originated is used. This is the site with the trunk that processed the inbound external call. The fax redirection extension must be an existing user.
Admission control bandwidth	This value defines the bandwidth that voice streams can consume between the local site and all other sites. The caller hears a “network busy” prompt if this value is exceeded. To compute the admission control value for the site, see the *MiVoice Connect Planning and Installation Guide*.
Intra-site calls	This drop-down list has the types of encoding available for making calls within a site.

Parameter	Description
Inter-site calls	This drop-down list has the types of encoding used for calls between Mitel sites.
Fax and Modem Calls	This drop-down list has the types of encoding used for faxing or for calls made from a modem.
Virtual IP address	This parameter defines the IP address of the site's SIP Proxy Server and Registrar server. The IP address is independent of the switch that performs the server functions. SIP extensions require that this parameter be set to a valid address. See Introduction to SIP Profiles on page 673 for more information about SIP network elements.
Proxy switch 1	Specifies the switch that performs the site's SIP server functions. The drop down menu lists all switches that have SIP proxy resources and are assigned to the site. SIP extensions require a setting for this parameter.
Proxy switch 2	Specifies the switch that performs the site's SIP server functions when the switch specified by Proxy Switch 1 is not available. This parameter is optional.
SMTP relay server	Specifies the IP address or fully qualified domain name of the server to use as the SMTP relay for all voicemail enabled switches on this site.
Network time protocol server	Specifies the IP address for the Network Time Protocol server.

Table 31: Sites Page: Parameters on the Night Bell Call Handling Tab

Parameter	Description
Night bell extension	This is the extension that is used to ring the site's night bell. This extension must be associated with a Mitel switch audio output port that you specify as the next parameter. This extension is unique. You must configure the appropriate switch before assigning the night bell extension.
Night bell switch	This is the Mitel switch associated with the night bell extension. The night bell extension can share the same switch port as the paging extension.
Paging extension	This is the extension used for your overhead paging system. This extension must be associated with a Mitel switch audio output port that you specify as the next parameter. There is only one paging extension per site. You must assign switches to the site and select the switch that will support the paging extension before you can save a paging extension.
Paging switch	This is the Mitel switch associated with the paging extension. The paging extension can share the same switch port as the night bell extension. **Note**: This switch must not be a voicemail model switch.

Parameter	Description
Call forward condition	Select one of the following options for call forwarding of the night bell: • **Always** indicates that calls to the night bell extension should always be forwarded to the number in the **Always destination** field • **No Answer/Busy** indicates that calls to the night bell extension when that extension is not answered or is busy should be forwarded to the number in the **Busy destination** field. • **Never** indicates that calls to the night bell extension should never be forwarded.
Always destination	Specify the extension that a night bell call should be forwarded to when the Always call forwarding condition is in effect.
Busy destination	Specify the extension that a night bell call should be forwarded to when the Busy call forwarding condition is in effect.
No answer destination	Specify the extension that a night bell call should be forwarded to when the No Answer call forwarding condition is in effect.
Forward after	The number of rings after which the call should be forwarded.
Call stack size	The maximum number of simultaneous calls that can be “stacked” on the night bell extension.

Table 32: Sites Page: Parameters on the HELD Configuration Tab

Parameter	Description
Vendor Name	The third-party vendor enables retrieving the location during emergency calls. For example, RedSky or Intrado. The third-party vendor enables you to retrieve the location indirectly through a Location URI provided by the vendor's location information service (LIS).
Main HELD Server URL	The address of the third-party vendor's main LIS server. Example: https://api.primelab.e911cloud.com
Back-up HELD Server URL	The address of the third-party vendor's back-up LIS server. Example: https://api.primelab.e911cloud.com
Secret Key	Enter the secret key obtained from the third-party vendor. **Note**: • Click the **SHOW/HIDE** option alternatively to view or hide the secret key. • Secret Key is a mandatory parameter for RedSky. Contact the RedSky vendor for the secret key.

Parameter	Description

HELD Parameters	The HTTPS-Enabled Location Discovery (HELD) parameters for a specific third-party vendor.
	
	Note:
	The administrator can specify any number of vendor-specific parameters in this field using the following format:
	
	`key1=value1`
	
	`key1=value2`
	
	`...`
	
	`keyN=valueN`

Note:

- The **HELD Configuration** tab is applicable as part of RAY BAUM only for US customers.
- For information regarding the HELD parameters for RedSky and Intrado, see the following:
  - *HELD parameters for Intrado* table in the *Connect Client Integration with Intrado* section in the MiVoice Connect RAY BAUM'S General Overview and Solution Deployment Guide for Intrado.
  - *HELD parameters for RedSky* table in the *Connect Client Integration with RedSky* section in the MiVoice Connect RAY BAUM'S General Overview and Solution Deployment Guide for RedSky.

7.4 Viewing the Servers Assigned to a Site

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. In the **List** pane, click the site for which you want to view the servers.

4. In the **Details** pane, click the **Servers** tab.

> **Note**:
> The **Servers** tab displays the name and description for each voicemail switch, distributed voice server, and service appliance configured for that site.

5. If you want to see configuration details for that server, click its link in the Name column.

   The configuration page for that server is displayed.

7.5 Using Service Appliances as a Back-up Resource

This section describes how to configure two forms of backup that a service appliance can provide.

> **Note**:
>
> - A Headquarters site does not have any installed service appliances.
> - The main server fails at a site that also has a service appliance.

7.5.1 Registering a Remote Service Appliance for Access to the Headquarters Site

To ensure that all system users have access to service appliance functions when the Headquarters site has no installed service appliances, you can register a service appliance at the Headquarters site as a backup. Registering the back-up site with the Headquarters server establishes a hierarchical branch that gives service appliance services to all users throughout the network.

To register a backup service appliance site on the Headquarters server:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page opens.
3. In the **Site** column, select the Headquarters site.

Note:
The **Details** pane displays the **General** tab, which shows the configuration information for the Headquarters site.

4. In the **Service Appliance Conference backup site** drop-down list, select the site to use as a back-up site.

Note:
The backup site can be a logical site.

5. Click **Save**.

7.5.2 Creating a System Failover Mechanism for Conferencing

The MiVoice Connect system can ensure that conference resources remain available if the Connect headquarters server fails. While registering a service appliance at headquarters site, you can also specify a back-up Mitel site server that the system can use to access the service appliance if the headquarters site fails.

To assign a service appliance as a backup site server:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page opens.
3. In the **Site** column, select the headquarters site.

Note:
Details for the headquarters site appear in the **General** tab of the details pane.

4. In the **Service Appliance Conference backup site** drop-down list, select the site that you want to use for back up.

Note:
The back up site can be a logical site, and it must be physically separate from the headquarters site.

5. Click **Save**.

Configuring Application Servers 8

This chapter contains the following sections:

This chapter describes how to set up servers.

8.1 Overview

The MiVoice Connect system supports Distributed Voice application Servers (DVS). Distributed servers reduce WAN bandwidth by providing local voice mail and auto-attendant services, and increase the scale of the system.

Even though there are multiple servers, the MiVoice Connect system provides a single image of your entire network. The system is currently certified to support up to 21 servers; one main server, and up to 20 distributed servers. Consider adding a server at a site when the site exceeds 100 users. Add a new server for every 1,000 users.

The distributed servers run the following voice applications:

- Voice Mail – Each server supports 254 simultaneous voice mail, auto-attendant, account code prompts, workgroups, and paging connections. The voice mail system uses SMTP to transport composed messages between the distributed servers. The MiVoice Connect system also supports linking to legacy voice mail systems using AMIS protocols.
- File-Based Music on Hold – The system uses SMTP to distribute MOH files to the distributed servers.
- Auto-Attendant – The system supports up to 1000 menus that are hosted on every server.
- Configuration – The system enables users to log in and make configuration changes, such as call availability states, from their Connect client or from the Connect Client for Mobile device, if supported.
- Maintenance – The system provides a web site accessible through Connect Director for the maintenance of all the remote servers.

The distributed voice applications use a Remote TAPI Service Provider that relies on the call control information from the main server.

8.2 Distributed Voice Mail

The MiVoice Connect system uses distributed voice mail to provide high voice mail availability. Each remote server includes an instance of the telephony platform, allowing voice mail and auto-attendant services to maintain full functionality during short-term WAN outages. The distributed voice mail on the DVS allows users with mailboxes on the DVS to receive and pick up voice mail messages without depending on WAN connectivity to the headquarters server. The message waiting indicator (MWI) lights will update correctly regardless of WAN connectivity.

Additionally, incoming calls can still reach the automated attendant, access the dial-by-name directory, and reach the intended local party during a WAN outage. If a party cannot be directly reached due to a WAN outage and his or her availability state is configured to send unanswered calls to voice mail, the call is processed by the local voice mail server. Callers hear a generic greeting, including the called party's recorded name, and can leave a message that is later forwarded to the home voice mail server for the addressee.

Similarly, the DVS provides greater Connect client availability during WAN outages. If the WAN loses connectivity, users will retain full Connect client functionality as long as there is a DVS at the same site as the users, the users' voice mailboxes are on that server, and the DVS is managing the switch that manages the users' phones.

Although each voice mail server is autonomous in delivering voice services, it still must have connectivity to the configuration data stored on the headquarters server in order to make configuration changes. Specifically, users on an isolated remote server would not be able to change availability state modes or make other changes that require modification to the configuration data on the headquarters server. If you enable Distributed Database (DDB) on DVS, you can change the availability state modes locally without headquarters server connectivity.

8.2.1 IP Phone Limitations/Requirements

Basic connectivity, which is connectivity between the phone and the switch that is controlling the phone, is required. All aspects of the phone's operation are functional when this basic connectivity exists, with the following exceptions:

- For the IP100-series, IP200-series, and IP500-series phones, the Directory feature requires connectivity between the switch and a headquarters server or distributed voice server (DVS) that controls that switch.
- For the IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones, the Directory, History, visual voicemail, user options, and phone user interface assignment

features require connectivity to the headquarters server or distributed voice server. The IP655 phone also relies on connectivity to the server for Directory, History, and visual voicemail features.

- Options features, Changes to Availability State, Wrap-Up: In addition to basic connectivity, these features require either connectivity between the switch and a headquarters server or DVS that controls the switch. In addition, if the aforementioned server is a DVS, connectivity is required between that server and the headquarters server or Distributed Database (DDB) services must be enabled for the DVS. Further, connectivity between the DVS and the headquarters server is required for successful synchronization between the Replication Primary and Secondary databases.

Note:
See Mitel Distributed Database on page 140 for more information about this feature and how to enable it.

- Switch-to-switch extension monitoring: This condition exists when a programmed button requires monitoring activity on an extension that is serviced by a different switch than the one that controls the phone. For example, if switch A, which is the phone's switch, is controlled by server X, and switch B, which is the monitored extension's switch, is controlled by server Y, then servers X and Y may be a DVS or the headquarters server. For proper functionality of the switch-to-switch extension monitoring, the following conditions must exist:
  - Switch A must be able to talk to server X.
  - Server X must be able to talk to server Y.
  - Server Y must be able to talk to switch B.
  - If X and Y servers are the same, connectivity is, of course, assumed to exist.
- Auxiliary information about incoming calls, such as trunk information and called workgroup information, requires connectivity between the switch and a headquarters server or DVS that controls that switch.

8.2.2 Connect Client Limitations/Requirements

The following list details limitations and requirements for using the Connect client:

- Connect client: As long as the client can reach Headquarters and DVS servers, Connect client is fully functional.
- First-time Connect client users: When a user logs into Connect client for the first time, the Client Application Server (CAS) communicates with the headquarters server to find out which server they need to use. Thus, for first-time users, a connection is required between the client and the headquarters server regardless of where voice mail and extensions are serviced.

- Work group functionality: If users are configured to have work group functionality, they can access the mailboxes of all work groups to which they belong. This requires connectivity to the server(s) on which those mailboxes reside.
- Use Windows credentials: Connect client on MAC does not support domain credentials. The **Use Windows Credentials** option is disabled by default.

8.3 Configuring Application Servers

8.3.1 Adding Application Servers

The **Administration** > **Appliances/Servers** > **Platform Equipment** page in Connect Director provides access to the Platform Equipment list. The list is displayed in alphabetical order.

- To configure the SA100 Server, see the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.
- To configure the SA400 Server, see the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.
- To configure the Virtual Service Appliance, see the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.
- To configure the Linux DVS server, see Adding a Linux DVS Server on page 127.
- To configure voice switches, see Configuring Primary Voice Switches and Service Appliances on page 162.

By default, a MiVoice Connect system is configured with one server at the headquarters site. For more information on adding remote sites, see Overview on page 100.

Note:
With DDB enabled, if you upgrade the Headquarters server with unsupported client ID, country, or language, you must manually resync the Headquarters server.

8.3.2 Adding a Windows DVS Server

Note:
The following instructions assume a Windows DVS has already been installed. See the *MiVoice Connect Planning and Installation Guide* for Windows DVS installation information before proceeding.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the upper-right corner of the **Platform Equipment** page, click **New**. The **General** page opens.
4. From the Site drop-down list, select a **Site**.
5. Select **ShoreGear SoftSwitch** from the **Hardware** type drop-down list to display the list of parameters.
6. Enter the basic parameters based on the information in the Linux DVS Basic Parameters on page 127 section, voice mail and auto-attendant parameters based on the information in Table 41: Linux DVS Voice Mail General Parameters on page 134.

8.3.2.1 Windows DVS Basic Parameters

The following table includes a list of basic parameters required for configuring a new Windows DVS.

Table 33: Windows Base Parameters

Parameter	Description
Name	Name of a new or existing server.
Description	Description of the server type, for example “DVS1”. (Optional)
Site	Appliance location. The location of the appliance is a read-only parameter and cannot be changed. The default name of the main site is Headquarters, which can be changed on the **Edit Site** page.
IP Address	IP address of the server.

Parameter	Description
Fully Qualified Domain Name	Fully qualified domain name (FQDN) for the server, for example, stdvs1.acme.com.
Proxy Server URL	This parameter is the address of the site's operational proxy server. (Optional)
Allow Voice Mailboxes	Select this checkbox to enable voice mailboxes on this server. Clear this checkbox to disable voice mailboxes on this server. For app server deployments, such as ECC or Call Recording, disable voice mailboxes on the server. When the checkbox is empty, voice mail configuration fields are still available because the server can still operate as a back-up VM server. However, SMDI is not available, and the drop-down menu is disabled. If the server operates as a VM server, it also supports mailboxes by default, and Connect Director does not allow you to clear this check box.
Account Code Local Extension	This is the account code for local extensions. This is set automatically for the Headquarters server. For DVS, this is set manually.
Voice Mail Extension	Extension used by the voice mail server.
Voice Mail Login Extension	Extension used to log in to the voice mail server.
Auto-Attendant Extension	Extension used by the auto-attendant server. When a Windows DVS user dials AA, this extension is dialed.
Default Auto-Attendant Menu	Each server can have a different default auto-attendant menu. This is the menu reached when none is specified - for instance, when a caller dials 9 to escape from voice mail and return to the auto-attendant.

Parameter	Description
User Group	Assigned user group for the server. Due to voice mail placing outbound calls, the server must have assigned permissions.
Maximum Trunks for Voice Mail Notification	Maximum number of media streams used simultaneously to access voice mail. The valid range is 1-254. The default is 10.

8.3.3 Editing Windows DVS Parameters

Edit an existing Windows DVS server to configure additional parameters or modify existing basic parameters.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. On the **Platform Equipment** page that opens, click on the Windows DVS server.

Note:
The **Details** pane displays information about the selected DVS.

4. Change parameters as needed for the new server, and then click **Save**.

8.3.3.1 General Parameters

Windows Additional Basic Parameters includes a list of basic parameters that are accessed when editing an existing Windows DVS.

Table 34: Windows Additional Basic Parameters

Parameter	Description
Enable Local Database	Select to enable the distributed database on this server.

Parameter	Description
Use Database on Server	If Enable Local Database is chosen, select Local. Local is the default. Use caution before selecting this option as selecting Headquarters disables the local database.

8.3.3.2 Music On Hold Parameters

Click the Music on Hold tab to configure music on hold (MOH) on a Windows DVS. Windows Music on Hold Parameters includes the list of MOH parameters that are accessed when editing an existing server.

Table 35: Windows Music on Hold Parameters

Parameter	Description
Enable File Based Music on Hold	Select this check box to enable file based MOH streaming from this server.
Local Extension	This is the extension used by the music-on-hold server. This extension must be configured when file-based MOH is enabled.
Maximum Concurrent Music on Hold Calls (1 - 250)	This is the maximum number of calls that can simultaneously access music on hold on this server.

8.3.3.3 External Voice Mail Extension

Windows External Voice Mail Extension Parameters includes a list of parameters used for configuring external voice mail extensions.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, go to **Voice Application** tab > **Voice mail interface mode** field and select **External Voice Mail**.

Note:
These parameters are also accessed when editing an existing server. See Legacy Voice Mail Integration on page 126 for details about this feature.

Table 36: Windows External Voice Mail Extension Parameters

Parameter	Description
COM Port (1-10)	This is the COM port used by SMDI.
Message Desk Number (1-999)	The Message Desk default is 1. Valid values are 1 through 999. Set the number that the voice mail system expects. This parameter is most often set to 1, since only one system will be using the SMDI link. In some configurations, however, a number of SMDI links can be daisy-chained together and the Message Desk Number value is used to allow each system to know which data belongs to it.
Number of Digits (2-32)	This field sets the number of digits the MiVoice Connect system sends in the SMDI extension fields. Set this number to the value the voice mail system expects, most commonly 7 or 10. If the number of digits and the MiVoice Connect system extension value differ, the extension number is padded. For example, if Mitel needs to send extension 456 and the Number of Digits field is equal to 7, extension 0000456 is sent. If no padding is desired, the Number of Digits field would be set to 3 in this example. Then, only 456 is sent.
Translation Table Use for Call Data	This check box indicates that the digit translation table is to be used for call data, when checked. Both Translation Table boxes may be checked at the same time.
Translation Table Use for MWI Data	This check box indicates that the digit translation table is to be used for Message Waiting Indicator data, when checked. Both Translation Table boxes may be checked at the same time.

Parameter	Description
Extension List (extension - port - logical terminal number)	The SMDI message must contain the user extension, port number, and logical terminal number (exact trunk number). Note that these extensions forward to the Backup Auto-Attendant on No Answer or Busy. See Extension List Mapping on page 124 for additional details.

8.3.3.3.1 Extension List Mapping

To add extension list mapping to an application server configured for external voice mail, click **Add** found near the bottom of the edit page. The External Voice Mail dialog box appears.

Enter the **Extension** to be used to access the legacy voice mail system, the physical **Port** to be assigned to the extension, and the **Logical Terminal Number** for the extension. Trunks in the trunk group that send calls to external voice mail use this terminal number.

8.3.3.4 Mitel Voice Mail Extension

Windows Mitel Voice Mail Extension Parameters includes a list of parameters used for configuring Mitel voice mail extension parameters.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, go to **Voice Application** tab > **Voice mail interface mode** field and select **ShoreTel Voice Mail**.

Note:
These parameters are accessed when editing an existing server. See Legacy Voice Mail Integration on page 126 for details about this feature.

Table 37: Windows Mitel Voice Mail Extension Parameters

Parameter	Description
Trunk Group	Select the trunk group to be used by the legacy PBX for voice mail traffic.

Parameter	Description
COM Port (1-10)	This is the COM port used by SMDI.
Message Desk Number (1-999)	The Message Desk default is 1. Valid values are 1 through 999. Set the number that the voice mail system expects. This parameter is most often set to 1, since only one system will be using the SMDI link. In some configurations, however, a number of SMDI links can be daisy-chained together and the Message Desk Number value is used to allow each system to know which data belongs to it.
Number of Digits (2-32)	This field sets the number of digits the MiVoice Connect system sends in the SMDI extension fields. Set this number to the value the voice mail system expects, most commonly 7 or 10. If the number of digits and the MiVoice Connect system extension value differ, the extension number is padded. For example, if Mitel needs to send extension 456 and the Number of Digits field is equal to 7, extension 0000456 is sent. If no padding is desired, the Number of Digits field would be set to 3 in this example. Then, only 456 is sent.
Translation Table	Select a translation table from the drop-down list. For information on creating translation tables, see Configuring Digit Translation Tables on page 46.
Use for Call Data	This check box indicates that the digit translation table is to be used for call data, when checked. Both Translation Table boxes may be checked at the same time.
Use for MWI Data	This check box indicates that the digit translation table is to be used for Message Waiting Indicator data, when checked. Both Translation Table boxes may be checked at the same time.

Parameter	Description
Use Flash to Route Calls	Select this checkbox to use flash, such as a short hang-up, to provide signaling instructions to a PBX, to route calls between the Mitel voice mail system and the legacy PBX. Enabling this feature may result in a more efficient trunk allocation. **Note**: Analog trunks support the use of flash for this purpose, but other types of trunks, such as SGT1, do not. Clear this checkbox to prevent the system from attempting to use flash to route calls.

8.3.3.5 Legacy Voice Mail Integration

Mitel integrates with legacy phone systems for customers who would like to have the freedom and flexibility to continue to use their legacy systems while migrating toward a newer IP telephony solution. The legacy system must continue to work flawlessly regardless of whether calls are traversing the Mitel PBX on their way to the legacy voice mail system, or they are traversing the legacy PBX on their way to Mitel voice mail.

To address these needs, Mitel uses the Simplified Message Desk Interface (SMDI) protocol. SMDI allows dissimilar voice mail and PBX systems to work together. The protocol evolved at a time when voice mail services and PBX services were provided by separate physical devices, and enabled the disparate devices to share information over an out-of-band serial cable connection.

There are two modes of operation with respect to integrating a MiVoice Connect system and a legacy system using SMDI:

- External voice mail – In this configuration, the legacy system provides voice mail services while the MiVoice Connect system acts as the PBX for users.
- Mitel voice mail – In this configuration, the MiVoice Connect system provides voice mail services while the legacy system acts as a the PBX for users.

Voice mail extension lengths for the legacy voice mail system may be different from the Mitel voice mail extension lengths. In this case, digit translation information is required. For more information about digit translation tables, see Configuring Digit Translation Tables on page 46.

For more information about integration to legacy voice mail systems using SMDI, refer to the *MiVoice Connect Planning and Installation Guide*.

8.3.4 Adding a Linux DVS Server

Note:
The following instructions assume a Linux DVS has already been installed. Refer to the MiVoice Connect Planning and Installation Guide for Linux DVS installation information before proceeding.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, click **New**.

   The **General** tab page displays.
4. In the **Hardware** type field, select **Linux DVS Appliance** to display the list of parameters. Enter the basic parameters based on the information in the *Linux Base Parameters* table in Linux DVS Basic Parameters on page 127, voice mail and auto-attendant parameters based on the information in the *Linux DVS Voice Mail General Parameters* table in Additional Voice Mail, Auto-Attendant and Extension Parameters on page 133.

8.3.4.1 Linux DVS Basic Parameters

Linux Basic Parameters includes a list of basic parameters required for configuring a new Linux DVS.

Table 38: Linux Basic Parameters

Parameter	Description
Name	Name of a new or existing server.
Description	Description of the server type, for example “DVS1”. (Optional)

Parameter	Description
Site	Appliance location. The location of the appliance is a read-only parameter and cannot be changed. The default name of the main site is Headquarters, which can be changed on the **Edit Site** page.
IP Address	IP address of the server. Click **Find Switches** to choose from a list of available Linux DVS appliances.
MAC Address	MAC address of the server. Enter in xx-xx-xx-xx-xx-xx format.
Fully Qualified Domain Name	Fully qualified domain name (FQDN) for the server, for example “stdvs1.acme.com”. For Linux DVS, FQDN is the IP address.
Proxy Server URL	This parameter is the address of the site’s operational proxy server. (Optional)
Allow Voice Mailboxes	Select this checkbox to enable voice mailboxes on this server. Clear this checkbox to disable voice mailboxes on this server. When the checkbox is empty, voice mail configuration fields are still available because the server can still operate as a back-up VM server. However, SMDI is not available, and the drop-down menu is disabled. If the server operates as a VM server, it also supports mailboxes by default, and Connect Director does not allow you to clear this check box.
Account Code Local Extension	This is the account code for local extensions. This is set automatically for the Headquarters server. For Linux DVS, this is set manually.
Voice Mail Extension	Extension used by the voice mail server.

Parameter	Description
Voice Mail Login Extension	Extension used to log in to the voice mail server.
Auto-Attendant Extension	Extension used by the auto-attendant server.
Default Auto-Attendant Menu	Each server can have a different default auto-attendant menu. This is the menu reached when none is specified - for instance, when a caller dials 9 to escape from voice mail and return to the auto-attendant.
User Group	Assigned user group for the server. Due to voice mail placing outbound calls, the server must have assigned permissions.
Maximum Trunks for Voice Mail Notification	Maximum number of media streams used simultaneously to access voice mail. The valid range is 1-1000. The default is 10.

Parameter	Description

Enable daily backup	When selected, allows you to specify a server to use for backup.
	
	Specify the following to enable backup in FTP or HTTPS server:
	
	• **IP address**
	  • For FTP server, enter the IP address of the FTP server to which the switch files must be backed up.
	  • For HTTPS server, enter the IP address of the HQ server to which the switch files must be backed up.
	• **FTP Port**—enter the port number that the switch is to use to communicate with the recipient FTP server. The default port number is 21.
	• **Directory**
	  • For FTP server, enter the path to the file on the FTP server to which you want to back up the switch files.
	  • For HTTPS server, enter the path to the file on the HQ server to which you want to back up the switch files.
	• **Username** — enter the user name that the appliance is to use to access the FTP server files for backup.
	• **Password**—enter the password that the switch uses to access the FTP server files for backup. Reenter the password again in the second field.
	• **Enable HTTPS** — select this check box to enable backup using HTTPS.

8.3.5 Editing Linux DVS Parameters

Edit an existing Linux DVS server to configure additional parameters or modify existing parameters.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.

3. In the **Platform Equipment** page that opens, click on a Linux DVS server.

> **Note**:
> The **Details** pane displays information about the selected Linux DVS.

4. Change parameters as needed for the new server. Use Table 40: Linux Music on Hold Parameters on page 133 for Music on Hold parameters and Linux DVS Voice Mail General Parameters to modify previously configured voice mail parameters.
5. Click **Save**.

8.3.5.1 General Parameters

The following table includes a list of basic parameters that are accessed when editing an existing Linux DVS.

Table 39: Linux Base Parameters

Parameter	Description
Enable Local Database	Select to enable the distributed database on this server.
Use Database on Server	If Enable Local Database is chosen, Local is selected by default. Selecting Headquarters disables the local database. Use caution before selecting this option.

Parameter	Description

Enable daily backup	When selected, allows you to specify a server to use for backup.
	
	Specify the following to enable backup in FTP or HTTPS server:
	
	• **IP address**
	  • For FTP server, enter the IP address of the FTP server to which the switch files must be backed up.
	  • For HTTPS server, enter the IP address of the HQ server to which the switch files must be backed up.
	• **FTP Port**—enter the port number that the switch is to use to communicate with the recipient FTP server. The default port number is 21.
	• **Directory**
	  • For FTP server, enter the path to the file on the FTP server to which you want to back up the switch files.
	  • For HTTPS server, enter the path to the file on the HQ server to which you want to back up the switch files.
	• **Username** — enter the user name that the appliance is to use to access the FTP server files for backup.
	• **Password**—enter the password that the switch uses to access the FTP server files for backup. Reenter the password again in the second field.
	• **Enable HTTPS** — select this check box to enable backup using HTTPS.

8.3.5.2 Music On Hold Parameters

Click the **Music on Hold** tab to configure music on hold (MOH) on a Linux DVS. The following table includes the list of MOH parameters that are accessed when editing an existing server.

Table 40: Linux Music on Hold Parameters

Parameter	Description
Enable File Based Music on Hold	Select this check box to enable file based MOH streaming from this server.
Local Extension	This is the extension used by the music-on hold server. This extension must be configured when file-based MOH is enabled.
Maximum Concurrent Music on Hold Calls (1 - 250)	This is the maximum number of calls that can simultaneously access music on hold on this server. This is a maximum limit, not a guaranteed number.

8.3.5.3 Additional Voice Mail, Auto-Attendant and Extension Parameters

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, go to the **Voice Application** tab to configure additional voice mail parameters.

Linux DVS Voice Mail General Parameters includes a list of parameters used for configuring additional general voice mail parameters that were configured in Adding a Linux DVS Server on page 127. These parameters are also accessed when editing an existing server. The default **Voice mail interface mode** is **None** and displays the following parameters:

Table 41: Linux DVS Voice Mail General Parameters

Parameter	Description
Allow Voice Mailboxes	Select this checkbox to enable voice mailboxes on this server. Clear this checkbox to disable voice mailboxes on this server. When the checkbox is empty, voice mail configuration fields are still available because the server can still operate as a back-up VM server. However, SMDI is not available, and the drop-down menu is disabled. If the server operates as a VM server, it also supports mailboxes by default, and Connect Director does not allow you to clear this check box.
Account Code Local Extension	This is the account code for local extensions. This is set automatically for the Headquarters server. For DVS, this is set manually.
Voice Mail Extension	Extension used by the voice mail server.
Voice Mail Login Extension	Extension used to log in to the voice mail server.
Auto-Attendant Extension	Extension used by the auto-attendant server.
Default Auto-Attendant Menu	Each server can have a different default auto-attendant menu. This is the menu reached when none is specified - for instance, when a caller dials 9 to escape from voice mail and return to the auto-attendant.
User Group	Assigned user group for the server. Due to voice mail placing outbound calls, the server must have assigned permissions.
Maximum Trunks for Voice Mail Notification	Maximum number of media streams used simultaneously to access voice mail. The valid range is 1-1000. The default is 10.

8.3.5.4 Generating a Certificate

Follow these steps to generate a certificate:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, select the required server.
4. Click the **Certificate** tab to generate a certificate.

Note:
Certificate Parameters includes a list of parameters used for generating the certificate. These parameters are accessed when editing an existing server.

Table 42: Certificate Parameters

Parameter	Description
Name	Enter a name for the certificate.
Subject Domain	Displays certificate information.
Issuer	Details about the Certificate Authority for the installed certificate. This information is read-only.
Password/Passphrase	If the certificate files are password protected, enter the password or passphrase for the files.
Certificate files	Click Choose File to select a new certificate to install. Typically, this would be a certificate purchased from a well-known Certificate Authority. You must select and upload all the files provided by the Certificate Authority.
Delete certificate	Click the Delete Current Certificate button to delete the selected certificate.

1. Click **Save** to save the certificate to the Mitel database and the key to Shoreline Data > keystore > private folder.

Note:

The **Fully qualified domain name** field in the **General** tab displays the fully qualified domain name server IP address.

8.3.6 Adding Ingate

Follow these steps to add the Ingate appliance:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, click **New**.

   The **General** tab page opens.

> **Note**:
> You must leave the **Sites** field in the **General** tab page as is because Ingate is not bound to any site.

4. In the **Hardware type** field, select **InGate** to display the list of parameters.
5. Enter the basic parameters based on the information in InGate Basic Parameters.
6. Click **Save**.

> **Note**:
> After you click **Save**, Ingate is added and the certificate and key for InGate is automatically generated.

7. After the Ingate configuration is saved, administrators can copy the certificate and key by clicking the **Download** option. The administrator can copy and save these manually in a .cer file. This file will be used during the TLS configuration as a private certificate for the Ingate internal interface.

Table 43: InGate Basic Parameters

Parameter	Description
Hardware type	Select **InGate** from the list of options.
Name	Name of the Ingate appliance.
Description	Description of the Ingate appliance, for example “Ingate1”.

Parameter	Description
IP address	IP address of the Ingate internal interface.
MAC address	MAC address of the internal ingate interface. Enter in xx-xx-xx-xx-xx-xx format. **Note**: To obtain the MAC address, see the *Adding InGate and Creating a HQ-Signed Certificate* section in the *MiVoice Connect Installing and Configuring MiVoice Connect with InGate Server Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.
Fully qualified domain name	Fully qualified domain name (FQDN) of Ingate, for example “stdvs1.ingate.com”.
Note	This option allows you to add any additional information.
Download	Administrators can copy the Ingate certificate and key by clicking the **Download** option.

8.3.7 Editing InGate Parameters

Edit an existing InGate server to configure additional parameters or modify existing parameters.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, click the InGate server to edit.

Note:
The **Details** pane displays information about the selected InGate Server.

4. Add new parameters as needed or use Table 43: InGate Basic Parameters on page 136 to modify previously configured InGate parameters.

Note:
You cannot edit the **IP address** and **MAC address** fields. To add a new IP address or MAC address, you follow the instructions in Adding Ingate on page 136.

5. Click **Save**.

8.4 Disabling TLS 1.0

Note:
Beginning with Release 19.3, MiVoice Connect will implement the **Enable TLS1.0 and TLS 1.1** option to disable TLS1.0 and TLS1.1 Customers are recommended to use this option to disable TLS 1.0 rather than following manual steps explained in this section.

You can disable TLS 1.0 either on Windows HQ servers (Windows Server 2012, Windows Server 2016, and Windows Server 2019) or on Linux DVS server. This section describes the steps to disable TLS on Windows HQ server and Linux DVS server.

Note:
TLS 1.0 is still required for:

- MGCP phones.
- VxWorks-based switches (non voice-enabled SG switches).

You must upgrade these devices if you want to disable TLS 1.0 in the customer environment.

To disable TLS 1.0 using Windows HQ server:

1. In the Windows start menu, type **regedit** and click **OK**.
2. In the dialog box that opens, click **Yes**.

> **Note**:
> It is recommended that you back up your current registry before making any changes. To do this, click **File** > **Export** and then save the backup to a safe location.

3. Go to the following path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`.
4. Right-click the empty space in the pane on the right side and do the following:
   a. Select **New** > **Key**.
   b. Name the new key **TLS 1.0**.
5. Select the new key, right-click the empty space on the right side, and add two new keys named **Client** and **Server**.

> **Note**:
> You can skip step 4 and step 5 if the **TLS 1.0** folder already exists.

6. Select the **Client** key, right-click the right pane, and create a DWORD value as follows:
   a. Select **New** > **DWORD (32-bit) Value**.
   b. Edit the new DWORD value and name it **Enabled**.
   c. Ensure the value data is **0** (0x0).
   d. Click **OK** to save the settings.f
7. Select the **Server** key and repeat step 6 to create a DWORD value named **Enabled** with setting of **0** (0x0).

To disable TLS 1.0 on Linux DVS server:

1. Perform SSH to Linux server with the FQDN or IP address of the Linux server using admin credentials.
2. In the window that opens, change to root permissions with root credentials.
3. Navigate to the following path: `etc/nginx`.
4. Open the **nginx.conf** file in **Edit** mode.
5. Search for the **ssl_protocols** in the **nginx.conf** file.
6. Remove instances of **TLSv1** from all the **ssl_protocols** in **nginx.conf** file.

7. Save the file.

Note:
After disabling TLS 1.0 and upgrading the HQ server, TLS 1.0 is automatically re-enabled. To fix this issue, TLS 1.0 must be explicitly disabled every time the HQ server is upgraded.

8.5 Mitel Distributed Database

Organizations with remote sites often rely on the headquarters location to host and maintain the database for the entire company. A database on the Headquarters server gives convenient access to IT groups for upgrades and real-time maintenance activities.

Customers can also deploy a read-only copy of the Mitel database on Mitel's DVS. Using a distributed database speeds up local queries and can reduce network traffic. Scalability is improved because the Headquarters server is not a bottleneck for database accesses.

Applications on the DVS typically connect to a copy of the database that runs on the local server.

The following write operations are possible on the local DVS:

- User-changes to Availability State
- Re-synchronization of SIP phone registration

All other write operations are performed on the database at the Headquarters server.

Note:
Initial registration for SIP phones still requires a write to the Headquarters server. Also, initial login of users and agents requires write operations to a Headquarters server.

8.5.1 Benefits of a Distributed Database

This section outlines some of the benefits of activating the Distributed Database feature.

- Availability – A server at a remote site with a Distributed Database can run without disruption if the headquarters server becomes unavailable. If necessary, the system administrator can reboot the remote server without connectivity to the Headquarters server.

- Scalability – Implementing a Distributed Database on remote servers can reduce the workload on the Headquarters. The remote server can respond to queries locally.
- A distributed database also provides the following benefits:
  - Connect client users do not need access to the Headquarters server to modify availability states.
  - Normally, the administrator does not need to perform additional tasks after completing the initial configuration. The database on the Headquarters server acts as the replication primary, and the remote servers are replication secondary servers.
  - Updates from the remote server automatically go to the headquarters database. All applications continue working without changes while the headquarters system is unavailable and continue to work while the Headquarters database is receiving updates.

8.5.2 Important Considerations and Warnings

This section contains important information for system administrators who are configuring servers.

- Voice Mailbox Server switches do not host copies of the database.
- In the current release, the Distributed Database feature and the Distributed Workgroups feature cannot be active on the same MiVoice Connect system at the same time. The choice for which feature is more important depends on the needs of the customer.
- When the Distributed Database is active, changing the name of the remote application server (DVS) breaks the database replication. To re-establish DDB replication between the headquarters and the DVS servers, delete the log file and then manually re-synchronize the databases.

  The log file is located at `C:\Shoreline Data\Database\ShoreTelConfig \Data\relay-log.info`.
- When the DVS is down for an extended period of time and then comes back up, the DDB is not automatically re-synchronized with the headquarters database. In this case, you must manually re-synchronize the databases.

8.5.3 Configuration of Distributed Database Service

Configuring the Replication Primary and Secondary

The Mitel installer configures the headquarters database as the replication primary by enabling replication for new installations and for upgrades. By default, the Mitel installer installs a MySQL instance on every remote server. However, this MySQL instance is not a writable copy of the Mitel database.

All applications on the remote server normally point back to the headquarters database by default. For an application to use the local copy of the MySQL database, additional configuration steps are necessary.

8.5.3.1 Configuring Distributed Application Servers to Host the Mitel Database

The Headquarters/DVS Edit Server page contains a section for specifying the location of the database server. This is configurable after the initial settings have been applied in Adding a Windows DVS Server on page 118 or Adding a Linux DVS Server on page 127. Administrators can create a local database by selecting the appropriate check box. The database instance can be created on the remote server as needed.

For example, a Distributed Voice Server can use the headquarters database when initially installed. As the demands on the headquarters server increase, the administrator may decide to add a local database instance on the DVS and configure the applications on the DVS to use the local database. Mitel provides a drop down list that will allow the DVS to switch to other databases, thus allowing for local or default database operation. For DVS's not configured with a local database, including VMBs, the administrator needs to select a proper database, usually a database server on the same site. Otherwise, the default action is to use the headquarters database.

When **Create Local Database** is unchecked, the local database instance will be removed. If the local database is referenced by other DVS's, the operation will fail. If the DVS that hosts the database is the only one that references the database, deletion of the local database will be allowed. The DVS will then be switched to use the headquarters database.

1. Click **Enable local database**.
2. Click **OK** in the popup to continue.
3. Click **Save**.

Note:
Enabling the local database does not show Distributed Voice Servers in the Workgroups Server drop-down list. Only the Headquarters server is available. If the local database is disabled, all DVS components and Headquarters are displayed. If distributed Workgroups are created, **Enable local database** check box is greyed out.

8.5.3.1.1 Distributed Database in Diagnostics and Monitoring

The **Diagnostics and Monitoring** > **System** page in Connect Director shows the database replication status in the Servers area. If a distributed database (DDB) is present, a small disk icon under the DB heading on the server line indicates the server has a database instance. Green and red color coding shows replication status.

Click the name of the server to see status for more services in addition to the database on the server and to start or stop individual services.

Note:
The database section in the **Diagnostics and Monitoring** > **Servers** page shows the primary status, which includes the log file name and log position for the primary. Use this page to compare this information with the corresponding secondary database information on the DVS maintenance page to determine how far out of sync the remote database instance and headquarters system might be. If connectivity to the headquarters server is long-term, you can manually synchronize the systems. The synchronization point is the last snapshot performed on the primary database. Clicking the **Snapshot** button at the bottom of the Database area triggers an instant snapshot of the database that is used for synchronization or installation purposes.

8.6 Moving Components from Windows DVS to Linux DVS

The process of “upgrading” from a Windows DVS to a Linux DVS is achieved by creating a Linux DVS and moving users, auto-attendant, work groups, paging groups, and route points from the Windows server to the Linux server. Refer to Adding a Linux DVS Server on page 127before attempting to complete this procedure.

Moving components from Windows DVS to Linux DVS is accomplished by updating existing Shoreware Director fields and completing a process which automatically moves these components to the new Linux server. Use the following procedures to complete this operation:

After completing the steps in each of these areas, you may delete the Windows DVS from the system.

Note:

- Moving users from a Windows DVS to a Linux DVS residing at different sites may require planning, upgrading and/or installation procedures prior to performing the following steps. See the *Upgrades* and *Server Requirements* section in the *MiVoice Connect Planning and Installation Guide* for planning information.
- .Attempting to delete the Windows DVS from the system prior to completing the previous tasks displays an error and warning to complete these tasks first.

8.6.1 Moving Switch and Users

Linux DVS must be added to the same site as the Windows DVS assuming that the switch is also in the same site. If the Linux DVS is added in a different site other than the Windows DVS, switch can be pointed to the Linux DVS. However, to move phones, modify the IP phone address map from Windows DVS server to Linux DVS in the IP Phone Address Map page under Telephones.

Complete the following procedure to move a Switch managed by a Windows DVS to a Linux DVS:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the upper window, click the switch.
4. In **Server to manage switch**, select the name of the Linux DVS created in Adding a Linux DVS Server on page 127.
5. Click **Administration** > **Users** > **Users**.
6. In the **Users** page that opens, go to **General** tab > **Mailbox server** field to view the mailboxes.
7. Click the search field (magnifying glass) to display the fields under each parameter. In the **Mailbox server** field, enter the name of the remote server. Click the -> icon, or press Enter.
8. Select the appropriate user(s) or use the select-all checkbox in the upper left to select all users.
9. Click **Bulk Edit**.
10. In the **Mailbox server** field, click the Linux DVS and click **Save**. Check the **Results** tab to verify if the system operation is complete.

11. After moving the mailbox, phones must be moved to the same site as the Linux DVS, if the Linux DVS is added in a different site other than Windows DVS.

8.6.2 Moving Auto Attendant

Complete the following procedure to assign the Auto Attendant managed by a Windows DVS to a Linux DVS:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the upper window, click **Auto Attendant**.
4. Click the **Voice Application** tab > **Default Auto Attendant menu**.
5. Select the appropriate Auto Attendant from the pull-down menu.

> **Note**:
> The same auto attendant used for Windows DVS must be retained. In the Linux DVS page, select the same auto attendant.

6. Click **Save**.

8.6.3 Moving Work Groups

Complete the following procedure to move a Work Group managed by a Windows DVS to a Linux DVS:

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Workgroups**.
3. In the upper window, click the Workgroup to move the workgroup server from Windows DVS to Linux DVS.

> **Note**:
> If Distributed Database (DDB) is enabled, the “Server” change is not required.

4. Change **Mailbox Server** to the name of the Linux DVS created in Adding a Linux DVS Server on page 127.
5. Repeat these steps for every Work Group.
6. Click **Save**.

8.6.4 Moving Paging Groups

Complete the following procedure to move a Paging Group managed by a Windows DVS to a Linux DVS:

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Call Control** > **Paging Groups**.
3. In the upper window, click the Paging Groups to move the Paging Group server from Windows DVS to Linux DVS.
4. Change **Group Paging Server** to the name of the Linux DVS created in Adding a Linux DVS Server on page 127.
5. Repeat these steps for every Paging Groups.
6. Click **Save**.

8.6.5 Moving Route Points

Complete the following procedure to move Route Points managed by a Windows DVS to a Linux DVS:

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Call Control** > **Route Points**.
3. In the upper window, click **Route Point** to move the route point server from Windows DVS to Linux DVS.

> **Note**:
> If Distributed Database (DDB) is enabled, the “Server” change is not required.

4. Change **Mailbox Server** to the name of the Linux DVS created in Adding a Linux DVS Server on page 127.
5. Repeat these steps for every route points.
6. Click **Save**.

8.6.6 Deleting the Windows DVS

After completing the previous procedures to move all the users from the Windows DVS to the Linux DVS, you may delete the Windows DVS.

Note:
After completing the procedures in Moving Components from Windows DVS to Linux DVS on page 143, all the users will be deleted from the Windows DVS and moved to the Linux DVS. Attempting to delete the Windows DVS from the system prior to completing the procedures displays an error and warning to complete these tasks first.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**, then select the Windows DVS and click **Delete**.
3. Click **OK** to complete the operation. Any remaining tasks to complete popup as a warning. Return to the location noted in the popup and complete the operation before re-attempting to delete the Windows DVS.

8.7 Integration through Q-Signaling Protocols

Mitel supports the integration of the Unified Communications solution with other PBX platforms and the Q-Signaling protocol (QSIG) supplemental services for call diversion and message-waiting indication. Refer to Moving Auto Attendant on page 145 for details about configuring basic QSIG services. This integration allows a voice mail system located on either side of the QSIG link to be used by other system administrators to configure a Mitel user for voice mail that is hosted on a legacy PBX system using the same QSIG trunks on the same system.

QSIG is a Common Channel Signaling (CCS) protocol that runs over the ISDN D-channel for signaling between nodes in a Private Integrated Services Network (PISN). QSIG supports call setup, call tear down, and transparency of features such as message waiting, camp-on, and callback.

The current release of Mitel supports both ECMA and ISO versions of QSIG.

8.7.1 Configuring Mitel Users for External Voice Mail with QSIG

The process for configuring QSIG External Voice Mail involves the following activities:

- Configuring a QSIG Tie Trunk to integrate with the external system. See Configuring Trunk Groups on page 219 for details about configuring tie trunks.
- Defining QSIG Server integration
- Configuring a User Group for use of external QSIG Voice Mail
- Creating an Extension-Only user in the User Group

Use the following steps to configure QSIG External Voice Mail:

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Voice Mail** > **External Voice Mail Servers (QSIG)** menu. The **External Voice Mail Servers (QSIG)** page opens.
3. Select a site and click its name to open External Voice Mail.
4. Enter the name of the integration in the **Name** field and the pilot number for the voice mail in the **Voice mail pilot number** field. The pilot number is the OSE number for voice mail login or redirection included in the PRI or BRI Off System Extension range.
5. Configure a User Group that uses external QSIG voice mail by selecting **External Voice Mail, QSIG** in the drop-down list for **Voice Mail Interface Mode**.

Note:
See the *MiVoice Connect Planning and Installation Guide* for sample Use Cases for implementing Mitel users with External Voice Mail QSIG.

8.7.2 Configuring Legacy Users for Mitel Voice Mail through QSIG

The following steps describe the procedures necessary to configure an external user with Mitel voice mail service with QSIG External Voice Mail.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Select the **Voicemail Application** tab.
4. In the **Voice mail interface mode** field, select **<None>**.
5. Configure a Mailbox-Only account for the external user. The external user is now configured for Mitel voice mail on the MiVoice Connect system.

Note:
See the *MiVoice Connect Planning and Installation Guide* for sample use cases for implementing legacy users with Voice Mail QSIG.

8.7.2.1 Important Considerations

The following list includes important considerations to make when configuring application servers:

- The diversion implementation on both sides is not limited to voice mail service. Diversion due to call-forwarding, for example, is signaled by the same methods.
- Some Mitel features, such as Find Me, can result in multiple trunks being used to host a call.
- No QSIG channel usage is available for secondary calls. See *Mitel's Norton Option 11C QSIG application note* for more details on configuring this feature.

8.8 Fax Server Connection to a Switch

A Voice Switch can connect directly to a fax server. End-users can receive faxes sent to their primary phone. When a call is answered either by the original called user or through call forwarding, the system redirects it to the fax redirection extension.

The fax redirection extension is the first port allocated to the fax server. When multiple switch ports are dedicated to the fax server, a fax call to the user phone is redirected to the first port connected to the fax server. If the first port is busy with a call, the fax goes to the next port.

The sequence of events for a fax call is as follows:

1. When the fax call is answered by the user's primary phone, the switch immediately sends the original user's extension as DTMF.
2. The fax server detects the completion call when the loop current switches off.
3. When the fax call is complete, the fax server looks up the user extension in its configuration and then routes the fax to the called user.

The fax can go to the user as an email attachment if the fax server is configured to support this function.

Note:
For more information on fax server integration, refer to the *MiVoice Connect Planning and Installation Guide*.

Configuring Voice Switches 9

This chapter contains the following sections:

This chapter provides a general overview of the Voice Switches and information on how to configure them through Connect Director. A Voice Switch connects to the IP network over a 10/100/1000M Ethernet port.

For more information about the features supported outside the U.S. and Canada, see the *International Planning and Installation* in the *MiVoice Connect Planning and Installation Guide*.

9.1 Switch Types

The following types of voice switches are available:

- 1U Full- and Half-Width SG and ST Voice Switches
- Virtual switches

The sections that follow briefly introduce each switch family. See the “Voice Switches” appendix in the *MiVoice Connect Planning and Installation Guide* for details about voice switches. This appendix includes LED behavior, interface details, capacity, and front panel illustrations.

9.1.1 1U Half-Width Voice Switches

The 1U Half-Width switches can support IP phones, softphones, SIP trunks, SIP devices, analog trunks and devices, and SGT1/SGE1 digital connections. 1U Half-Width Switches have a smaller footprint, use less power, and have lower heat dissipation requirements than earlier Voice Switches. These switches offer higher granularity in the number of IP users supported, allowing customers to precisely program the switch to satisfy their requirements.

The switches can be stacked or mounted in a standard 19-inch rack. Rack mounting 1U Half-Width Switches requires one of the rack mounting kits listed below. One or two

switches are inserted side-by-side into the Dual Tray, which is then mounted into the 19-inch rack.

- Use the Rack Mount Dual Switch Tray to mount SG Voice Switches. See the *ShoreGear Dual Tray: Wall Mount Kit Quick Install Guide* for information about this kit.
- Use the ST Voice Switch Wall Mount Bracket Kit to mount ST Voice Switches. See the *ST Voice Switch Wall Mount Bracket Kit Quick Install Guide* for information about this kit.

Note:
To prevent overheating and fire hazard, do not use the Rack Mount Dual Switch Tray to wall mount the following devices: ST1D/ST2D, ST50A/ST100A, ST200/ST500, or ST100DA. Use the ST Voice Switch Wall Mount Bracket to wall mount these devices.

1U Half-Width Voice Switch models include the following. Voice switch names followed by V denote voice switches that support both voice mail and auto-attendant applications:

- ST1D
- ST2D
- ST50A
- ST100A
- ST100DA
- ST200
- ST500
- Voice Switch SG90V
- Voice Switch SG90
- Voice Switch SG50V
- Voice Switch SG50
- Voice Switch SG30
- Voice Switch SG90BRIV
- Voice Switch SG90BRI
- Voice Switch SG30BRI
- Voice Switch SG220T1
- Voice Switch SG220T1A
- Voice Switch SG220E1
- Voice Switch SGT1k
- Voice Switch SGE1k

9.1.2 1U Full Width Voice Switches

The 1U Full Width Switch family models support analog data streams. Full width switch models can be stacked or mounted in a standard 19-inch equipment rack. These switches have a height of 1 U and an RJ21X connector for connection to analog phones and trunks. They also have redundant Ethernet LAN connections to ensure availability.

The 1U Full Width Voice Switch models include:

- Voice Switch ST24A/ST48A

9.1.3 Virtual Switches

With the proper license and VMware® software configuration, Mitel offers the capability to configure the following types of virtual switches:

- A Virtual Phone Switch (vPhone Switch) can support up to 5,000 IP phone SIP proxy ports, depending on the configuration. In addition, virtual phone switches support the following features:
  - Up to 5000 IP Phone SIP Proxy Ports
  - Backup auto attendant
  - Make Me conferences — 6 per 100 users with a max of 60
  - Hunt groups capacity as follows:
    - Hunt groups — 4 per 100 users with a maximum capacity of 40
    - Total hunt group users — 16 per 100 users with a maximum capacity of 160
    - Total number of users per hunt group — 16 per 100 users with a maximum capacity of 16
  - Pick up groups
  - Bridged call appearance
  - Extension monitoring
  - SIP Proxies for third-party devices
- A Virtual Trunk Switch (vTrunk Switch) can support the following features:
  - Up to 2000 SIP trunks with media proxy, depending on the configuration
  - Backup auto attendant
  - Transcoding between mismatched codecs
  - Trunk recording
  - Three party mesh conferencing

See the *MiVoice Connect Planning and Installation Guide* for details about virtual switch capacities.

Note:
SIP media proxies are always on and are not dynamic.

9.2 Switch Resources

Voice switches provide telephony, IP phone, and SIP phone resources to Mitel users. Each voice switch offers a combination of resources that can be customized to support specific, individual configurations.

This section describes the resources available on voice switches, including details about the features available on the switch.

9.2.1 Analog Circuits

Voice switches support three analog circuits: Extensions, DID trunks, and Loop Start trunks.

- Extensions: Extensions are telephony foreign exchange station (FXS) circuits that:
  - Transmit and receive voice signals
  - Supply power to phones
  - Provides loop current to analog phones for dial tone and ring signals
  - Indicate on-hook or off-hook state

Connect Director shows extensions as *analog ports*. They are assigned to user extensions.

- DID Trunks: DID trunks support inbound Loop Reversal trunks that provide DID service from the central office. DID trunks are assigned to trunk groups. Analog DID trunks are inbound only.
- Loop Start Trunks: Loop start trunks are foreign exchange office (FXO) circuits that support inbound and outbound calls. These trunks accept ring signals, go on-hook and off-hook, and transmit and receive voice signals.

9.2.2 Digital Circuits

Mitel offers SGT1, SGE1, and BRI digital circuits that support Channel Associated Signaling (CAS) and Integrated Service Digital Network (ISDN) signaling through various 1U Half-Width and 1U Full-Width switches. Circuit channels are configured in Connect Director in the **Administration** > **Appliances/Servers** > **Platform Equipment** > **Switch** page for the switch that is being configured.

9.2.3 IP Phone Ports

Voice switches and virtual switches support varying numbers of IP phones, as specified by the Switch Edit page in Connect Director.

Switch processing resources that support Digital and Analog ports on most Voice Switches can be reallocated to support five IP phone ports. For example, resources on a switch that supports 12 analog ports can be reallocated to support 60 IP phone ports.

9.2.4 SIP Trunks

Voice Switches, virtual phones, and virtual switches support varying numbers of SIP trunks, as specified in Connect Director in the **Administration** > **Appliances/Servers** > **Platform Equipment** > **Switch** page.

Switch processing resources that support Digital and Analog ports on most Voice Switches can be reallocated to SIP trunks. For example, the ST2D has 60 digital trunks, which can be replaced with 60 SIP Trunks.

9.2.5 SIP Proxies

Voice Switches, virtual phones, and virtual switches support varying numbers of SIP proxies, as specified by the Connect Director **Administration** > **Appliances/Servers** > **Platform Equipment** > **Switch** page.

Switch processing resources that support Digital and Analog ports on most switches can be reallocated to support 100 SIP proxies. For example, resources on a switch that supports 14 analog ports can be reallocated to support 1400 SIP proxies.

When SIP proxies are configured on SG switches, the switches do not use the Make Me conference ports for three-party conferences.

9.2.5.1 Built-In Capacities for IP Phone Ports, SIP Trunks, and SIP Proxies

Many switches provide processor resources that support IP phones without disabling telephony ports. Built-in capacity can be configured to allocate resources for IP phones, SIP Trunks, or SIP Proxy ports. Resources allocated to support IP phones cannot support SIP trunks or SIP proxies.

For SIP proxies, you can use built-in capacity to configure SIP Proxy ports in increments of 20.

9.3 Configuration Parameters

Before configuring your switches in Connect Director, you must determine the IP and MAC address assignments for each voice switch. Refer to the *MiVoice Connect Planning and Installation Guide* for more information about getting an IP address for each voice switch.

The items that you need before you begin configuring your switches are:

- Model of each voice switch you are configuring.
- Internet Protocol (IP) address of each switch.
- Ethernet address (MAC address) of each switch.

For 1U Full-Width and Half-Width voice switch models, the model of the switch and the Ethernet address (MAC address) of the switch are printed on the rear panel of each voice switch.

9.3.1 Setting Passwords and Designating Download Server for VA

On the Appliance Options page (**Administration** > **Appliances/Servers** > **Options**), you can designate the server from which software for virtual appliances is downloaded and you can set the ‘admin’ and ‘root’ passwords. For details on these options, see Fields on the Appliance Options Page.

Table 44: Fields on the Appliance Options Page

Parameter	Description
Download Mitel software to virtual appliances from	Select the source that Connect Director will use to obtain software downloaded to virtual appliances: • Mitel-maintained cloud mirror server URL • Connect Managing Server
“admin” password	The password for accessing the administrator account on appliances. The system allows the following characters: !#$%&'()* +,-.0123456789:;=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_/ `abcdefghijklmnopqrstuvwxyz{|}~ The system disallows the following characters: ? “ <>

Parameter	Description
“root” password	The password for accessing the root account on appliances. The system allows the following characters: !#$%&'()* +,-.0123456789:;=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_/ `abcdefghijklmnopqrstuvwxyz{|}~ The system disallows the following characters: ? “ <>

9.3.2 IP Phone, SIP, and Make Me Conference Support

If the system is using IP phones, SIP devices, or SIP trunks, you must allocate ports on voice switches. These configurations also apply to virtual phones and virtual trunks. Each allocated port supports one of the following configurations:

Table 45: Voice Switch Device Support

Voice Switch(es)	Ports	Configuration for Participant Max
Virtual Phone Switch	• 250 Built-in IP. • 1000 Configured max IP phone capacity. This setting must be configured by the system administrator. • 60 Configured max built-in Make Me conference ports.	—

Voice Switch(es)	Ports	Configuration for Participant Max
Virtual Trunk Switch	• 5 IP phones • 5 SIP trunks • 1 SIP media proxy • 100 SIP proxy ports (5 IP resources) • Make Me conference port **Note**: • Virtual trunk switches support only SIP trunks. • Built in SIP Trunk ports are not configurable.	—
SG 220T1/220T1A	• 5 IP Phone • 5 SIP trunk • 100 SIP proxy ports (5 IP resources) • Digital ports as SIP Trunks with Media Proxies • 20 for the SG 220T1 • 14 for the SG 220T1A with the option to use six additional analog ports for a total of 20.	SG Voice Switches support a maximum of eight conference participants on SG devices that have enough physical ports to support this configuration. —
SG90v/SG50v SG50/SG90	• 5 IP phones • 5 SIP trunks • Make Me conference port • 100 SIP proxy ports (5 IP resources) • SIP trunk with Media Proxy	
SG24A	• Make Me conference port	

Voice Switch(es)	Ports	Configuration for Participant Max
SG30	• 5 IP phones • 5 SIP trunks • 100 SIP proxy ports (5 IP resources) • SIP trunk with Media Proxy	
SGT1k	• Trunk	

ST50A/ST100A	• 1 Trunk
	• 1 SIP trunk with Media Proxy
	• 1 trade off conference port
	• 500 SIP proxy ports
	• Built-in IP phones:
	  • 50 for the ST50A
	  • 100 for the ST100A
	• Built-in Make Me conference ports:
	  • 6 for the ST50A
	  • 12 for the ST100A
		ST Voice Switches support a maximum of eight conference participants, and there is a one-to-one correlation between conference participants and conference ports. You define the participant maximum by user in the **Administration > Users > Class of Service > Telephony Features Permissions** page.
		
		To configure the maximum number of conference participants, you can use a combination of the built-in Make Me conference ports and the trade off conference ports. For example, to support eight conference participants on an ST50A, configure two trade off conference ports in addition to the six built-in Make Me conference ports.

Voice Switch(es)	Ports	Configuration for Participant Max

ST200/ST500	• SIP proxy ports:
	  • 500 for the ST200
	  • 1000 for the ST500
	• Built-in IP phones:
	  • 200 for the ST200
	  • 500 for the ST500
	• Built-in Make Me conference ports:
	  • 12 for the ST200
	  • 24 for the ST500
		For devices that do not have trade off conference ports, you can configure conferences that use the total number of built-in conference ports without exceeding the participant maximum. For example, to use all of the built-in conference ports on the ST200 and adhere to the participant maximum, you might configure one 8-port conference and one 4-port conference, or you might configure two 6-port conferences.

ST24A/ST48A	• 1 trade off conference	

ST1D/ST2D	• 1 Trunk
	• Digital ports as SIP Trunks with Media Proxy:
	  • 30 for the ST1D
	  • 60 for the ST2D	

ST100DA	• 100 built-in IP phones • 500 built-in SIP proxy ports • 12 Built-in Make Me conference ports • 30 digital ports as SIP Trunks with Media Proxy — You can use the analog ports as 8 additional SIP Trunks with Media Proxy • 1 Trunk • 1 trade off conference	

Make Me conference is used when a third-party SIP endpoint or Mobility is involved in a conference call with three or more participants (the maximum is eight participants). All the Make Me conference settings are valid in this situation. Although only three parties are involved in a conference call involving a SIP endpoint or Mobility, four Make Me conference ports are reserved as this is an enforced rule for all Make Me calls.

For information about the conference involving a SIP trunk, see Conferencing and SIP Trunks on page 676.

Make Me conference is also used when four or more IP400-Series and 6900-Series (6910, 6920, 6930, 6940, and 6970) phones are involved in a conference call.

If you do not reserve sufficient ports for IP phones on the voice switches, the MiVoice Connect system does not recognize some or possibly all IP phones. For more information about MiVoice Connect system requirements, see the *MiVoice Connect Planning and Installation Guide*.

9.3.3 Backup Operator

Voice Switches feature a backup operator in case the site operator is unreachable due to a network outage. For most switches, the backup operator is on the same port as the Power Fail Transfer port. To use this feature, select the port to match the switch model:

- Port 1 and 12 on the Voice Switch 50V.
- Port 1 and 12 on the Voice Switch 90V.
- Port 12 on the Voice Switch 30, Voice Switch 50, Voice Switch 90, and Voice Switch 220T1A.

9.4 Connect Director Pages for Voice Switches

After a voice switch has been installed, you can configure its parameters in Connect Director. This section describes the pages for configuring and monitoring voice switches. Subsequent sections provide details about the switch parameters.

For descriptions of the columns on the Platform Equipment page list pane, see Platform Equipment Page: List Pane.

Table 46: Platform Equipment Page: List Pane

Column Name	Description
Name	Name of the appliance.
Description	The type of appliance.
Sites	Name of the site where the appliance is located.
Server	Name of server configured to manage the appliance.

Column Name	Description
Database Server	Name of the database server the device uses for backup.
Type	Type of appliance.
IP Address	IP address of the appliance.
Secondary Address	IP address of the failover switch assigned to the selected switch.
MAC Address	MAC address of the appliance.
Serial Number	Serial number of the appliance.
IP Phones in Use	Number of IP phones connected through the appliance.
IP Phones Capacity	Number of IP phones the appliance can support based on the number of ports reserved for IP phones.
SIP Trunks in Use	Number of SIP trunks connected through the appliance.
SIP Trunk Capacity	Number of SIP trunks the appliance can support based on the number of ports reserved.
SIP Proxy Capacity	Number of SIP proxies the appliance can support.
Proxy Switch	Indicates if the selected appliance is configured to act as a proxy.
Conference Capacity	Number of ports reserved for conferences.
Hunt Groups	Number of hunt groups the appliance is hosting.

Column Name	Description
Jack-based Music	Indicates whether there is a jack-based music source for music-on-hold.
File-based Music	Indicates whether there is a file-based music source for music-on-hold.

9.4.1 Adding a New Switch at a Site

To add a new switch at a site, follow these steps:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment** > **New**.
3. Select the **Site**.
4. Select the appropriate switch in **Hardware type**.

   The country in which the site is located impacts the selections available in **Hardware type**. For example, if your site is located in the UK, BRI switches will be available in the **Hardware** type drop down, but if your site is located in the US, BRI switches are not available in the **Hardware** type drop down.
5. Complete step 3 in Configuring Primary Voice Switches and Service Appliances on page 162.

9.4.2 Configuring Primary Voice Switches and Service Appliances

The **Administration** > **Appliances/Servers** > **Platform Equipment** page lists the switches installed in the Mitel network. To access the page:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. In the **Platform Equipment** page that opens, select the switch you want to configure.

The **Platform Equipment** page provides voice switch information as described in Platform Equipment Page: Voice Switch/Service Appliance Parameters (Switches Page). Some of the voice switch information is configurable on the General tab, as described in Platform Equipment Page: General Tab Parameters (Switches Page).

Table 47: Platform Equipment Page: Voice Switch/Service Appliance Parameters (Switches Page)

Parameter	Definition
Name	Name of the switch or Service Appliance.
Description	Describes the appliance. This field is an optional entry that typically tells where the appliance is located or describes how it is used. For example, the appliance description might indicate the wiring closet where the appliance is located.
Sites	Name of the site where the appliance is located.
Server	Name of server configured to manage the appliance.
Database Server	Name of the database server the device uses for backup. This field applies only to virtual switches.
IP Address	IP address of the appliance.
Secondary IP Address	Secondary IP address for the appliance. This field is typically used only by the Headquarters server.
MAC Address	MAC address of the appliance.

9.4.3 Device Page

To view the device page, follow these steps:

1. Launch Connect Director.
2. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment** and select a switch.

The **Device** page allows you to configure the identification and operating parameters of switches installed in the Mitel network. Connect Director provides a specific page for each available switch that lists only the relevant parameters for that switch.

The device page typically consists of the **General, Switch**, and **Voice Application** (applicable to voice mail switches only), which allow you to configure the information described in the following tables:

- General Tab — Platform Equipment Page: General Tab Parameters (Switches Page) table in the General Tab Parameters on page 164 section.
- Switch Tab — Platform Equipment Page: Switch Tab Parameters (Switches Page) table in the Switch Tab Parameters on page 166 section.

9.4.3.1 General Tab Parameters

Platform Equipment Page: General Tab Parameters (Switches Page) lists the parameters on the General tab of the Platform Equipment page.

Table 48: Platform Equipment Page: General Tab Parameters (Switches Page)

Parameter	Definition
Name	Name of the voice switch.
Description	A short description of the switch. This optional entry typically describes where the switch is located or how it is used. For example, the switch description might indicate the wiring closet where the switch is located.
Site	Site where the switch resides. This is a read-only parameter. If you want to move the switch to another site, you must move all the associated users and trunks, delete the switch from the current site, and add the switch to the new site.
IP Address	IP address of the switch. If the Voice switch has a valid IP address, whether static or dynamic, and is present on the network, click **Find Switches**. Use the resulting dialog box to choose the correct switch, which will auto-complete the IP address and MAC address fields. If the switch is not discoverable by using the **Find Switches** button, you must manually enter in the IP address and MAC address of the switch.

Parameter	Definition
Fully Qualified Domain Name	FQDN of the switch. While this field is not required for switches, you might use DNS on your LAN and assign FQDNs to your switches to simplify the process of updating addresses in the event you replace the switch(es).
MAC Address	MAC address that is printed on the back panel of the switch. If the DHCP server is running and you clicked **Find Switches** to select an IP address, the switch's MAC address has already been added in this field. If the DHCP server is not running, you must manually enter the switch's MAC address in this field.
Server to Manage Switch	Server that manages the switch. Select the appropriate server from the drop-down list.
Caller's Emergency Service Identification (CESID)	Enter the Caller's Emergency Service ID to be used. For example, enter **+14085555555.** For more information, see Configuring a System for Emergency Calls on page 983. **Note**: • Whenever you enter the CESID, it will be saved in the database as entered and will not be formatted as per the Country-specific numbering plan. • (For US customers) If the third-party vendor trunks are not used for RAY BAUM conformance, then the CESID will be the telephone number that will identify the location and the callback number.
Use database on server	Allows you to select the server that hosts the database you want to use for the switch.

Parameter	Definition

Enable daily backup	When selected, allows you to specify a server to use for backup.
	
	Note:
	This field applies only to voice mail switches.
	
	Specify the following to enable backup in FTP or HTTPS server:
	• **IP address**
	  • For FTP server, enter the IP address of the FTP server to which the switch files must be backed up.
	  • For HTTPS server, enter the IP address of the HQ server to which the switch files must be backed up.
	• **FTP Port**—enter the port number that the switch is to use to communicate with the recipient FTP server. The default port number is 21.
	• **Directory**
	  • For FTP server, enter the path to the file on the FTP server to which you want to back up the switch files.
	  • For HTTPS server, enter the path to the file on the HQ server to which you want to back up the switch files.
	• **Username** — enter the user name that the appliance is to use to access the FTP server files for backup.
	• **Password**—enter the password that the switch uses to access the FTP server files for backup. Reenter the password again in the second field.
	• **Enable HTTPS** — select this check box to enable backup using HTTPS.

9.4.3.2 Switch Tab Parameters

Platform Equipment Page: Switch Tab Parameters (Switches Page) lists the parameters on the **Switch** tab of the Platform Equipment page.

Table 49: Platform Equipment Page: Switch Tab Parameters (Switches Page)

Parameter	Definition
Enable Jack Based Music on Hold	Enables the jack-based music-on-hold port. Select or clear this check box to enable or disable this feature. This parameter enables and disables jack-based music on hold for all trunks, including SIP trunks, and cannot be applied to a specific trunk type. Each site requires a separate music-on-hold source. To save bandwidth, music is not available between sites across the WAN. Enabling or disabling MOH for a switch affects only the local region associated with that switch. If MOH is enabled for a remote site but the headquarters switch has MOH disabled, then people calling into the headquarters switch will not hear music when placed on hold. Callers who dial into the remote site will, or course, hear music when placed on hold. A music source, such as a CD player, must be connected to the Music On Hold jack on the front panel of the switch. Jack Based Music On Hold Gain (-49 to 13): Specifies the gain (in dB).

Parameter	Definition
Enable File Based Music on Hold	Enables the file-based music-on-hold port. **Note**: This parameter is applicable only to voice mail switches. Select or clear this check box to enable or disable this feature. This parameter enables or disables file-based music on hold for all trunks, including SIP trunks, and cannot be applied to a specific trunk type. Each server can be a source of music on hold. If the Headquarters server has music on hold enabled, by default its associated sites and servers inherit this setting. To save bandwidth, music on hold can also be enabled on other servers. When a switch has file-based music on hold enabled, all sites associated with that switch have music on hold enabled. For example, if a switch at the Headquarters site has file-based music on hold enabled, this MOH source also applies to all child sites and servers. If a switch at a remote site has music on hold enabled, then any child sites associated with that switch can use that MOH source. Because the Headquarters server is the parent server, it cannot obtain its music-on-hold source from a switch at a remote site. For example, if MOH is enabled for a switch at a remote site but the Headquarters switch has MOH disabled, then people calling into the remote site hear music when placed on hold, but callers dialing into a switch at the Headquarters site do not hear music when placed on hold.

Parameter	Definition
Enable File Based Music on Hold (continued)	**Local Extension:** This is the extension used by the music-on-hold server. This extension is set manually when file-based MOH is enabled. **Maximum Concurrent Calls (1-9):** This is the maximum number of calls that can simultaneously access music on hold on this switch. This is a maximum limit, not a guaranteed number. (The concurrent call limit for the 90V switch is 1-9; for the 50V switch, the limit is 1-5.)
Built-in IP Phone Capacity	For a virtual phone (vPhone) switch, this is the number of IP phones that the virtual switch supports. This information is for reference only in the **Administration** > **Appliances/Servers** > **Platform Equipment** > **Switch page**.
Built-in Make Me Conference Capacity	For a virtual phone (vPhone) switch, this is the number of Make Me conferences that the virtual switch supports. This information is for reference only in the **Administration** > **Appliances/Servers** > **Platform Equipment** > **Switch page**.
Built-in SIP Trunk Capacity	For a virtual trunk (vTrunk) switch, the number of SIP trunks that the virtual switch supports. This number is calculated based on the number of CPU cores configured in the virtual machine, as follows: For a small virtual trunk switch with a capacity of 100 SIP trunks, the virtual machine has 4-7 CPU cores configured. For a medium virtual trunk switch with a capacity of 200 SIP trunks, the virtual machine has 8-15 CPU cores configured. For a large virtual trunk switch with a capacity of 2000 SIP trunks, the virtual machine has 16 or more CPU cores configured.

Parameter	Definition
Configured max IP phone capacity	Indicates how many IP phones can be assigned to the switch.
Use Analog Extension Ports as DID Trunks	Configures all analog extensions as analog DID trunks. SG 1U Half-Width analog extension ports cannot be individually configured as DID trunks, but by selecting this parameter, you can configure all analog extensions as analog DID trunks. When this parameter is selected, analog ports on the switch cannot be assigned to a user extension port.
Max SIP trunk capacity (G.711): 500/1000 with/ without advanced features	Allocates switch resources to support IP phones, SIP trunks, and SIP proxies on the Mitel network. Resource availability varies for each model. To allocate IP phone and SIP trunk resources, enter the desired number of resources in the data entry boxes. To determine the allocated SIP proxy resources, subtract the number of available resources from the sum of the entered numbers, and then multiply the difference by 20. For example, the SG90 provides 30 resources. If 5 resources are allocated for IP phones and 5 resources are allocated for SIP trunks, then 400 SIP proxy resources are available: (30 - (5+5))*20.

9.4.3.3 SGT1 Signaling Parameters

The Voice Switches page for SGT1 switches configures SGT1 circuit Layer 3 and Layer 1 parameters. These parameters are displayed for the SGT1k, SG220T1, SG220T1A, ST1D, and ST2D switches. For descriptions of the SGT1 signaling parameters, see SGT1 Signaling Parameters.

Table 50: SGT1 Signaling Parameters

Parameter	Definition
Enable jack-based music on hold	Enables/disables jack-based music on hold.

Parameter	Definition
Jack-based music on hold gain	Specifies the gain setting for jack-based music on hold.
Enable contact closure for paging	Enables/disables contact closure for paging. This feature can be used with the Paging Adapter. Refer to the *Mitel Paging Adapter Quick Install Guide* for information about this device.
Assign digital ports as SIP Trunks with Media Proxies	Assigns digital ports as SIP trunks with media proxies. SG switches support 20 digital ports as SIP trunks with media proxies. ST switches support 30 (ST1D) or 60 (ST2D) digital ports as SIP trunks with media proxies.
Layer 3 – Network Layer Parameters	
Protocol Type	Specifies the protocol type. From the drop-down list, select one of the following protocols: • CAS • ECMA QSIG Master • ECMA QSIG Slave • ISDN Network • ISDN User • ISO QSIG Master • ISO QSIG Slave
Central Office Type	Specifies the central office type. From the drop-down list, select one of the following central office types: • 4ESS • 5ESS • DMS-100 • NI-2 (National ISDN-2)

Parameter	Definition
Call by Call Service (4ESS only)	Specifies whether a user can access different services, such as an 800 line or WATS line, on a per-call basis. This parameter is available only when Central Office Type is set to 4ESS.
Enable Outbound Calling Name	Sends the caller name with the caller ID for outbound calls. The default is disabled.
Layer 1 – Physical Layer Parameters	
Clock Source	Configures the clock source for the switch. From the drop-down list, select either Master or Slave. Typically the switch is secondary to the central office. The default is Slave.
Framing Format	Configures the framing format for the SGT1 switch. From the drop-down list, select either ESF or D4, depending on the type of SGT1 service you receive. The default is ESF.
Line Code	Configures the line code for the SGT1 switch. Depending on the type of SGT1 service you receive, select either B8ZS or AMI. The default is B8ZS.
Line Build Out	Provides a list of SGT1 trunk line distances, specified in decibels (dB) and in feet. Select the appropriate value from the drop-down list.

9.4.3.4 SGE1 Signaling Parameters

The SGE1 Signaling parameters are displayed for the SGE1k and SG220E1 switches. Platform Equipment Page: SGE1 Signaling Parameters (Switches Page)describes the SGE1 signaling parameters.

Table 51: Platform Equipment Page: SGE1 Signaling Parameters (Switches Page)

Parameter	Definition
Layer 3 – Network Layer Parameters	
Protocol Type	Specifies the signaling protocol. From the drop-down list, select one of the following protocols: • ISDN User • ISDN Network • ISO QSIG Master • ISO QSIG Slave • ECMA QSIG Master • ECMA QSIG Slave
Central Office Type	Specifies the central office type. The SGE1 supports a single signaling type per country, which is typically Euro-ISDN(TBR4). This parameter is active only if Protocol Type is set to **ISDN User** or **ISDN Network**.
Enable Outbound Calling Name	Sends the caller name with the caller ID for outbound calls. The default is disabled.
Layer 1 – Physical Layer Parameters	
Clock Source	Configures the clock source for the switch. From the drop-down list, select either Master or Slave. Typically the switch is secondary to the central office. The default is Slave.
Framing Format	Specifies whether the framing format is enabled or disabled. SGE1 switches support the CRC-4 framing format.

9.4.3.5 BRI Signaling Parameters

The BRI signaling parameters are displayed for switches that support BRI. Four BRI spans are displayed, but the 30 BRI supports only one BRI span. Platform Equipment Page: BRI Signaling Parameters (Switches Page) describes the BRI signaling parameters.

Table 52: Platform Equipment Page: BRI Signaling Parameters (Switches Page)

Parameter	Definition
Analog Ports	
Port Type	Configures the port resources. From the drop-down, select one of the following options: • Available: Configures the port resources to support either an extension port or DID trunk. Port capabilities depend on the switch model. • Trunk: Configures the port as an analog trunk assigned to the Trunk Group specified by the Trunk Group parameter. • 5 IP Phones: Configures the resource to support 5 IP phones. • SIP Trunk with Media Proxy: Configures the resource to support a single SIP trunk with a media proxy. Select this setting when connecting the SIP trunk to an ITSP. • 5 SIP Trunks: Configures the resource to support 5 SIP trunks. Select this option when using the SIP trunk as a tie trunk or when connecting it to Mobility. • 100 SIP Proxy: Configures the resource to support 100 SIP proxies.
Trunk Group	Specifies the Trunk Group to which the port is assigned. This parameter is available only when Port Type is set to Trunk.
Description	Lists a descriptive name for the switch port. Description is an optional field.

Parameter	Definition
Jack Number	Lists the patch-panel jack number to which the port is connected. Jack Number is an optional field.
Tx Gain (db)	Specifies the gain added to received digital signals. The default is 0 dB.
Rx Gain (db)	Specifies the gain added to transmitted digital signals. The default is 0 dB.
Location	Comment field option for typing location information about a port.
Caller's emergency service identification (CESID)	Enter the CESID for the analog port. To comply with RAY BAUM, you must provide the CESID for the analog port. **Note**: • Whenever you enter the CESID, it will be saved in the database as entered and will not formatted as per the Country-specific numbering plan. • (For US customers) If the third-party vendor trunks are not used for RAY BAUM conformance, then the CESID will be the telephone number that will identify the location and the callback number.
Fill Down	Duplicates the contents of the first row of the data entry field in all other rows. The channel number, in parenthesis, is appended to the contents of the Description field.
Digital Ports	

Parameter	Definition
Enable Span as BRI	Activates the corresponding Digital Channels as a BRI span. When this parameter is not selected, the Channel resources are available for reallocation to support IP phones, SIP trunks, or SIP proxies.
Layer 3 Parameters – Network Layer	
Protocol Type	Specifies the signaling protocol. • ISDN User and ISDN Network are ISDN signaling protocols. • QSIG is an ISDN based signaling protocol used for signaling between PBXs in a private network.
Central Office Type	The BRI supports a single signaling type per country, which is typically Euro-ISDN. This parameter is active only if Protocol Type is set to ISDN User or ISDN Network.
Enable Outbound Calling Name	Sends the caller name with the caller ID for outbound calls. The default is disabled.
Layer 2 Parameters – Data Link Layer	
Signaling	Specifies the signaling type. From the drop-down list, select either Point-to-Point or Point-to-Multipoint.
Layer 1 - Physical Layer Parameters	
Clock Source	Configures the clock source for the switch. From the drop-down list, select either Master or Slave. Typically the switch is secondary to the central office. The default is Master.

Parameter	Definition
Clock Priority	• Never • High • Medium • Low • Lower
Digital Channels – For switches that provide digital channels	
Port Type	Configures the port resources as follows: • Available: Indicates that the channel resources is available for assignment. • Trunk: Configures the port as an digital trunk assigned to the Trunk Group specified by the Trunk Group parameter. • 5 IP Phones: Configures the resource to support 5 IP phones. • SIP Trunk with Media Proxy: Configures the resource to support a single SIP trunk with a media proxy. Select this setting when connecting the SIP trunk to an ITSP. • 5 SIP Trunks: Configures the resource to support 5 SIP trunks. Select this setting when using the SIP trunk as a tie trunk or when connecting it to Mobility. • 100 SIP Proxy: Configures the resource to support 100 SIP proxies. • Unavailable: Indicates that digital channel is not available.
Trunk Group	Specifies the Trunk Group to which the port is assigned. This parameter is available only when Port Type is set to Trunk.
Description	Optional comment field that lists a descriptive name for the switch port.

Parameter	Definition
Jack Number	Optional comment field that can contain the patch-panel jack number to which the port connects.
Tx Gain (db)	Specifies the gain added to received digital signals. The default is 0 dB.
Rx Gain (db)	Specifies the gain added to transmitted digital signals. The default is 0 dB.
Fill Down	Duplicates the contents of the first row of the data entry field in all other rows. The channel number, in parenthesis, is appended to the contents of the Description field.

9.5 Failover for IP Phones: Spare Switch

To ensure high availability of IP phones, MiVoice Connect provides failover mechanisms, as follows:

- One mechanism is the redistribution of IP phone service by the Headquarters server after a switch fails. This mechanism involves resource planning and configuration. Though it does not involve extra equipment, it does require enough available capacity on the remaining active voice switches.
- The other mechanism involves an extra voice switch that is reserved as a *spare switch*.

IP phones can get immediate reassignment when the voice switch to which they are assigned does not respond. For details about how legacy and 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones behave during failover, see Call Continuation During Failover on page 294.

If resources are insufficient and a *spare switch* is available, the Headquarters server activates the spare switch as a site resource and reassigns the remaining IP phones to it. The Headquarters server records these failover transactions so an administrator can manually restore regular service after the problem is corrected. If resources are still insufficient even after the Headquarters server activates a spare switch, the affected IP phones remain unavailable to users until the problem is solved.

Failover for IP phones is transparent to the end user. A keep-alive function ensures that failover can occur without users taking remedial actions on their phones and even during

a phone call. If the user tries to use the phone before failover takes place, the phone automatically queries the Headquarters server for reassignment when the assigned switch does not respond. When implemented, the failover transaction occurs within seconds. However, if resources are not available, failover cannot occur and the user is unable to use the phone.

Upon a switch failure, the phones are reassigned in the order that they notify the Headquarters server of the switch's unavailability. If the resources are available, the network's failover operation takes up to about four minutes after initial detection of a voice switch failure.

The MiVoice Connect system provides for two levels of switch failover to assure high availability of IP phones. The first level involves setting aside capacity on site switches to handle failover situations. This method is referred to as N+1. In N+1 applications, you deploy more switches (hence ports) than your absolute need. The MiVoice Connect system automatically implements load balancing when it assigns IP phones to switches so that the load is always evenly distributed. An example of an N+1 application is the following:

A site has 99 users on 3 Voice Switch 50s. The configuration on each switch assigns 33 IP phones and keeps 17 ports in reserve (33 + 17 = 50). If one of the switches fails, the Headquarters server reassigns the 33 IP phones to the 2 functioning switches.

The second level of failover involves a spare switch that provides failover protection. Certain switch models can serve as a spare, and the MiVoice Connect system does not assign IP phones to these spare switches during normal operation.

If a voice switch fails and the Headquarters server cannot reassign all of the IP phones to the remaining switches at the site, the Headquarters server activates the spare switch at the affected site and reassigns the remaining IP phones from the failed switch to the spare. Reassignment should be a temporary state—until the problem that triggered that failover is solved.

The spare switch provides basic telephony functionality and cannot support such functions as hunt groups, trunk access, Backup Auto-attendant, analog extensions, trunks, media proxy, Make Me conference ports, and so on. However, Extension Assignment is supported.

Spare switch failover support is hierarchical. Spare switches provide failover support for IP phones installed on the same site only. Moreover, spare switches provide failover support for IP phones at or below the level where the switch is installed. This means that a switch installed on a child site cannot be used to provide failover for IP phones installed on the parent site or any site connecting through the parent site. It can be used to provide failover for child sites below it in the hierarchy. Indeed, when necessary, the system searches the entire, relevant hierarchy until it finds an available spare switch it can use for failover. You can also install spare switches on the Headquarters server sites to provide universally accessible failover for all sites on the system.

Voice Switches that Can Serve as Spare Switches on page 180 describes how to configure spare switches.

9.5.1 Voice Switches that Can Serve as Spare Switches

The following Voice Switches can serve as spare switches:

- Voice Switch ST50A/ST100A
- Voice Switch ST200/ST500
- Voice SwitchST100DA
- Voice Switch 50
- Voice Switch 90
- Voice Switch 220T1
- Voice Switch 220E1
- Voice Switch 90BRI
- Voice Switch 220T1A
- Voice Switch 30
- Voice Switch 30BRI
- vPhone Virtual Switch

Note:

- Voicemail switches (such as the 90V and the 50V) cannot serve as spare switches.
- The vTrunk Virtual Switch cannot be a spare switch.
- Spare switches cannot change languages while they are carrying traffic. Language incompatibilities are indicated by a **Firmware upgrade available** message when the switch is configured for a site with a different language.

9.5.2 Adding a Spare Switch to the System

This section describes how to configure a switch to be a spare. The physical installation of a spare switch is the same as the installation of a primary switch. (For details about how to install primary and spare switches in a Mitel network, refer to the *MiVoice Connect Planning and Installation Guide*).

The information required to configure a spare switch is as follows:

- IP address for the spare switch
- Ethernet address of the switch (located on a label on the back of the switch)

- Name of the server to manage the switch

To configure a voice switch as a spare:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Spare Equipment**. The **Spare Equipment** page opens.
3. Click **New**.
4. Select the **Site**.
5. Select the switch type to add as a spare by selecting a switch model in the **Hardware type** drop-down list. The **Edit Switch** page opens.
6. In the **Name** field, enter the name to identify this switch in the system.
7. In the **Description** field, enter a description for this switch.
8. In the **IP Address** field, enter the IP address assigned to the switch. If the switch is located on the same network segment as the Headquarters server, you can use the **Find Switches** function to locate the IP address.
9. In the **MAC address** field, enter the Ethernet address for the switch.
10. In the **Server to manage** switch field, select the server that you want to manage the switch.

Note:

- We recommend that you do not select a server that has Music On Hold enabled to manage the spare switch. Doing so could mean sending MOH across the WAN, which Mitel does not support.
- We recommend that you do not select a switch with CESID configured. The spare switch can be temporarily deployed in a remote location.

11. Click **Save**.

Note:
Current Site is the site where the switch is currently being used to provide failover. If the switch is not currently being used, this field is empty.

9.5.2.1 Spare Switches List Pane and Parameters

For descriptions of the columns on the Spare Switches page, see Spare Switches Page: List Pane.

Table 53: Spare Switches Page: List Pane

Column Name	Description
Name	Name of the switch.
Description	The type of switch.
Home Site	Home Site is the location where the switch is configured.
Current Site	Current Site is the site where the switch is currently being used to provide failover. If the switch is not currently being used, this field is empty.
Server	Name of server configured to manage the switch.
Type	Type of switch.
IP Address	IP address of the switch.
MAC Address	MAC address of the switch.
Serial Number	Serial number of the device.
IP Phones in Use	Number of IP phones connected through the switch.
IP Phones Capacity	Number of IP phones the switch can support based on the number of ports reserved for IP phones.

9.5.2.2 General Tab

Spare Swiches Page: General Tab Parameters describes the parameters on the General tab of the Spare Switches page.

Table 54: Spare Swiches Page: General Tab Parameters

Parameter	Definition
Site	Select the site for the spare switch.
Hardware type	Select the switch type.
Name	Name of the voice switch.
Description	A short description of the switch. This optional entry typically describes where the switch is located or how it is used. For example, the switch description might indicate the wiring closet where the switch is located.
Current Site	Current Site is the site where the switch is currently being used to provide failover. If the switch is not currently being used, this field isempty.
IP Address	IP address of the switch. If the Voice switch has a valid IP address, whether static or dynamic, and is present on the network, click ‘Find Switches’. Use the resulting dialog box to choose the correct switch, which will auto-complete the IP address and MAC address fields. If the switch is not discoverable by using the ‘Find Switches’ button, you must manually enter in the IP address and MAC address of the switch.
MAC Address	MAC address that is printed on the back panel of the switch. If the DHCP server is running and you clicked Find Switches to select an IP address, the switch’s MAC address has already been added in this field. If the DHCP server is not running, you must manually enter the switch’s MAC address in this field.

Parameter	Definition
Server to Manage Switch	Server that manages the switch. Select the appropriate server from the drop-down list.
IP Phone Capacity	IP Phone capacity of the spare switch. This field is read only.

9.5.3 Enabling IP Phone Failover

You must configure the system to allow IP phones to failover. To set the parameter to allow IP phones to failover, do the following:

1. Launch Connect Director.
2. Click **Administration** > **Telephones** > **Options**.

   The IP Phone Options page appears.
3. Select the **Enable IP Phone Failover** check box.
4. Click **Save**.
5. For Mitel 100-Series, 200-Series, 500-Series, and 600-Series IP phones, reboot the phones to apply the new setting for the parameter.

9.5.4 Temporarily Disabling IP Phone Failover

For some maintenance tasks, you temporarily disable IP phone failover (such as for system-wide maintenance work).

1. Launch Connect Director.
2. Click **Maintenance** > **Status and Maintenance** > **System**.
3. Select the **Temporarily disable IP phone failover across sites** check box. When this feature is enabled, spare switches do not fail over throughout the system.

Note:
Ensure to reverse this process to enable IP phone failover when the maintenance task is finished.

9.5.5 Performing a Manual Fail Back

The Maintenance – Switches Summary page displays a section listing the Spare Switches at the specified site. This section indicates the activity level of the spare switch and, when active, the site where the spare switch is deployed.

Manual failbacks are performed on the Maintenance – Switches Summary page by accessing the drop-down list for the desired switch and selecting **Fail Back**.

9.5.6 Restoration

The spare switch is designed as a temporary measure to ensure that IP phone users have basic phone connectivity if their primary switch fails. To ensure that users have their full connectivity, you must repair or replace the failed primary switch as soon as possible. This section describes the following aspects of restoring normal operation after a failover occurs:

- How to re-assign the original primary switch profile to a new switch.
- How to move IP phones from the spare switch to the restored primary switch.
- How to fail back the spare switch to the spare state.

9.5.6.1 Reassigning the Primary Switch Profile to a Replacement Switch

If you must physically replace a primary switch that fails, you can re-assign the original switch profile to the new physical switch rather than create a new profile. This section describes how to re-assign the switch profile.

9.5.6.1.1 Requirements

- Obtain a replacement switch that has the same capabilities as the failed switch.
- Physically install the replacement switch on the same network as the old switch.
- Assign the new switch an IP address. Refer to the *MiVoice Connect Planning and Installation Guide* for more information about IP address assignment.
- Unplug the port connections (telephones, trunks) from the existing voice switch and plug them into the new voice switch.

To reassign the switch profile:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.

3. Click the name of the voice switch to replace.

   The **Edit Switch** page for the switch appears.
4. Do one of the following:

   - In the **IP address** field, enter the IP address (or Ethernet address) of the new switch that is replacing the inoperative switch.
   - Click **Find Switches**, and then select the new voice switch.
5. Click **Save**.

The switch might take up to two minutes to come on-line.

Note:
You can use Diagnostics and Monitoring to confirm that the new voice switch is online.

9.5.6.2 Moving IP Phones to the Primary Switch

1. Launch Connect Director.
2. Click **Administration** > **Telephones** > **Telephones**. The **Telephones** page opens.
3. In the **Move to Site** field, select the site where the failover has occurred and you want to perform restoration.
4. In the **and switch** field, select the switch you want to move the phone to.

Note:
You can select multiple phones to move at one time. The phones do not have to be registered to the same switch.

5. Click **Move**.

   The phones are moved to the target primary switch.

Note:
Calls that are currently in progress are dropped during the move to the target switch.

9.5.6.3 Failing Back the Spare Switch

After you move the IP phones to the primary switch on the site, you must manually fail back the spare switch. To fail back the spare switch:

1. Launch Connect Director.
2. In the navigation pane, click **Maintenance** > **Status and Maintenance** > **Appliances**. The **Appliances** page opens.
3. In the list pane, select the spare switch to fail back.
4. In the **Command** drop-down list, select **Failback From Spare**.

Note:
The failback process starts. The process takes a few minutes to complete and includes rebooting the spare switch. When the process is complete and successful, the spare switch returns to the spare state.

To verify that the switch has returned to the spare state, do the following:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Spare Equipment**. The **Spare Equipment** page opens.
3. Verify the following:
   - The **Current Site** column is empty.
   - The **IP Phones in Use** column lists zero (0).

9.6 T.38 Support on Switches

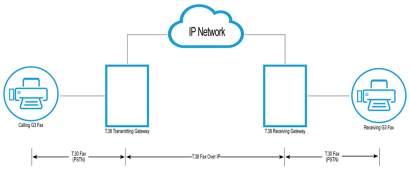
T.38 works in conjunction with SIP and is implemented as a fax codec on Mitel's half-width voice switches and virtual voice switches. (SG generation full-width voice switches do not support T.38, but the ST generation full-width switch does (ST48A)). T.38 can be used on SIP-enabled voice switches (if the switch supports T.38), servers, and SIP endpoints.

On all switches, T.38 functions as a gateway.

Note:
If a switch does not support T.38, the MiVoice Connect system can translate T.38 for that switch. If a switch does not support T.38 or is configured not to use T.38, it can use pass-through (voice band data) to transport faxes.

The following figure shows how T.38 supports fax transmission between two sites.

Figure 7: T.38 over IP Network Connecting to Fax Machines



9.6.1 Usage

The fax capability is enabled by default on the half-width switches. Only the UDPTL format (UDP packet for transporting faxes) is supported. Fixed redundancy is available on all calls.

Mitel implements T.38 through a gateway on the switches. Parameters for the T.38 UDPTL packets (those UDP packets used to transport fax) are negotiated through the session description protocol (SDP). The negotiation follows the offer/answer exchange model for SIP between Voice Switches SIP trunks and a SIP-based, third party device, such as an IP fax extension.

Between voice switches, the system uses ShoreSIP. The system uses SIP only if SIP-based, third-party, end points or SIP trunks are encountered about the fax codec list—the built-in fax codec list (high bandwidth and low bandwidth) are enough. Mitel considers the fax codec list to be adequate and, therefore, customers should not need to add to it.

Note:
To connect a T.38 fax server to a MiVoice Connect system, one of the following two requirements must be met:

- The T.38 fax server must be able to fall back to G.711 clear channel.
- If the fax server is T.38 only, all the switches within the system must be upgraded to one of the supported voice switches, otherwise, fax calls from those switches always fail. For a list of voice switches, see the *Voice Switches section* in the *MiVoice Connect Planning and Installation Guide*.

Note:
Ensure that fax machines or modems are connected only to extensions with one of the following labels:

- Fax machine
- Fax server
- Non-T.38 fax server
- Non-T.38 data terminal

An extension that is labeled as a fax server can also be used as a site-specific fax redirect destination. Be sure that extensions designated as fax extensions are not fowarded to other phones or trunks that use the Anyphone feature, otherwise fax operation is impacted.

9.6.2 Important Considerations

T.38 support is subject to the following considerations:

- The following Voice Switches do not support T.38. For these and older switches, G711/L16 clear channel is used for fax purposes.
  - SG40
  - SG60
  - SG120
  - SG220T1
  - SG220E1
  - SG24A
  - ST200
  - ST500
- The fax machine/fax server behind the Mitel PBX should disable the V.34 feature to keep the fax from using G711/Linear clear channel for better performance.
- V.34 Faxes are not supported.
- Mitel supports only T.38 in UDPTL form. T.38 calls in RTP or TCP form are not supported.
- Mitel does not support either IP media or RFC2833-based fax tone detection (in RFC2833, Mitel only supports DTMF but no named telephony events), therefore Mitel cannot detect a fax tone coming from an SIP end-point. The exception is a SIP connection that is established with a physical port on a switch. In this case, the switch can detect a fax tone from the SIP endpoint and either switch to fax mode or redirect the call.

- Mitel depends on fax CNG tone detection or T.38 invite to redirect an incoming fax call. If the fax connection is established with one SIP based endpoint (such as SIP extension or SIP trunk), Mitel depends on SIP invite to either establish a fax connection or redirect the call to a pre-configured fax device.
- T.38 is not supported on SIP-BRI.
- Mitel supports modem speeds up to 9600 at V.29. Mitel does not support V.17 or V.34.

9.6.3 Enabling T.38 on a Switch

Note:
T.38 must be enabled on a switch only if custom codec lists have been created.

T.38 is the first codec in the list of codec members for “Fax Codecs - Low Bandwidth” and “Fax Codecs - High Bandwidth” in Connect Director.

“Fax Codecs - High Bandwidth” is the default codec list selected when a site is created.

For more information on the default codec lists available from Mitel, see Enabling Intersite Video on page 447.

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Call Control** > **Codec Lists**.

   The **Codec Lists** page opens.
3. In the **Description** column, select the fax codec profile for which you want to enable T.38 support or click **New** to create a new codec profile.
4. Ensure that T.38 appears in the **Selected** field in the position that reflects your preference for the order the switch should use for fax calls.
5. Click **Save**.
6. Click **Administration** > **System** > **Sites**.

   The **Sites** page is displayed.
7. Select the site on which you want to enable the T.38 codec.

   The **Edit Site** page opens.
8. In the **Fax and modem Calls** field, select a fax profile in which the T.38 codec is enabled.
9. Click **Save**.

9.6.4 Third-Party T.38 Configuration Support

Mitel T.38 implementation also supports GFI Software/Brooktrout SR140. For the configuration procedure, see the following Mitel application note:

ST10238: How to configure GFI Software/Brooktrout SR140 with the Mitel System

For more information about configuring additional Mitel-supported, third-party solutions, contact the Mitel Innovation Network Partner Program at the following URL:

https://www.mitel.com/developer/mitel-solutions-alliance/tech-connect

Voicemail Model Switches 10

This chapter contains the following sections:

This chapter describes the voicemail switches that support voicemail services. In addition to the regular voice switching functionality, these voice switches have a subset of the server functionality that Mitel provides.

10.1 Overview

The voicemail-enabled switches are specially-equipped voice switches that provide voicemail services and access to auto attendant menus for telephones that the switch is hosting. These voicemail-enabled switches store voicemail on Compact Flash (CF) cards. They provide local access to voicemail.

The Auto Attendant menus, greetings, and prompts reside in permanent flash memory. For routine protection of voice mail, backup and restore tasks are configurable through Connect Director. If a switch becomes disabled, the information on the CF card can migrate to another switch of the type.

V Model Switches differ from other Voice Switches in the following ways:

- V Model switches have a slot on the side of the chassis for accessing the CF card.
- V Model switches provide Voicemail and auto attendant services normally provided by the Main Server or a Distributed Server.
- V Model switches run on Linux.
- V Model switches do not support Simplified Message Desk Interface (SMDI).

10.2 Functional Description

This section outlines the capacities and capabilities of the voicemail-enabled switches. These voice switches are similar to other 1-U Half Width Voice Switches, but they also have permanent flash and Compact Flash memory to provide a subset of the sever functions of voicemail, automated scripts, and other services.

10.2.1 Switch Capacity of a Voicemail-Enabled Switch

This section lists the capacities of the voicemail-enabled switches. It contains:

- Some network-wide values
- Voice switch capacity
- Server capacity

The global capacity of these voicemail-enabled switches is as follows:

- Maximum voicemail-enabled switches in a Mitel network: 500
- Maximum simultaneous calls to voice mailboxes on a switch: 9
- Maximum CF card capacity in the current release: 2 GB

A voicemail-enabled switch utilizes only the codecs that reside on that switch. As with other 1-U, half-width switches, the switch's codecs cannot serve as a G.729 proxy.

10.2.2 Voice Switch Functions

The voicemail-enabled switches provide the same types of voice services as other 1-U, half-width switches. Voice Switch Capacities lists the voice switching capabilities for each model of voicemail-enabled switch.

A voicemail-enabled switch utilizes only the codecs that reside on the switch. As with other 1-U half width switches, the on-board codecs cannot serve as a G.729 proxy.

Note:
A voicemail-enabled switch has two analog ports on the faceplate. The upper port accepts line input from a radio or CD player; the lower port can drive an amplifier of a paging system.

Table 55: Voice Switch Capacities

Switch Element	90V	90BRIV	50V
Analog telephony	12 ports • 8 ports support trunks • 4 ports configurable as extensions or DID trunks	4 extension ports	6 ports • 4 ports support trunks • 2 ports configurable as extensions or DID trunks
IP and SIP resources Built-in capacity and reallocated telephony resources are in upper and lower part of switch configuration screen	Built-in capacity, independent of telephony support, any combination of: • 30 IP phones • 30 SIP trunks • 600 SIP proxies Requires reallocation of telephony resources: • 90 IP Phones • 90 SIP trunks • 1800 SIP proxies max.	Built-in capacity, independent of telephony support, any combination of: • 30 IP phones, 30 SIP trunks or • 600 SIP proxies Requires reallocation of telephony resources: • 90 IP Phones, or: • 90 SIP trunks, or: • 1800 SIP proxies max.	Built-in capacity, independent of telephony support, any combination of: • 20 IP phones, 20 SIP trunks or • 400 SIP proxies Requires reallocation of telephony resources: • 50 IP Phones • 50 SIP trunks • 1000 SIP proxies max.
Voicemail boxes	90	90	50
Digital telephony	N/A	4 BRI ports; 8 channels Each port supports 1 BRI span, which consists of 2 channels.	N/A

Switch Element	90V	90BRIV	50V
Audio format	8-bit WAV (µ-law)	8-bit WAV (µ-law)	8-bit WAV (µ-law)
Music on Hold	Supported	Supported	Supported
Paging support	Yes	Yes	Yes
Codecs	G.711 and G.729 Can negotiate: • ADPCM (DVI/8000) • Linear (L16/8000)	G.711 and G.729 Can negotiate: • ADPCM (DVI/8000) • Linear (L16/8000)	G.711 and G.729 Can negotiate: • ADPCM (DVI/8000) • Linear (L16/8000)

10.2.3 Server Functions

A voicemail-enabled switch supports a subset of the server functions that a Headquarters or Distributed Voice Server provides. The sub-sections that follow describe the server features of the voicemail-enabled switches.

10.2.3.1 Voicemail Capacity

A voicemail-enabled switch provides voicemail services to local users under normal conditions. If resource utilization reaches its limit, a DVS can provide services to the users.

Switch functions and Server routines run under Linux. The voicemail-enabled switches use Qmail instead of SMTP.

The total time for voicemail recordings depends on the capacity of the CF card. A 1-GB CF card can hold up to 1500 minutes of audio. Therefore, each user on a Voice Switch 90V can have about 15 minutes of voicemail.

When a user requests voicemail through an IP phone, a voicemail-enabled switch provides the messages directly to the IP Phone. In contrast, when a user requests voicemail through the computer, the voicemail-enabled switch first sends the message to a Headquarters or DVS. The server sends the message to Connect client on the user's computer.

When the CF card is full, callers cannot leave a voice message and instead hear a recorded message that the mailbox is full.

Note:

When callers try to leave voicemail messages or users attempt to call an auto attendant, a recording plays stating that there is no space available and a message cannot be left. In the voicemail log for calls, a message indicates the current percentage of disk space used.

Example:

```
09:12:20.017 ( 4600: 5096) [MS]
VMSystem::getAvailableMessageStores , maxMessageStores = 1

09:12:20.017 ( 4600: 5096) [MS] Calling GetDiskFreeSpaceEx,
Path= C:\Shoreline Data\Vms\Message

09:12:20.017 ( 4600: 5096) [MS] GetDiskFreeSpaceEx method
returned, FreeSpace=2526 MB

09:12:20.017 ( 4600: 5096) [MS]
VMSystem::getAvailableMessageStores ,FreeSpace.QuadPart <
MIN_DISKSTORAGE_FOR_RECORD returning -1, FreeSpace =2526 MB,
currPercentUsed=96

09:12:20.017 ( 4796: 4992) [PM] VoiceApp::recordMessage,
messageStoreIndex = -1

09:12:20.017 ( 4796: 4992) [PM] PM: Play phrase 80 lang 1
```

Recordings are no longer created if 95% or more of disk space has been used.

Clearing space on the drive will correct this issue.

10.2.3.2 File-Based Music on Hold Capacity

A voicemail-enabled switch can provide file-based MOH services.

10.2.3.3 Conferencing on a Voicemail-Enabled Switch

Linux-based voicemail-enabled switches can conference up to eight people in one conversation, very much like the VxWorks-based regular switches. To host more than

one conference at the same time, the switch must reserve more of the configurable DSP computing power.

10.2.3.4 Auto-Attendant Menus

Each voicemail-enabled switch receives a copy of the system's auto-attendant menus.

10.2.3.5 Recorded Name Storage

When configuring their voicemail, users can record their name to an audio file. The recording is part of the greeting to callers. The switch stores the greetings only for the users whose mailbox resides on the switch. (Headquarters and DVSs keep the recorded name files for the other users.) When a voicemail-enabled switch requires an audio file that it does not have, it gets the file from the Headquarters server or a DVS.

10.2.3.6 Voicemail Prompts

All non-English voicemail prompts reside on the Headquarters Server and simultaneously on all Distributed Servers. A voicemail-enabled switch can keep a subset of the prompts. It can hold prompts in the local, default language and three other languages.

10.2.4 Connectivity Requirements

Voicemail and Auto-attendant availability requires connectivity to the boot-time server so the switch can read the configuration database on the Headquarters server. Voicemail and the Auto-attendant on a voicemail-enabled switch are not active until it connects to the Headquarters server. The voicemail-enabled switches do not require a restart to enable voicemail support and Auto-attendant if the initial connectivity was established after the initial boot.

Voicemail and auto attendant services require that the switch has connectivity with a Network Time Protocol (NTP) server.

System backup requires FTP or HTTPS server connectivity. When backing up data, it goes to the Main Server or to any computer with FTP or HTTPS server capabilities that supports RFC 959, the MDTM command, and the SIZE command.

Although a DVS can manage a voicemail-enabled switch, the switch applications still need access to the database on the Headquarters server. Examples of the applications that run on a voicemail-enabled switch are voicemail and the Telephone Management System (TMS).

Personal Connect client connects only to the Main Server or a Distributed Server, even for users whose host port is on a voicemail-enabled switch.

10.3 Implementing Voice Switch Functionality

This section describes how to implement the voice switch functionality on the switches that also host email. Connect Director supports the following tasks:

- Adding a new voicemail model switch to a Mitel server, described in Adding and Configuring a Voicemail-Enabled Switch on page 198
- Configuring voice mail, described in Configuring Voice Mail on page 207
- Specifying Linux root and administrator passwords, described in Specifying Root and Administrator Passwords for CLIs on page 209
- Specifying maximum size and age of log files stored on the CF card, described in Modifying the Log File Size and Age on page 218
- Configuring automatic backup of voice mail , described in Configuring Automatic Backup for a Switch on page 210
- Monitoring memory usage on the CF card, described in Monitoring Memory Usage for a Voicemail Model Switch on page 217

10.3.1 Adding and Configuring a Voicemail-Enabled Switch

After physically connecting a voicemail-enabled switch to the network, the system administrator adds the switch to the system through Connect Director.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click **New**. The **General** tab in the **Details** pane displays the parameters for the new switch.
4. In the **Site** list, select the site where you want to add the switch.
5. In the **Hardware type** list, select the model of the switch to add to the site.
6. Review the parameters on all of the tabs in the details pane, and specify values as appropriate. For more information about all of the voicemail-enabled switch parameters on the various tabs of the **Details** pane, see Voicemail Model Switch Parameters on page 199. See Configuring Primary Voice Switches and Service Appliances on page 162 for instructions on configuring a Voice Switch.

The switch configuration window for Voice Model Switches contains voice mail and back-up options in addition to voice switch options available for other switches. See Configuring Voice Mail on page 207 for instructions on configuring voice in mail. See Configuring Automatic Backup for a Switch on page 210 for instructions on configuring system back-up.

10.3.1.1 Voicemail Model Switch Parameters

You can configure parameters for a voicemail model switch on the following tabs, which you can access on the details pane for a particular switch:

- General Tab on page 199
- Voice Application Tab on page 201
- Switch Tab on page 203

10.3.1.1.1 General Tab

General information about a voicemail model switch is provided on the **General** tab on the **Platform Equipment** page.

Table 56: Platform Equipment Page: General Tab (Voicemail Model Switch)

Parameter	Definition
Name	Specifies the name of the voicemail model switch.
Description	Specifies a short description of the switch. This optional entry typically describes where the switch is located or how it is used. For example, the switch description might indicate the wiring closet where the switch is located.
Site	Specifies the site where the switch is located. This is a read-only parameter. If you want to move the switch to another site, you must move all the associated users and trunks, delete the switch from the current site, and add the switch to the new site.
IP address	Specifies the IP address of the switch. If the DHCP server is running, click **Find switches** and use the resulting dialog box to select an IP address. This also adds the switch's **MAC address** in the MAC Address field. If the DHCP server is not running, you must manually enter the switch's IP address and MAC address.

Parameter	Definition
MAC address	Specifies the MAC address of the switch. The MAC address is printed on the back panel of the switch. If the DHCP server is running and you clicked **Find switches** to select the IP address, the switch's MAC address has already been added in this field. If the DHCP server is not running, you must manually enter the switch's MAC address.
Server to manage switch	Specifies the server that manages the switch. Select the appropriate server from the drop-down list.
Caller's emergency service identification (CESID)	Specifies the phone number sent to the service provider when an emergency services number is dialed from a user extension. For more information, see Configuring a System for Emergency Calls on page 983. **Note**: Whenever you enter the CESID, it will be saved in the database as entered and will not be formatted as per the Country-specific numbering plan.
Use database on server	Specifies the server that hosts the database you want to use for the switch.
Enable daily backup	Select this check box to enable daily backup of voice mail and auto-attendant data. See Configuring Automatic Backup for a Switch on page 210for more information about this feature.
Start time	Specifies the start time of the daily backup. The default start time is 2:00 AM.

Parameter	Definition
IP address	• For FTP server, enter the IP address of the FTP server to which the switch files must be backed up. • For HTTPS server, enter the IP address of the HQ server to which the switch files must be backed up.
FTP port	Specifies the port number that the switch uses to communicate with the recipient FTP server. The default port number is 21.
Directory	• For FTP server, enter the path to the file on the FTP server to which you want to back up the switch files. • For HTTPS server, enter the path to the file on the HQ server to which you want to back up the switch files.
Username	Specifies the user name that the switch uses to access the FTP server for backup.
Password	Specifies the password that the switch uses to access the FTP server for backup. Enter the same password in both the **Password** fields to verify.
Enable HTTPS	Select this check box to enable daily backup of voice mail and auto-attendant data using HTTPS.
Note	This option allows the user to add any additional information.

10.3.1.1.2 Voice Application Tab

Voice mail and auto-attendant information for a voicemail model switch is provided on the Voice Application tab on the Platform Equipment page.

Table 57: Platform Equipment Page: Voice Application Tab (Voicemail Model Switch)

Parameter	Definition
Account code local extension	Specifies the extension on the headquarters SoftSwitch associated with the account codes application. When account code collection is optional or forced, calls are routed to this extension for an account code prompt. **Note**: The Account code local extension must be manually entered for Windows DVS and Linux DVS appliances. Refer to Configuring Account Codes on page 352 for more information.
Voice mail extension	Specifies the extension the system uses for forwarding calls to voicemail.
Voice mail login extension	Specifies the extension used to log in to the voice mail server.
Auto-attendant extension	Specifies the extension used by the auto-attendant server.
Default auto-attendant menu	Each server can have a different default auto-attendant menu. This is the menu reached when none is specified - for instance, when a caller dials 9 to escape from voice mail and return to the auto-attendant.
User group	Specifies the assigned user group for the server. Because voice mail places outbound calls, the server must have assigned permissions.

Parameter	Definition
Maximum trunks for voice mail notification	Specifies the maximum number of trunks that can be used in the event of a voice mail notification. If many escalation profiles have been configured, it may be desirable to set this to a relatively low number to prevent notifications from overwhelming the system and making it impossible for users to make an outbound call.

10.3.1.1.3 Switch Tab

Switch information for a voicemail model switch is provided on the **Switch** tab on the **Platform Equipment** page.

Table 58: Platform Equipment Page: Switch Tab (Voicemail Model Switch)

Parameter	Definition
Enable jack-based music on hold	Enables/disables jack-based music on hold.
Jack-based music on hold gain	Specifies the gain setting for jack-based music on hold.
Music on Hold	
Enable file based music on hold	Select this check box to enable file-based music on hold for the switch.
Local extension	Specifies the local music on hold extension.
Maximum concurrent calls	Specifies the maximum number of concurrent calls to allow for MOH. This is a maximum limit, not a guaranteed number.

Parameter	Definition
Use analog extension port as DID trunks	Select this check box to configure all analog extensions as analog DID trunks. **Note**: 1-U Half- Width analog extension ports cannot be individually configured as DID trunks, but by selecting this check box, you can configure all analog extensions as analog DID trunks. When this parameter is selected, analog ports on the switch cannot be assigned to a user extension port.
Built-in capacity	Allocates switch resources to support IP phones, SIP trunks, and SIP proxies on the Mitel network. Resource availability varies for each switch model. To allocate IP phone and SIP trunk resources, enter the desired number of resources in the **IP phones** and **SIP trunks** fields. The number of allocated SIP proxy resources is displayed in parenthesis under **Total**. This number is the number of available resources minus the sum of the IP phone and SIP trunk resources, multiplied by 20. For example, the SG90V provides 30 resources. If 5 resources are allocated for IP phones and 5 resources are allocated for SIP trunks, then 400 SIP proxy resources are available: (30 - (5+5))*20.

Parameter	Definition
Port Type	Select one of the following for each port to specify how each port resource is configured: • **Available**: Indicates that the channel resources is available for assignment. • **Trunk**: Configures the port as a trunk assigned to the trunk group specified by the Trunk Group parameter. • **5 IP Phones**: Configures the port resource to support 5 IP phones. • **Conference**: Configures the port resource to support Make Me conferencing. • **5 SIP Trunks**: Configures the port resource to support 5 SIP trunks. • **100 SIP Proxy**: Configures the port resource to support 100 SIP proxies. • **SIP Trunk with Media Proxy**: Configures the port resource as a SIP trunk with media proxy.
Trunk Group	In the drop-down list, select the trunk group to which the port is assigned. This parameter is available only when Port Type is set to Trunk.
Description	Type a descriptive name for the switch port.
Jack Number	Type the patch-panel jack number to which the port connects.
Tx Gain (db)	Type the gain added to received digital signals. The default is 0 dB.
Rx Gain (db)	Type the gain added to transmitted digital signals. The default is 0 dB.
Location	Enter a description of the location of the physical switch.

Parameter	Definition
Caller's emergency service identification (C ESID)	Enter the CESID for the analog port. To comply with RAY BAUM, you must provide the CESID for the analog port. **Note**: • Whenever you enter the CESID, it will be saved in the database as entered and will not be formatted as per the Country-specific numbering plan. • (For US customers) If the third-party vendor trunks are not used for Ray Baum conformance, then the CESID will be the telephone number that will identify the location and the callback number.
Fill Down	Click to duplicate the contents of the Port 1 fields for all other ports. The channel number, in parenthesis, is appended to the contents of the Description field.

10.3.2 Replacing a Switch

When replacing a voicemail-enabled switch, the CF card retains the voicemail contents. The card can go into the replacement switch if the switch is the same model as the original.

To replace a voicemail-enabled switch and retain the voicemail on the original switch:

1. Remove the original switch from the Mitel network.
2. Remove the plate covering the memory slot on the left side of the original switch.
3. Remove the CF card from the memory slot.
4. Remove the plate covering the memory slot on the left side of the replacement switch.
5. Insert the CF card into the memory slot and replace the memory slot cover.
6. Connect the replacement switch into the network.
7. Launch Connect Director.

8. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
9. Click the name of the replaced switch in the **List** pane.

   The **General** tab in the details pane displays parameters for the selected switch.
10. In the **MAC address** field, enter the MAC address of the new switch and click **Save**.
11. Boot the V-switch and configure the normal settings (IP/NTP/Server/etc).
12. Log into the Linux shell of the V-switch and execute the following commands.

```
cd /cf/shorelinedata

rm -f MACADDRESS.txt
```

10.3.3 Upgrading a Switch

Upgrading a voicemail-enabled switch uploads new switch firmware and server software to the device. Switch upgrades are necessary to maintain compatibility with the remainder of the system when the MiVoice Connect system is upgraded. Refer to the *MiVoice Connect Maintenance Guide* for complete information about upgrading a switch.

Note:
A regular voice switch cannot be converted to a voicemail-enabled switch.

10.3.4 Configuring Voice Mail

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the switch to configure voice mail for in the **List** pane.

   The **General** tab in the details pane displays parameters for the selected switch.
4. Select the **Voice Application** tab.
5. In the **Account code local extension** field, enter an available extension number.
6. In the **Voice mail extension** field, enter the extension the system uses for forwarding calls to voicemail.
7. In the **Voice mail login extension** field, enter the extension used to log in to the voice mail server.
8. In the **Auto-attendant menu** list, select the extension used by the auto-attendant server.
9. In the **User group** list, select the assigned user group for the server.

10. In the **Maximum trunks for voice mail notification** field, enter the maximum number of trunks that can be used in the event of a voice mail notification.

10.3.5 Configuring File-Based Music on Hold

File-based MOH can be configured for application servers and voicemail-enabled switches. After file-based MOH is configured, you can then select the MOH file to use for the following:

- DNIS - See Configuring DNIS on page 244.
- User Groups - See Adding or Editing a User Group on page 483.
- System-Wide Default - See Configuring Other System Parameters on page 53.

Note:
If an MOH file is defined for DNIS, it is played first. If an MOH file is not defined for DNIS, the MOH file defined for the User Group is played. If an MOH file is not defined for the User Group, the MOH file defined for the system-wide default is played. If an MOH file is not defined for DNIS, the User Group, or the system-wide default, the audio input jack is used.

10.3.5.1 Configuring MOH for an Application Server

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the server to configure in the **List** pane.

   The **General** tab in the **Details** pane displays parameters for the selected server.
4. Select the **Music on Hold** tab.
5. Select the **Enable file based music on hold** check box.
6. In the **Local extension** field, enter an available extension number.
7. (Optional) In the **Maximum concurrent calls** field, enter the maximum number of concurrent calls to allow for MOH. This is a maximum limit, not a guaranteed number.

10.3.5.2 Configuring MOH for a Voicemail-Enabled Switch

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.

3. Click the name of the switch to configure in the **List** pane.

   The **General** tab in the **Details** pane displays parameters for the selected switch.
4. Under **Music on Hold**, select the **Enable file based music on hold** check box.
5. In the **Local extension** field, enter an available extension number.
6. Optional: In the **Maximum concurrent calls** field, enter the maximum number of concurrent calls to allow for MOH. This is a maximum limit, not a guaranteed number.

10.3.6 Specifying Root and Administrator Passwords for CLIs

The voicemail-enabled switches provide access to command line interfaces (CLIs) for diagnostics and advanced configuration tasks. Other than specifying a fixed IP address, CLI access is not required for typical switch operation and maintenance.

Mitel provides two default accounts for accessing these CLIs:

- **Admin:** This account is for configuring tasks that require CLI access.
- **Root:** The user with a root account has access to all internal Linux commands.

Note:
Mitel recommends using the Root command only under direct supervision of Mitel personnel. The root admin does not restrict command scenarios that can render the switch unusable.

You can use Connect Director to change the passwords for logging into these accounts.

Note:
Passwords for accessing CLIs must have a minimum of 4 ASCII characters and a maximum of 26 ASCII characters.

The system permits the following characters:

!#$%&'()*+,-.0123456789:;=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_/
`abcdefghijklmnopqrstuvwxyz{|}~

The system does not permit the following characters:

? “ <>

To change the Voice Switch CLI account passwords:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Options**. The **Options** page opens.
3. Under **Password**, in the first **"admin" password** field, enter the new password for the admin account.
4. In the second **"admin" password** field, reenter the password that you entered into the first field.
5. In the first **"root" password** field, enter the new password for the root account.
6. In the second **"root" password** field, enter the password that you entered into the first field.
7. Click **Save**.

10.3.7 Configuring Automatic Backup for a Switch

Due to the limited CF card capacity, we recommend daily backup of voice mail and auto-attendant data. Automatic backup begins immediately after the server completes its daily house-keeping operation. (The house-keeping utilities are built-in and remove log files and old voice mails based on the configuration data in Connect Director.)

Automatic backup also does the following:

- Stores voice mail, auto-attendant custom and default prompts, workgroup name and greeting prompts (if the workgroup voice mailbox is on the VMB), and switch log files to an FTP or HTTPS server. After completion of the daily file-system cleanup tasks, the switch begins automatic backup. A time stamp is appended to the name of files copied to the target server.
- Provides a source for the most recent day's voice mail and other data in the event of a system failure. It is not intended to be an archive of voice messages or a source for retrieving deleted voice mail.

Note:
Any machine capable of supporting an FTP or HTTPS server can be the target of a backup. The FTP or HTTPS server must be RFC 959 compliant and additionally support the commands MDTM and SIZE. The FTP or HTTPS servers on most versions of Microsoft Windows, including Windows Server 2012 meet these requirements.

To configuring automatic backup for a switch:

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the V model switch to configure in the **List** pane.

   The **General** tab in the **Details** pane displays parameters for the selected switch.
4. Do either of the following:

   - Follow these steps to enable backup using FTP:

     a. Select the **Enable daily backup** check box.

     Note:
     The default start time to enable daily backup is 2AM.

     b. For 50V and 90V switches, under **Enable daily backup**, in the **Start time** field, enter the time of day to start the daily backup.
     c. In the **IP address** field, enter the IP address of the FTP server to which the backup files will be saved.
     d. In the **FTP port** field, enter the port number that the switch uses to communicate with the recipient FTP server.
     e. In the **Directory** field, enter the name of the folder on the FTP server to which you want to back up the switch files.

        The default location is `\inetpub \ftproot\`.
     f. In the **Username** field, enter the user name that the switch uses to access the backup files on the FTP server.
     g. In the first **Password** field, enter the password that the switch uses to access the backup files on the FTP server.
     h. In the second **Password** field, reenter the password that you entered in the first field.
   - Follow these steps to enable backup using HTTPS:

     a. Select the **Enable daily backup** check box.

Note:
The default start time to enable daily backup is 2AM.

b. For 50V and 90V switches, under **Enable daily backup**, in the **Start time** field, enter the time of day to start the daily backup.
c. In the **IP address** field, enter the IP address of the HQ server to which the backup files will be saved.
d. In the **Directory** field, enter the name of the folder on the HQ server to which you want to back up the switch files.
e. Select the **Enable HTTPS** check box.

5. Click **Save**.

10.3.8 Configuring a Target Server for Backup

For backing up the voice mail on a Voice Model switch (V Model switch), there must be a target FTP server, which will receive these files. A Mitel main server or a third-party server can function as the recipient for V Model switch backup files.This section describes the FTP server installation and configuration steps and also explains the corresponding configuration to be made on Connect Director for backing up files.

Installing the FTP Server and Management Tools

Follow these steps to install the FTP Server components on the Windows server:

1. On the Windows desktop, click **Start** > **Programs** > **Administrative Tools** > **Server Manager** to launch the Server Manager Dashboard.
2. In the Server Manager Dashboard, under **Configure this local server**, click **Add roles and features**. The **Add Roles and Features** Wizard appears, and displays the **Before you begin** page.
3. After reading the **Before you begin** page, click **Next**. The **Select installation type** page appears.
4. In the middle pane, select **Role-based or feature-based installation**, and then click **Next**. The **Select destination server** page appears.
5. Choose **Select a server from the server pool**, highlight a server in the pool, and click **Next**. The **Select server roles** page appears.
6. Select the **Web Server (IIS)** check box and click **Next** to install the IIS Web Server.
7. Repeat steps 1 through 5.

8. In the **Select server roles** page, go to **Web Server (IIS)** > **FTP Server** and select the following:
   - **FTP Service**
   - **FTP Extensibility**
9. Under **Management Tools**, select all the options.
10. Click **Next** to install the FTP Server and Management Tools.

Configuring the FTP Server

Follow these steps to configure the FTP server:

1. On the Windows desktop, click **Start** > **Programs** > **Administrative Tools** > **Server Manager** to launch the Server Manager Dashboard.
2. Open **Administrative Tools** and double-click **Internet Information Services (IIS) Manager**.
3. Expand and right-click **Sites** on the **Connections** pane and select **Add FTP Site**.
4. In the window **Add FTP Site** window that opens, complete the following fields:
   - **FTP site name**
   - **Physical path**

Note:

- Click the **Make New Folder** option to create a specific folder to store the FTP files.
- It is recommended that you create a folder in the root of the main system drive, or on an entirely different hard drive. Otherwise, if you set the home folder in one of your default folders, while adding multiple accounts, users will not have permission to access the folder.

5. Click **Next**.
6. In the **On Binding and SSL Settings** page that opens, do the following:
   a. Enter the IP address in the **IP Address** field.
   b. Select the **Start FTP site automatically** option.
   c. Select **No SSL**
7. Click **Next**.

8. In the **Authentication and Authorization Information** page that opens, do the following:

   a. Under **Authentication**, select **Anonymous**.
   b. Under **Authorization** > **Allow access to**, select **Anonymous users**.
   c. Under **Permissions**, select the following options:

      - **Read**
      - **Write**

9. Enable write permissions to FTP folder. To do this, follow these steps:

   a. Navigate to the FTP folder that was created, right-click it, and select **Properties**.
   b. In the **Properties** window that opens, click the **Security** tab and click **Edit**.
   c. In the **Edit** window that opens, click **Add**, enter **IUSR** in the **Enter the object names to select** field, and click **OK**.
   d. In the window that opens, under **Group or user names**, select **IUSR**.
   e. Under **Permissions for Authenticate User**, select either **Write** or all the options.
   f. Click **OK** and **Apply** to provide write permissions.

10. Click **Finish** to complete the FTP server configuration.

Configuring the Corresponding Changes in Connect Director

To configure the changes in Connect Director corresponding to the FTP server configuration, follow these steps:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the V Model switch to configure in the **List** pane.

   The **General** tab in the **Details** pane displays parameters for the selected switch.
4. Select the **Enable daily backup** check box.

> **Note**:
> The default start time when daily backup is enabled 2AM.

5. For 50V, 90V, and SG90BRIV switches, in the **Start time** field, under **Enable daily backup**, enter the time of day to start the daily backup.
6. In the **IP address** field, enter the IP address of the FTP server on which the backup files must be saved.

7. In the **FTP port** field, enter the port number that the switch uses to communicate with the recipient FTP server (server that receives the backup files).
8. In the **Directory** field, enter the name of the folder on the FTP server in which you want to back up the switch files.

   The default location is `\inetpub \ftproot\`.
9. In the **Username** field, enter the user name that the switch uses to access the backup files on the FTP server.
10. In the first **Password** field, enter the password that the switch uses to access the backup files on the FTP server.
11. In the second **Password** field, reenter the password that you entered into the first field.
12. Click **Save**.

10.4 Rebooting and Restarting

Rebooting voicemail-enabled switches is different from restarting voicemail-enabled switches.

- Rebooting a voicemail-enabled switch also reboots the Linux kernel and everything that a kernel reboot entails.

  A reboot takes much longer than a restart.
- Restarting a voicemail-enabled switch reboots only the Mitel application layer.

  On switches running on VxWorks, rebooting and restarting are identical.

When a voice switch boots, it requires an IP address to connect to the network and an application program. voice switches are set to use a DHCP server for an IP address and to retrieve the application from the switch's flash memory.

Mitel recommends using static IP parameters configured via the serial port, as this is much more reliable. When using DHCP, Mitel recommends using DHCP reservations for each switch to ensure that DHCP leases are not lost.

If a DHCP server is not available, you can set the IP address manually from the switch's maintenance port from STCLI.

If the switch fails to load the application from flash and does not have the IP address of the Mitel server, you can set the IP address and boot parameters by connecting to the maintenance port and using the configuration menu. The configuration menu allows you to set the IP address of the switch and enter the Mitel server (boot host) IP address.

A voicemail-enabled switch can be brought up by a regular boot (flash memory-sourced) or by a software upgrade boot.

10.4.1 Specifying a Time Source

Mitel servers maintain an internal time-of-day (TOD) clock, which is initialized by input received at boot time from an NTP server. Mitel servers use the time of day clock to mark voicemail and track other transactions.

The voicemail-enabled switches begin server operations only after they receive an initial TOD input. If the time is not available from a designated source at boot time, the V Model switch supports all switch operations and will periodically poll for the time of day setting. After receiving the time of day setting, the V model switch begins server operations.

The NTP server can be specified through DHCP or as a static address. If no address is specified, the V Model switch polls NTP servers at addresses specified by an internal configuration list. The internal configuration list includes the Headquarters server and Internet based NTP servers.

- If an IP address is listed that does not point at an NTP server, the V Model switch will not begin server processes until the address is corrected.
- If the IP address points at a server that is not available, the V Model switch periodically polls the IP address for the NTP server. When the server becomes available, the V Model switch begins performing server operations after it polls the server and receives the time of day setting.

Note:
DHCP option 42 can be configured and is supported on 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones.

After the server becomes available, rebooting the V model switch may be faster than waiting for it to poll the NTP server.

10.4.2 Reboot Methods

Flash Boot

The standard method for booting a voice switch is to boot from the switch's flash memory. When a switch is first powered on, it reads the boot parameters stored on the non volatile memory, which instructs the switch to load software from flash memory. When the software starts, it loads its configuration, which is also stored in flash memory.

10.4.2.1 Default Button

The Default Button is the small “paperclip” button on the left side of the switch. Pressing this button replaces the two configuration files with their default variants. The Compact Flash is not affected.

Pressing this button and holding for 10 seconds, in addition to replacing the configuration files, removes all files from the Compact Flash.

10.4.2.2 FTP Boot

Booting from FTP is available when you cannot boot the switch from internal memory. When booting a switch from FTP, the operating system and software are loaded from the FTP site identified in the boot parameters. The loaded files define a default configuration.

Voicemail services on the switch are disabled after booting from FTP and are restarted only by booting from Flash. After an FTP boot, the switch can perform telephony functions as those available through other switches. V model switches started with an FTP boot can operate only as a voice switch (controlling phones, trunks, and call routing).

FTP boot is typically used for troubleshooting and also supports maintenance tasks and the backup and restore facilities.FTP boot supports certain maintenance functions, such as an emergency boot if the flash becomes damaged.

10.5 Monitoring Memory Usage for a Voicemail Model Switch

To avoid disk space problems for a voicemail model switch, you need to monitor and manage Compact Flash (CF) memory and log files to ensure adequate disk space.

Typical CF card capacities are 1 GB, 2 GB, and 4 GB. The proper planning of voice mail usage and aging can help prevent excessive buildup of voice mail on the CF card. If the CF card becomes full, it cannot accept new voice mail.

You can monitor disk space for voicemail model switches using either of the following methods, which are both available from the Maintenance menu in Connect Director:

- Display the status of voicemail model switches. For more information, see Monitoring Voice Mail Status on page 813.
- Display the status and other maintenance information for voice mail servers. For more information, see Monitoring Server Status on page 788.

In addition to monitoring memory usage through Diagnostics & Monitoring, you can create an event filter to send you an email message if memory usage is high. For information about using event filters, see Using Event Filters on page 832.

10.5.1 Modifying the Log File Size and Age

Due to the constraints on CF memory space, you should limit the amount of disk space that log files consume. When you add a voicemail-enabled switch to the system, you can modify the values for the maximum size and age of log files. These settings are available on the Additional Parameters page in Connect Director. See Configuring Other System Parameters on page 53 for information.

10.6 Configuring Service Appliances

Before you can use Mitel conferencing or instant messaging, you must configure any Service Appliances attached to your system. For detailed configuration procedures, see the *Conferencing and Instant Messaging Planning and Installation Guide*.

Configuring Trunks 11

This chapter contains the following sections:

This chapter describes how to configure trunks and trunk groups in Connect Director.

11.1 Overview

Before beginning, you should understand the different trunk types and trunk features that the MiVoice Connect system supports.

- A thorough description of the types of trunks and their associated features is included in the *MiVoice Connect Planning and Installation Guide*.
- A detailed description of how the dialing plan, network call routing, and digit manipulation operate is included in the *MiVoice Connect Planning and Installation Guide*.

For more information about the features supported outside the U.S. and Canada, refer to the *MiVoice Connect Planning and Installation Guide*.

For an overview of the various trunk types and trunk features, refer to the *MiVoice Connect Planning and Installation Guide*.

11.2 Configuring Trunk Groups

This section describes how to add or modify a trunk group.

11.2.1 Viewing Trunk Groups

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.

For descriptions of the columns on the Trunk Groups page, see Trunk Groups Page: List Pane.

Table 59: Trunk Groups Page: List Pane

Column Name	Description
Name	Name of the trunk group.
Type	The type of trunk group.
Site	The name of the trunk group site. A trunk group cannot span sites. For information about configuring sites, refer to Overview on page 100.
Trunks	The number of trunks in the trunk group.
DID	Indicates whether or not Direct Inward Dialing (DID) is enabled for the trunk group. **Note**: DID is not available for Analog Loop Start or Digital Loop Start trunk groups.

Column Name	Description
DNIS	Indicates whether or not Dialed Number Identification Service (DNIS) is enabled for the trunk group. **Note**: DNIS is not available for Analog Loop Start or Digital Loop Start trunk groups.
OSE	Indicates whether or not Off-System Extensions (OSE) are enabled for the trunk group.
Access Code	The access code for the trunk group.

11.2.2 Adding or Editing a Trunk Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.
3. Do one of the following:
   - To edit an existing trunk group, click the name of the trunk group in the **List** pane.
   - To create a copy of an existing trunk group, click **Copy**.
   - To create a new trunk group, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing trunk group.

4. Review the parameters on all of the tabs in the **Details** pane, and specify values as appropriate. For more information about all of the trunk group parameters on the various tabs of the details pane, see Trunk Group Parameters on page 222.
5. Click **Save**.

11.2.3 Trunk Group Parameters

A trunk group has many details. You configure trunk group parameters on the following tabs, which you can access on the details pane for a particular trunk group:

- General Tab on page 222
- Inbound Tab on page 225
- Outbound Tab on page 229

11.2.3.1 General Tab

General information about new and existing trunk groups is provided on the General tab in the details pane of the **Trunk Groups** page.

Trunk Groups Page: General Tab describes the parameters on the **General** tab of the **Trunk Groups** page.

Table 60: Trunk Groups Page: General Tab

Parameter	Description
Name	Specifies the name of the trunk group.
Site	In the drop-down list, select the trunk group site.
Trunk type	In the drop-down list, select the type of trunk group.
Language	In the drop-down list, select the language for the trunk group.

Parameter	Description
Enable SIP info for G.711 DTMF Signaling	Select this check box to enable the SIP INFO Method for transmitting Dual Tone Multi-Frequency (DTMF). This check box must be selected for the following: • Mitel-to-Mitel SIP tie trunks or SIP devices that do not support RFC 2833 for G711. • Third-party SIP devices that do not support DTMF negotiation as described in RFC 2833. If the device does not support RFC 2833 and this check box is not selected, DTMF negotiation will fail. **Note**: This option applies to SIP trunks only. SIP INFO must be supported by the SIP trunk provider and is necessary for passing of DTMF digits for Extension Assignment over SIP Trunks. See Extension Assignment over SIP Trunks on page 677 for more information. For more information about DTMF, see Dual Tone Multi-Frequency Support on page 676.
Profile	In the drop-down list, select the profile for the trunk group. This profile applies to all trunks in the trunk group. **Note**: This option applies to SIP, PRI, and BRI trunk groups only. SIP profiles are available for SIP trunk groups; ISDN profiles are available for PRI and BRI trunk groups. For more information about SIP trunk profiles, see Configuring SIP Trunk Profiles on page 683. For more information about ISDN trunk profiles, see Introduction to ISDN Profiles on page 262.

Parameter	Description
Digest authentication	In the drop-down list, select the type of calls for which to perform authentication over the trunk: • **None** - to disable authentication for inbound and outbound calls • **Inbound-Only -** to perform authentication of credentials for inbound calls only • **Outbound-Only** - to provide credentials for outbound calls when authentication is required by the call recipient • **All** - to perform authentication for inbound calls and provide credentials for outbound calls If SIP trunk registration is required by SIP ITSP, this parameter cannot be set to **None**. **Note**: This option applies to SIP trunks only.
Username	Specifies the user name for digest authentication. **Note**: This option applies to SIP trunks only and might be obtained from the SIP ITSP service provider.
Password	Specifies the password for digest authentication. **Note**: This option applies to SIP trunks only and might be obtained from the SIP ITSP service provider.
Note	This option allows you to add any additional information.

11.2.3.2 Inbound Tab

All inbound calls are routed to a destination, such as an extension (user, workgroup, or route point) or a specific menu.

Inbound calls first try to match set parameters in the following order:

1. DNIS
2. DID
3. Extension
4. Tandem Trunking
5. Destination; the destination for a trunk group is the default auto-attendant

Note:

- An individual trunk group cannot have overlapping DID and DNIS numbers (received digits).
- Users, Menus, Workgroups, Route Points, Hunt Groups, and Bridged Call Appearances can have only one DID number, but can have multiple DNIS entries.

Information about inbound settings for trunk groups is provided on the **Inbound** tab in the **Details** pane of the **Trunk Groups** page.

Trunk Groups Page: Inbound Tab describes the parameters on the **Inbound** tab of the **Trunk Groups** page.

Table 61: Trunk Groups Page: Inbound Tab

Parameter	Description
Number of digits from CO	Specifies the maximum number of digits expected from the central office (for User PRI configured trunks). Digit collection terminates when the maximum number of digits is received, the digit collection timeout is reached, or an exact match is found. A network PRI trunk connected to a legacy PBX collects digits from the legacy PBX side. When the Mitel system detects a trunk access code, it ignores the **Number of digits from CO** parameter and routes the call according to the dialing plan. **Note**: • This parameter is not applicable for Analog Loop Start or Digital Loop Start trunk groups. • For Digital Wink Start trunks, this parameter might need be changed according to the country dial plan.
DNIS	Select this check box to enable DNIS for the trunk group. For information about configuring DNIS, see Configuring DNIS on page 244. **Note**: DNIS is not applicable for Analog Loop Start or Digital Loop Start trunk groups.

Parameter	Description
DID	Select this check box to enable DID for the trunk group. For detailed information about configuring DID for a trunk group, see Configuring DID on page 239. **Note**: DID is not applicable for Analog Loop Start or Digital Loop Start trunk groups.

Parameter	Description
Extension	Specifies the extension to route calls to, based on the digits received from the central office (CO). You can use this option when configuring a tie trunk connected to a legacy PBX. **Note**: The extension length must match the number of digits from the CO. • **Translation table** - in the list, select the digit translation table to use to strip one or more digits from calls between two systems with extensions of different lengths; use this option when using the On-Net Dialing feature. For more information about translation tables, see Creating Digit Translation Tables on page 47 • **Prepend dial in prefix** - specifies one or more digits to add to calls between two systems with extensions of different lengths; use this option when using the On-Net Dialing feature. • **Use site extension prefix** - specifies the site extension prefix to add to calls going from a system that does not have a prefix to another system that does have a prefix; use this option when using the On-Net Dialing feature. **Note**: Extension is not applicable for Analog Loop Start or Digital Loop Start trunk groups.

Parameter	Description
Tandem trunking	Select this check box to allow legacy voice systems to use a Mitel system for outbound dialing. The Mitel system supports network-side PRI, which enables Mitel systems to flexibly support digital tie trunks to other systems. • **User group** - in the list, select the user group to associate tandem calls with for outbound trunk selection; inbound calls recognized as tandem calls are then redirected to an outbound trunk based on the call permissions and trunk group access associated with the user group in Connect Director. • **Prepend dial in prefix** - specifies one or more digits to prepend to the digits collected on tandem calls; the complete set of digits is then used in outbound trunk selection for the tandem call. For more information about tandem trunking, see Configuring Tandem Trunking on page 248. **Note**: Tandem trunking is not applicable for Analog Loop Start or Digital Loop Start trunk groups.
Destination	Specifies the destination number for inbound calls. **Note**: Inbound calls first try to match an entry in the following order: DNIS, DID, Extension, Tandem trunking. If no match is found, the inbound call is routed to the Destination entry. The destination for a trunk group is the default auto-attendant.

11.2.3.3 Outbound Tab

Information about outbound settings for trunk groups is provided on the **Outbound** tab in the details pane of the **Trunk Groups** page.

Trunk Groups Page: Outbound Tab describes the parameters on the **Outbound** tab of the **Trunk Groups** page.

Table 62: Trunk Groups Page: Outbound Tab

Parameter	Definition
Outgoing	Select this check box to enable settings for outbound calls.
Network call routing	
Access code	Specifies the access code for the trunk group. Typically the access code in the U.S. and Canada is 9. **Note**: The access code structure must already be established in the dial plan. See Setting Dial Plan Parameters on page 41for more information.
Local area code	Specifies the local area code for the trunk group. This area code is used for Network Call Routing and Digit Manipulation.
Additional local area codes	Specifies additional local area codes for the trunk group. These area codes are used for Network Call Routing and Digit Manipulation. Click **Add** to add each additional local area code.
Nearby area codes	Specifies nearby area codes that are cost-free for the trunk group. Click **Add** to add each nearby area code.

Parameter	Definition
Billing telephone number (BTN)	Specifies the billing telephone number (BTN) for the trunk group. The BTN specified for a trunk group is not used for billing purposes. This BTN is used to support an alternative to individual user DIDs when needed. Specifying a BTN for a trunk group enables the switch to forward an original caller's ID when a received call is redirected by one of Mitel's forwarding features. For example, if an outside caller dials a Mitel user whose Find-Me setup specifies a mobile phone number, the mobile phone can show the original caller's number. The applicable forwarding features are Find Me, some availability states, PSTN Failover, Extension Assignment, Allow Additional Phones to Ring Simultaneously, and Extension Reassignment. For more information, see Purpose of the Billing Telephone Number for Caller ID on page 260. **Note**: This parameter only applies to SIP, PRI, and BRI trunk groups.
Carrier code	Specifies the carrier code for the trunk group. For information about carrier codes, see the *MiVoice Connect Planning and Installation Guide*. **Note**: This parameter only applies if the trunk group is assigned to a site located in a country that supports carrier codes.
Trunk services	
Local	Select this check box to enable local calls.

Parameter	Definition
Long distance	Select this check box to enable long-distance calls.
National mobile	Select this check box to enable outbound calls to mobile numbers. Clear this check box to avoid costs associated with outbound calls to mobile numbers in caller-pays environments. **Note**: This option is only available for PRI trunks in countries with caller-pays billing plans (for example, Ireland).
International	Select this check box to enable international calls.

Parameter	Definition
Enable original caller information	Select this check box to enable the switch to forward an original caller's ID when a received call is redirected by one of Mitel's forwarding features. For example, if an outside caller dials a Mitel user whose Find-Me setup specifies a cell phone, the cell phone can show who dialed the Mitel number. This parameter applies to the following forwarding features: • Find Me • Some call handling modes • PSTN failover • Extension Assignment • Allow additional phones to ring simultaneously • Extension reassignment For more informations about enabling original caller information, see Enabling Original Caller Information on page 261. **Note**: This option does not apply to Analog Loop Start trunks.
n11 (e.g. 411, 611, except 911 which is specified below)	Select this check box to enable telephone service calls for service such as directory assistance or repair. For details about support for emergency services calls on trunks, see Configuring a System for Emergency Calls on page 983. **Note**: This option is not available for all countries.

Parameter	Definition
Emergency (e.g. 911)	Select this check box to enable emergency 911 calls. To support 911 in the U.S., at least one trunk group per site must allow 911 calls. For a detailed description of 911 support, see Configuring a System for Emergency Calls on page 983.
Easily recognizable codes (ERC) (e.g. 800, 888, 900)	Select this check box to enable services such as toll-free dialing for easily recognized codes like 800, 888, or 900. **Note**: This option is not available for all countries.
Explicit carrier selection (e.g. 10101xxx)	Select this check box to enable the caller to specify a particular long-distance carrier. The format of the carrier selection code is 1010xxx; for example, 1010811. **Note**: This option is not available for all countries.
Operator assisted (e.g. 0+)	Select this check box to enable operator dialing for the trunk group. **Note**: This option is not available for all countries

Parameter	Definition
Caller ID not blocked by default	Select this check box to enable the system to pass Caller ID information on outbound calls by default. Clear this check box to block Caller ID information on all outbound calls. In the United States, a user can override this option using Vertical Service Codes. For example, pressing *67 blocks, and pressing *82 unblocks. If configuring a SIP trunk, be sure the SIP trunk provider can provide these types of features. **Note**: This option is available only for PRI and SIP trunk groups and is not available for all countries.
Enable Pulse Dialing	Select this check box to enable pulse dialing. Dialed digits are sent through the selected trunk group to the CO in the form of pulses.The ON Duration, OFF Duration, and GAP Duration between digits is specified by the region or country. **Note**: This option is only available for Analog Loop Start Trunk Groups created in Connect Director for a region or country where pulse dialing is available.

Parameter	Definition
Enable caller ID name	Select this check box to provide the caller's name to the carrier or service provider. To provide text other than the caller's name to the carrier or service provider, type the text to provide in the **When Site Name is used for the Caller ID, overwrite it with** field. **Note**: This option is available only for PRI and SIP trunk groups.
Detect battery reversal	This option is not available in the United States, Canada, or Hong Kong.
Trunk digit manipulation Trunk Digit Manipulation controls how the trunk group manipulates the telephone number before outputting the digits to the central office. **Note**: All North American dial-plan numbers are converted into the1+10-digit format internally before they are passed to the trunk group for digit manipulation.	
Remove leading 1 from 1+10D	Select this check box to drop the leading 1 from a dialed number. Dialing only ten digits is required by some long-distance service providers. If a local prefix list is provided, seven digits are dialed for all entries in the list (applies to the local area code only, not additional local area codes).

Parameter	Definition
Remove leading 1 for local area codes (for all prefixes unless a specific local prefix list is provided below)	Select this check box to drop the leading 1 for all local area codes (applies to the local and any additional local codes). Dialing only ten digits for local area codes, particularly with overlay area codes, is required by some local service providers. If a local prefix list is provided, the leading “1” is removed for the all entries in the list.
Dial 7 digits for local area code (for all prefixes unless a specific local prefix list is provided below)	Select this check box to enable the trunk to dial numbers in the local area code with seven digits. This capability is required by some local service providers.
Dial in E. 164 format	Select this check box to enable this trunk group to support E.164 numbers. **Note**: This option is only available for SIP trunk groups.
Local prefixes	In the drop-down list, select the list of local prefixes for the trunk group. When you use a local prefix list, prefixes that are not in the prefix list are considered long distance and require a long distance trunk service. For information about adding a local prefix list, see Importing Local Prefixes on page 251.

Parameter	Definition
Prepend dial out prefix	Specifies the dial-out prefix for the trunk group. The dial-out prefix is prepended to the dial-out string that results from the other rules. (The dial-out prefix is not applied to off-system extension calls.) A dial-out prefix is typically required when connecting to, and leveraging the trunks on, a legacy PBX. For information about adding a pause to the dial out prefix, see Configuring Individual Trunks on page 254.
Translation table	In the drop-down list, select the translation table for the trunk group. The digit translation table is used by the system to strip one or more digits from calls between two systems with extensions of different lengths. Mitel does not apply inbound digit treatment to digit strings beginning with a trunk access code (such as 9) as would occur in tie trunk configurations. Digit strings beginning with a trunk access code are routed according to the dial plan. For information about translation tables, see Configuring Digit Translation Tables on page 46.

11.2.3.4 Enabling Original Caller Information

The **Enable Original Caller Information** parameter is a starting point for other tasks that you must perform to transmit the original caller ID. For descriptions of these tasks, see the following sections:

- For details about forwarding the original caller ID, see the Forwarding Original Caller ID Outside a Mitel Network on page 258.
- For the class of service (COS) that a user must have to ensure that the forwarding of an outside call is permitted, see the Specifying a Class of Service on page 461.
- For information about enabling Send incoming caller ID for call forwarding features such as Find-Me, External Assignment, and Allow Additional Phones, see Configuring Private Extensions on page 547.
- For information about responding to carriers who do not validate the caller ID in a SETUP message for an original caller ID, see Configuring an ISDN Profile for RNIE

on page 274. This advanced (and rarely needed) task follows the tasks described in Forwarding Original Caller ID Outside a Mitel Network on page 258.

Note:

In releases ST11, ST10.2, ST10.1, and ST10, the forwarding of the original caller ID to an outside device relied on custom dial plan elements from Mitel TAC. If TAC implemented such a custom dial plan, TAC must remove the elements related to this function before the current capability can work. (This issue does not exist for customers whose new installation contains the present implementation described in this book.) If a system with such a dial plan is upgraded, problem behaviors related to call forwarding or original caller ID can occur. Some possible behaviors are:

- Forwarded calls go to the user's voice mail instead of out the trunk.
- Forwarded calls are rejected by the carrier.

Upgraded customers who know or suspect that such a custom dial plan has been used should contact TAC for help. However, some customers might not know that a custom dial plan has been used for original caller ID. These customers should, therefore, monitor the call forwarding and caller ID performance after an upgrade.

11.2.4 Configuring DID

Direct Inward Dialing (DID) is a feature offered by telephone companies for use with their customers' PBX systems, where the telephone company allocates a range of numbers to a customer's PBX. As calls are presented to the PBX, the number that the caller dialed is also given, allowing the PBX to route the call to the intended party.

A DID range is a list of consecutive (non-overlapping) DID numbers assigned to a trunk group. Once a DID range is assigned to a trunk group, any available number within that range can be assigned to a user, workgroup, route point, auto-attendant, hunt group, or bridged call appearance from the corresponding pages in Connect Director.

Available DID numbers are DID numbers within a range that are not assigned to a user or entity within the context of that range.

Note:
DID number availability within a range does not consider DNIS assignments.

Although numbers assigned as a DNIS number are still enumerated as available within a DID range, attempts to assign these DID numbers will be unsuccessful.

Note:
DID is not applicable for Analog Loop Start or Digital Loop Start trunk groups.

11.2.4.1 Viewing DID Ranges

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **DID Ranges**. The **DID Ranges** page opens.

For descriptions of the columns on the DID Ranges page, see DID Ranges Page: List Pane.

Table 63: DID Ranges Page: List Pane

Column Name	Description
Trunk Group	Name of the trunk group the DID range is assigned to.
Base Phone Number	The starting number of the DID range.
Number of Phone Numbers	The number of phone numbers included in the DID range.

11.2.4.2 Enabling DID for a Trunk Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.
3. Click the name of the trunk group to enable DID for in the **List** pane.

Note:
The **General** tab in the **Details** pane displays parameters for the selected trunk group.

4. Select the **Inbound** tab.
5. Select the **DID** check box.

6. Click **Save**.

11.2.4.3 Assigning a DID Range to a Trunk Group

You can configure multiple DID ranges for each trunk group.

Note:

- Before you can configure a DID range for a trunk group, you must enable DID for the desired trunk group. For information about enabling DID for a trunk group, see Enabling DID for a Trunk Group on page 240.
- DID is not applicable for Analog Loop Start or Digital Loop Start trunk groups.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **DID Ranges**. The **DID Ranges** page opens.
3. Do one of the following:
   - To edit an existing DID range, click the name of the corresponding trunk group in the **List** pane.
   - To create a copy of an existing DID range, click **Copy**.
   - To create a new DID range, click **New**.

Note:

The **General** tab in the **Details** pane displays parameters for the new or existing DID range.

4. Review the parameters and specify values as appropriate. For descriptions of the DID range parameters, see DID Ranges Page: General Tab.
5. Click **Save**.

Table 64: DID Ranges Page: General Tab

Column Name	Description
Trunk Group	In the drop-down list, select the trunk group to assign the DID range to. **Note**: Only trunk groups that have DID enabled appear in this list.
Base Phone Number	Specifies the starting number of the DID range.
Number of Phone Numbers	Specifies the number of phone numbers included in the DID range.

11.2.4.4 Assigning DID Numbers

Once a DID range is assigned to a trunk group, any available number within that range can be assigned to a user, workgroup, route point, auto-attendant, hunt group, or bridged call appearance from the corresponding pages in Connect Director.

Note:

- An individual trunk group cannot have overlapping DID and DNIS numbers (received digits).
- Users, Menus, Workgroups, Route Points, Hunt Groups, and Bridged Call Appearances can have only one DID number, but can have multiple DNIS entries.

1. Launch Connect Director.

2. In the navigation pane, do one of the following;

   - Click **Administration > Users > Users**.
   - Click **Administration > Features > Workgroups**.
   - Click **Administration > Features > Auto-Attendant**.
   - Click **Administration > Features > Call Control > Bridged Call Appearances**.
   - Click **Administration > Features > Call Control > Hunt Groups**.
   - Click **Administration > Features > Call Control > Route Points**.

   The corresponding page is displayed.
3. Do one of the following:

   - To edit an existing item, click the name of the item in the **List** pane.
   - To create a copy of an existing trunk group, click **Copy**.
   - To create a new item, click **New**.

> **Note**:
>
> The **General** tab in the **Details** pane displays parameters.

4. Next to **DID Settings**, click **change settings** to display the DID parameters.
5. Select the **Enable DID** check box.
6. In the **DID Range** list, select the trunk group to which the desired DID range is assigned.
7. In the **DID number** field, enter the DID number (within the selected range) to assign to the user, workgroup, route point, auto-attendant, hunt group, or bridged call appearance.
8. Click **Save**.

11.2.4.5 Viewing the DID Map

You can view a list of all assigned DID numbers on the DID Map page.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **DID Map**. The **DID Map** page opens.

For descriptions of the columns on the DID Map page, see DID Map: List Pane.

Table 65: DID Map: List Pane

Column Name	Description
Trunk Group	Name of the trunk group the DID number is assigned to.
DID Number	The DID number.
Received Digits	The DID number that the telephone company sends.
Destination	The user, workgroup, route point, auto-attendant, hunt group, or bridged call appearance that the DID number is assigned to.
Music on Hold	The MOH used for the specified DID number; User groups or Mitel.

11.2.5 Configuring DNIS

Viewing DNIS Entries

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **DNIS Map**. The **DNIS Map** page opens.

For descriptions of the columns on the DNIS Map page, see DNIS Map Page: List Pane.

Table 66: DNIS Map Page: List Pane

Column Name	Description
Trunk Group	Name of the trunk group the DID range is assigned to.
Received Digits	The DNIS number that the telephone company sends.
Display Name	The description of the DNIS identifier.
Extension	The extension the DNIS is routed to, if the DNIS is routed to an on-system extension that is not a menu extension.

Column Name	Description
Menu Extension	The menu extension the DNIS is routed to, if the DNIS is routed to an auto-attendant extension.
Off System Extension	The off-system extension the DNIS is routed to, if the DNIS is routed to an off-system extension.
Music on Hold	The MOH used for the specified DNIS number; User groups or Mitel.

11.2.5.1 Enabling DNIS for a Trunk Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.
3. Click the name of the trunk group to enable DNIS for in the **List** pane.

Note:
The **General** tab in the **Details** pane displays parameters for the selected trunk group.

4. Select the **Inbound** tab.
5. Select the **DNIS** check box.
6. Click **Save**.

11.2.5.2 Assigning a DNIS to a Trunk Group

Note:

- DNIS is not applicable for Analog Loop Start or Digital Loop Start trunk groups.
- An individual trunk group cannot have overlapping DID and DNIS numbers (received digits).
- Users, Menus, Workgroups, Route Points, Hunt Groups, and Bridged Call Appearances can have only one DID number, but can have multiple DNIS entries.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **DNIS Map**. The **DNIS Map** page opens.
3. Do one of the following:

   - To edit an existing DNIS, click the DNIS in the **List** pane.
   - To create a copy of an existing DNIS, click **Copy**.
   - To create a new DNIS, click **New**.

> **Note**:
>
> The **General** tab in the **Details** pane displays parameters for the new or existing DNIS.

4. Review the parameters and specify values as appropriate. For descriptions of the DNIS Map parameters, see DNIS Map Page: General Tab.
5. Click **Save**.

Table 67: DNIS Map Page: General Tab

Column Name	Description
Trunk Group	In the drop-down list, select the trunk group to assign the DNIS to. **Note**: Only trunk groups that have DNIS enabled appear in this list.
Received digits	Specifies the DNIS number that the telephone company sends.
Display Name	Specifies a description of the DNIS identifier.

Column Name	Description
Type	In the drop-down list, select one of the following to specify the destination type to route the DNIS to: • **Extension** - to map the DNIS to an internal extension. • **Menu** - to map the DNIS to an auto-attendant. • **Off-System Extension** - to map the DNIS to an off-system extension; select the extension range that includes the extension you want to use. For information about configuring off-system extensions for use with DNIS, see Configuring Off-System Extensions on page 247.
Destination	Specifies the extension to route the DNIS to.
Music on Hold	Specifies the file-based MOH resource to use for the DNIS.

11.2.6 Configuring Off-System Extensions

Off-system extensions are typically used when setting up a tie trunk to a legacy PBX and configuring coordinated extension dialing.

11.2.6.1 Viewing Off-System Extensions

You can view a list of all available off-system extensions on the Off-System Extensions page.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Off-System Extensions**. The **Off-System Extensions** page opens.

For descriptions of the columns on the Off-System Extensions page, see Off-System Extensions Page: List Pane.

Table 68: Off-System Extensions Page: List Pane

Column Name	Description
Trunk Group	Name of the trunk group the off-system extension is assigned to.

Column Name	Description
From	The lower bound of the off-system extension.
To	The upper bound of the off-system extension.

11.2.6.2 Adding Off-System Extensions

1. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Off-System Extensions**. The **Off-System Extensions** page opens.
2. Do one of the following:

   - To edit an existing off-system extension, click the name of the trunk group in the **List** pane.
   - To create a new off-system extension, click **New**.

   The **General** tab in the **Details** pane displays parameters for the new or existing off-system extension.
3. Review the parameters and specify values as appropriate. For descriptions of the Off-System Extension parameters, see Off-System Extensions Page: General Tab.
4. Click **Save**.

Table 69: Off-System Extensions Page: General Tab

Column Name	Description
Trunk Group	In the drop-down list, select the name of the trunk group to assign the off-system extension to.
From	Specifies the lower bound of the off-system extension.
To	Specifies the upper bound of the off-system extension.

11.2.7 Configuring Tandem Trunking

Tandem trunking treats digits on an incoming trunk call as a PSTN number. Received digits are tested against DNIS, DID, Extension, and Tandem trunking, in that order. When Tandem trunking is enabled, the number of digits from the CO may have no effect if the first digit(s) matches a Trunk Access Code. To define trunk access and call permissions, associate a user group with the tandem trunk group.

Any associated dial in prefix is prepended to each set of inbound digits. You can use DNIS, DID, or Extension matching with a dial in prefix.

When using NI-2 signaling on PRI trunks—for example in a tie trunk scenario—the Caller ID name is also captured, when available, on all inbound calls. For outbound calls, the Caller ID name is delivered for calls that are made to off-system extensions, but not generally for all outbound calls.

Tandem calls are reported in the Trunk Activity Detail and Trunk Activity Summary reports, with incoming and outgoing legs reported according to the report format. For more information about CDR reports, see CDR Reports on page 993.

11.2.8 Configuring Additional Local Area Codes

1. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.
2. Do one of the following:
   - To edit an existing trunk group, click the name of the trunk group in the **List** pane.
   - To create a copy of an existing trunk group, click **Copy**.
   - To create a new trunk group, click **New**.

   Note:
   The General tab in the **Details** pane displays parameters for the new or existing trunk group.
3. Select the **Outbound** tab.
4. Select the **Outgoing** check box.
5. Under **Network call routing**, under **Additional local area codes**, click **Add**.
6. Do one of the following:
   - Click **Add** to add an additional local area code.
   - Click **Remove** next to a local area code to delete that area code.
7. Click **Save**.

11.2.9 Configuring Nearby Area Codes

1. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.

2. Do one of the following:

   - To edit an existing trunk group, click the name of the trunk group in the **List** pane.
   - To create a copy of an existing trunk group, click **Copy**.
   - To create a new trunk group, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the new or existing trunk group.

3. Select the **Outbound** tab.
4. Select the **Outgoing** check box.
5. Under **Network call routing**, under **Nearby area codes**, click **Add**.
6. Do one of the following:

   - Click **Add** to add a nearby area code.
   - Click **Remove** next to a nearby area code to delete that area code.

7. Click **Save**.

11.2.10 Configuring Local Prefix Exceptions

You can enter prefix exceptions against a local area code. The system handles prefix exceptions for the local area code as long distance numbers, minimizing toll charges.

For information about importing and exporting local prefix lists, see Importing Local Prefixes on page 251 and Exporting Local Prefixes on page 251.

1. In the navigation pane, click **Administration** > **System** > **Local Prefixes**. The **Local Prefixes** page opens.
2. Do one of the following:

   - To edit an existing list of local prefixes, click the name of the list in the **List** pane.
   - To create a new list of local prefixes, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays the local prefixes list.

3. Do one of the following:
   - To add a prefix, do the following:
     a. Click **Add**.
     b. In the **Area code** field, enter the area code.
     c. In the **Prefix** field, enter the prefix to create an exception for.
   - To delete a prefix, click **Remove** next to the prefix.
4. Click **Save**.

11.2.10.1 Importing Local Prefixes

You can import local prefixes from a `.txt` or `.csv` formatted file. Local prefix lists can be purchased or obtained free from various web sites. Individual records must be formatted as follows: area code, prefix (401,331).

To import local prefixes:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Local Prefixes**. The **Local Prefixes** page opens.
3. Click **New**.

   The **General** tab in the **Details** pane displays parameters for the new local prefixes.
4. Click **Import**.

   The **Import Local Prefixes** dialog box appears.
5. In the field, enter the path and name of the file to import or click **Browse** to search for the file.
6. Click **Import**.

   The **Local Prefixes edit** page appears.
7. Edit the list as needed. You can rename the list as well as add, edit, and remove prefixes.
8. Click **Save**.

The local prefix list is now available from the Local prefixes drop-down list on the **Outbound** tab in the details pane of the **Trunk Groups** page.

11.2.10.2 Exporting Local Prefixes

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **System** > **Local Prefixes**. The **Local Prefixes** page opens.
3. Click the name of the local prefixes list you want to export in the **List** pane.

> **Note**:
> The **General** tab in the **Details** pane displays the local prefixes list.

4. Click **Export**.
5. Follow the prompt to open or save the file.

11.2.11 Configuring a Pause in a Dial Out Prefix

The Pause in Dialing – Trunk Access feature allows the insertion of commas (,) into a dial out prefix associated with a trunk group. Each comma (,) specifies a one-second pause period during the transmission of pulse digits. Pause periods are permitted in the following trunk group types that send digits as pulses:

- Analog Loop Start
- Digital Loop Start
- Digital Wink Start

Example: Assume the prepend dial-out prefix of an analog trunk group is “9”. When a user dials “914085551111”, the following pulse-digit sequence is transmitted on the trunk: *“9<silence for two seconds>14085551111”*.

Feature restrictions include:

- The pause cannot be used to insert account codes.
- Commas in Connect client dial strings are ignored,.
- Commas in dial strings sent by other TAPI applications are ignored.

To include a dial pause in a dial out prefix:

1. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.
2. Do one of the following:
   - To edit an existing trunk group, click the name of the trunk group in the **List** pane.
   - To create a copy of an existing trunk group, click **Copy**.
   - To create a new trunk group, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing trunk group.

3. Select the **Outbound** tab.
4. Select the **Outgoing** check box.
5. In the **Prepend dial out prefix** field, type the dial out prefix, including a comma (,) for each pause.

   Commas are permitted anywhere within the dial out prefix.
6. Click **Save**.

11.2.12 Configuring Centrex Flash

Centrex Flash is useful in branch offices or small office environments with a limited number of analog Centrex lines. If an external caller needs to be transferred to an external number, the two trunks are cleared (instead of quickly busying-out the trunks after a few transfers). In this way, the feature reduces the number of physical trunks needed to transfer calls because no trunks are in use after the transfer is completed.

Centrex transfer is supported only on analog loop-start trunks. If the call is not on an analog loop-start trunk, the operation has no effect.

The trunk that transports the call must be configured on one of the following switches:

- ST50A
- ST100A
- ST100DA
- Voice Switch 30
- Voice Switch 50 and 50v
- Voice Switch 90 and 90v
- Voice Switch 220T1A (on analog loop-start trunk ports only)

This feature replaces a trunk-to-trunk transfer in which two trunks are tied up for the duration of the call. The current call must be connected and be a two-party call.

Note:

Centrex Flash configuration is required only on Analog Loop Start trunks.

You can program Centrex Flash on a custom button so that a Mitel user can transfer a call to another number in the PSTN. The following sequence begins when the user presses that customized button:

1. A flash is generated on the current call.
2. The central office presents a dial tone to the Mitel user.
3. The user can then dial any PSTN number.
4. Upon hearing the ring-back tone, the Mitel user completes the transfer by hanging up the handset.

For information about configuring a phone button for Centrex Flash, see Configuring Programmable IP Phone Buttons on page 327.

Note:

Because the user is directly connected to the central office, certain items disappear from consideration, as follows:

- No access code is required.
- No permissions are checked.
- No account code is supported.
- No CDR logging of the second call occurs.

11.3 Configuring Individual Trunks

This section describes how to add or modify individual trunks after you have created the associated trunk group. For information about configuring trunk groups, see Configuring Trunk Groups on page 219.

11.3.1 Viewing Trunks

The Trunks page includes a list of existing individual trunks.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunks**. The **Trunks** page opens.

For descriptions of the columns on the **Trunks** page, see Trunks Page: List Pane.

Table 70: Trunks Page: List Pane

Parameter	Definition
Name	The name of the individual trunk.
Group	The name of the trunk group that the trunk belongs to.
Type	The type of trunk (e.g., analog DID, analog loop start, SIP, etc.).
Site	The name of the trunk group site.
Switch	The IP host name of the voice switch to which the individual trunk is connected.
Port/Channel	The port number or channel to which the individual trunk is connected.
IP/FQDN	This IP address applies to SIP trunks only and corresponds to the SIP ITSP.

11.3.2 Adding or Editing an Individual Trunk

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunks**. The **Trunks** page opens.
3. Do one of the following:

   - To edit an existing trunk, click the name of the trunk in the **List** pane.
   - To create a copy of an existing trunk, click **Copy**.
   - To create a new trunk, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing trunk.

4. Review the parameters and specify values as appropriate. For descriptions of the trunk parameters, see Trunk Parameters on page 256.
5. Click **Save**.

11.3.3 Trunk Parameters

The parameters available for a trunk depend on the type of trunk group the trunk belongs to.

- PRI, BRI, Digital Loop Start, and Digital Wink Start Trunk Parameters on page 256
- Analog Loop Start and Analog DID Trunk Parameters on page 257
- SIP Trunk Parameters on page 257

11.3.3.1 PRI, BRI, Digital Loop Start, and Digital Wink Start Trunk Parameters

Trunks Page: General Tab (PRI, BRI, Digital Loop Start, and Digital Wink Start) describes the parameters for PRI, BRI, Digital Loop Start, and Digital Wink Start trunks on the General tab of the Trunks page.

Table 71: Trunks Page: General Tab (PRI, BRI, Digital Loop Start, and Digital Wink Start)

Parameter	Definition
Site	In the drop-down list, select the trunk site.
Trunk group	In the drop-down list, select the trunk group to assign the trunk to.
Name	Specifies the name of the individual trunk.
Switch channels	In the drop-down list, select the channel to which the trunk connects.
Jack #	Specifies the patch-panel jack number that is associated with the trunk's switch port. This parameter is optional.

11.3.3.2 Analog Loop Start and Analog DID Trunk Parameters

Trunks Page: General Tab (Analog Loop Start and Analog DID) describes the parameters for Analog Loop Start and Analog DID trunks on the General tab of the Trunks page.

Table 72: Trunks Page: General Tab (Analog Loop Start and Analog DID)

Parameter	Definition
Site	In the drop-down list, select the trunk site.
Trunk group	In the drop-down list, select the trunk group to assign the trunk to.
Number	Specifies the name of the individual trunk.
Switch port	In the drop-down list, select the switch port to which the trunk connects.
Jack #	Specifies the patch-panel jack number that is associated with the trunk's switch port. This parameter is optional.

11.3.3.3 SIP Trunk Parameters

Trunks Page: General Tab (SIP) describes the parameters for SIP trunks on the General tab of the Trunks page.

Table 73: Trunks Page: General Tab (SIP)

Parameter	Definition
Site	In the drop-down list, select the trunk site.
Trunk group	In the drop-down list, select the trunk group to assign the trunk to.
Name	Specifies the name of the individual trunk.

Parameter	Definition
Switch	In the drop-down list, select the switch to which the trunk connects. **Note**: Only switches that have SIP trunk resources available are displayed in the drop-down list.
IP address or FQDN	Specifies the IP address of the SIP ITSP Service Provider (or, in the case of a SIP Tie Trunk, the IP address of a Switch on a second Mitel system).
Number of trunks	Specifies the number of trunks to create on the selected trunk group. **Note**: This parameter is not visible when editing a trunk; it is only visible at the time a trunk is first created.

11.4 Forwarding Original Caller ID Outside a Mitel Network

This section describes the configuration tasks required to ensure that the original caller ID goes out an ISDN trunk when a call to a phone is forwarded outside the Mitel deployment. This section applies to all trunk groups, regardless of the way that carriers and service providers validate caller ID. This section also describes some of the operational behaviors related to forwarding the original caller ID and the different ways that carriers validate caller ID.

When a switch forwards a call out a trunk, the Q.931 SETUP message contains information about the original caller. However, carriers are not all uniform in the way they validate caller IDs and the way Caller ID is validated might not be clear to the Mitel customer. Mitel's responses to these differences are described in this section.

This section contains information about the following:

11.4.1 Carrier Validation of the Caller ID

Although many carriers and service providers validate the caller ID to ensure that then number is within the range of DID numbers that they have on record for the Mitel customer, some carriers and services providers do not.

The following sections describe what happens when carriers do or do not validate the caller ID.

11.4.1.1 When a Carrier Validates the Caller ID

Many carriers validate the caller ID to ensure that the number is within the range of DID numbers that they have on record for the Mitel customer. If the number is outside the range, the carrier could reject the call. However, the carrier usually checks the redirecting number field for a number within the DID range.

If a call enters a Mitel network and is then forwarded out an ISDN trunk to a remote device, the number of the forwarded caller can be outside the DID range on record. If the caller ID is outside the DID range, the carrier can check the content of the Redirecting Number Information Element (RNIE) to see if the number that forwarded the call is within the DID range. The redirecting number belongs to the Mitel user whose phone forwarded (redirected) the original call. Therefore, the contents of the RNIE field will match the carrier's records. The result is that the call is forwarded, and the far end device displays the ID of the original caller.

Although most carriers that verify the RNIE send the original caller ID, some carriers automatically forward the RNIE contents instead of the original caller ID. In this situation, the original caller ID does not reach the outside terminating device.

11.4.1.2 When a Carrier Does Not Validate the Caller ID

Some carriers and service providers do not validate the caller ID, so they do not determine what information is provided at the destination phone. Therefore, a Mitel user who is remote might not see the original caller ID, even with the correct configuration on the Voice Switch. To address this uncertainty, Mitel supports an *RNIE ISDN profile* that determines the information the carrier displays (even though the provider does not validate the caller ID). For information about configuring an RNIE ISDN profile, see Configuring an ISDN Profile for RNIE on page 274.

11.4.2 Purpose of the Billing Telephone Number for Caller ID

In general, the billing telephone number (BTN) is used by carriers for billing a Mitel customer. In contrast, a different role exists for the Billing telephone number (BTN) field in trunk group configuration. The BTN entered in this field is not used for billing purposes, but rather for supporting an alternative to individual user DIDs when an alternate is needed. For example, for a switch to forward the original caller ID, the Mitel user who redirects the call outside must have a DID and a Caller ID entry (on the Users page) that fit within the trunk group's DID range. However, for a variety of reasons, a user might not have a DID or a number within the trunk's DID range. For example, a Mitel user at a remote site would have a telephone number that is outside the DID range at the location of the server. In this case, the number in the Billing telephone number (BTN) field goes in the RNIE space in place of the user's DID number.

Note:

The Enable original caller information check box and the Billing telephone number (BTN) field are available on the Trunk Groups page. When the Enable original caller information check box is selected, the Billing telephone number (BTN) field becomes active and is automatically populated with the CESID configured on the server.

A Q.931 SETUP message contains information elements for the caller ID and a redirecting number. The carrier normally finds the caller ID to be within the DID range for the trunk. If the caller ID is outside the range, the provider checks the RNIE field to determine whether the number that redirected the call is within the DID range. If the Mitel user does not have a DID to serve as the caller ID, the Billing telephone number field on the Trunk Groups page can provide the redirecting number. This field can contain one of several types of phone numbers.

The preferred order of values to use in the Billing telephone number (BTN) field is as follows:

1. The first number in the trunk group's DID range (this is the default).
2. The actual BTN of the Mitel customer (used by the carrier for billing purposes).
3. The CESID (if the trunk group is configured to support CESID).

Note:

In Release 11.1, the Billing telephone number field was added to the Trunk Groups editing window. Some customers who upgrade might not know about this field. Regardless, the field is automatically populated with the base number of the DID range when the original caller information function is enabled.

11.4.3 Important Issue with Early Implementations of Original Caller ID

The information in this section does not apply to new installations; Release 11.2, 12.1, 12.2, and so on. This issue does not exist for new installations.

In releases ST11, ST10.2, ST10.1, and ST10, the forwarding of the original caller ID to an outside device relied on custom dial plan elements from Mitel TAC. If TAC implemented such a custom dial plan, TAC must remove the elements related to this function before the current capability can work. (This issue does not exist for customers whose *new installation* contains the present implementation described in this book.)

If a system with such a dial plan is upgraded, problem behaviors related to call forwarding or original caller ID can occur. Some possible behaviors are:

- Forwarded calls go to the user's voice mail instead of out the trunk.
- Forwarded calls are rejected by the carrier.

Upgraded customers who know or suspect that such a custom dial plan has been used should contact TAC for help. However, some customers might not know that a custom dial plan has been used for original caller ID. These customers should, therefore, monitor the call forwarding and caller ID performance after an upgrade.

11.4.4 Enabling Original Caller Information

1. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups**. The **Trunk Groups** page opens.
2. Do one of the following:

   - To edit an existing trunk group, click the name of the trunk group in the **List** pane.
   - To create a copy of an existing trunk group, click **Copy**.
   - To create a new trunk group, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing trunk group.

3. Select the **Outbound** tab.
4. Select the **Outgoing** check box.
5. Under the **Trunk services**, select the **Enable original caller information** check box.

Note:
The Billing telephone number (BTN) field is automatically populated with the base number of the DID range (if a DID range has been configured).

6. If required, enter a value in the **Billing telephone number (BTN)** field.
7. Click **Save**.

Note:
For a user to receive forwarded calls, the user must belong to a user group with a class of service (COS) that supports the call forwarding features. Trunk-to-trunk transfer and external call forwarding and find me destinations must be enabled for the COS enabled for the user. For more information about configuring a COS, see Configuring a COS for Telephony Features Permissions on page 461.

11.5 Introduction to ISDN Profiles

ISDN profiles are advanced tools that can be used to specify important information for a variety of features. ISDN profiles allow the system administrator to specify functions that extend the normal capabilities of Mitel trunks. The additional capabilities are enabled in the ISDN profile by the specification of information elements (IEs). After creating an ISDN profile, the profile is applied as needed to one or more PRI SGT1, BRI, or PRI SGE1 trunk groups. ISDN profiles are advanced tools because their purpose is outside the normal use of a Voice Switch.

In the two-stage implementation process, a function-specific ISDN profile with one or more manually typed parameters first is created and subsequently applied to a trunk group.

Example applications of ISDN profiles are as follows:

- For WANs in which a carrier or service provider does not automatically add the caller ID (CID) name, a CID name can be added to outbound calls. For a detailed description of this function, see Configuring Caller ID Name on SGT1-PRI Trunks on page 263.
- In Europe, up to 25 digits for a SETUP can be required for ISDN BRI and PRI. To provide these digits, the switch normally passes 20 digits in the SETUP message but can add 5 digits when necessary. For a description of this capability, see Configuring an ISDN Profile for SETUP Message on page 268.
- In Europe, an ISDN profile can direct the switch to support ISDN channel negotiation by the central office (only for outbound calls from a switch in the current release). For a description of this capability, see Configuring Euro-ISDN Channel Negotiation on page 270.
- In Europe, an ISDN profile can be created that allows an outside caller to a Mitel user to see the number of the Mitel user that answers the call. This feature is supported for carriers or service providers configured with PRI or BRI. For a description of this capability, see BRI Signaling Parameters on page 174.
- To meet a requirement of compliance testing in Europe, an outbound call can carry the progress indicator value 8. This ISDN profile for this function should be applied on a trunk only during a period of compliance testing.

11.6 Configuring Caller ID Name on SGT1-PRI Trunks

The Caller ID Name on SGT1-PRI function allows a Voice Switch to add the user name to caller ID (CID) information in an outbound call. The function is available on SGT1-PRI trunks but not BRI or SGE1-PRI trunks.

Prior to Release 11.2, Voice Switches did not send the user's name to carriers or service providers. Nevertheless, in the U.S., carriers and service providers could add the caller number and caller name (if the call originated on a Voice Switch).

Note:

Caller ID Name on SGT1-PRI is optional because most Mitel installations utilize the default state of Mitel's underlying CID mechanism. Therefore, only certain installations need the functionality of Caller ID Name on SGT1-PRI. Mitel created this function specifically for non-U.S. customers whose carrier or service provider needs the support of Caller ID Name on SGT1-PRI. Whether this function is really needed can be determined through consultation with the carrier or service provider if the actual need is unclear.

The following steps are required to configure CID name on SGT1-PRI trunks:

1. Understand CID name handling on the public network. See Understanding Caller ID Name on the Public Network on page 264 for more information.
2. Enable outbound calling name on the SGT1 Voice Switch with the PRI trunk that is to send the CID name. See Enabling Outbound Caller ID Name for SGT1-PRI on page 265 for more information.
3. Configure an ISDN profile for specifying the display method for CID name. See Configuring an ISDN Profile for CID Name on page 266 for more information.
4. Associate the ISDN profile with the desired trunk group. See Associating an ISDN Profile with a Trunk Group on page 277 for more information.
5. Enable CID name for the trunk group. See Enabling Caller ID Name for a Trunk Group on page 268 for more information.

11.6.1 Understanding Caller ID Name on the Public Network

This section provides an overview of the current handling of Caller ID names for outbound and inbound calls.

11.6.1.1 Inbound

In North America, some carriers can provide a Caller ID (CID) name in addition to the CID number. In the current release, voice switches support CID names on SGT1 PRI trunks. A carrier or service provider can deliver the CID name using either a display message or facility message method. The method depends on the protocol used, as follows:

- In a display message over NI-1
- In a facility message over NI-2

For CID name for an inbound call, switches support both methods at the same time, so no special configuration is required on a switch to accommodate the arrival of CID names.

11.6.1.2 Outbound

SGT1 voice switches can send a CID name for an outbound call using either a display message or a facility message. In contrast to inbound calls with a CID name, all outbound calls are configured to use either the display message or facility message method. The choice of method for outbound calls must be specified in Connect Director. Even as SGT1 voice switches support only NI-2 protocol, it is possible to create an ISDN profile for using NI-2 protocol and then specify either the display message or facility message method for outbound CID name delivery. For more information about this ISDN profile, see Configuring an ISDN Profile for CID Name on page 266.

The message method must match the method that the carrier or service provider expects. For example, if a carrier uses NI-1, programming NI-2 with the display method might be possible, such that the carrier accepts the outbound caller ID name from Mitel.

For the steps needed to select the message method and protocol, see Configuring an ISDN Profile for CID Name on page 266. These steps apply only to outbound calls.

11.6.1.3 Caller ID Name on SGT1-PRI Background Details

This section contains additional details that should be understood before implementing CID on SGT1-PRI.

Outside the U.S.—as in Canada, for example—the carrier or service provider might insert the geographic or metropolitan origin of the call as the CID name (“Coquitlam,” for example). However, to send the actual user name of the caller, some carriers or service providers outside the U.S. require the information provided by Caller ID Name on SGT1-PRI. Therefore, for customers in Canada and elsewhere who want a CID name to accompany the call, this function enables a Voice Switch to provide the CID name information.

11.6.1.4 Character Limit and Name Masking

The maximum number of characters that a CID name supports is 34. Although Mitel supports up to 34 characters, a carrier or service provider might truncate the CID name. It might, for example, pass only 16 or even 12 characters. This possibility is one of the reasons that customers must know the support provided and consult as needed with the carrier or service provider.

Note:

For privacy reasons, the actual name can be masked by inserting a generic label; see Enabling Caller ID Name for a Trunk Group on page 268 for more information.

11.6.2 Enabling Outbound Caller ID Name for SGT1-PRI

Some configuration steps for CID are mandatory, regardless of the carrier or service provider and regardless of whether the network calls for an ISDN profile to activate Caller ID Name. An example of such a mandatory step is enabling the sending of CID name on an outbound call. This step is required for sending a name in the CID, but in some countries a carrier or service provider might require additional configuration supplied by an ISDN profile configured specifically for the purpose of facilitating Caller ID Name for SGT1-PRI.

Note:
Before enabling the Caller ID Name on SGT1-PRI function, the administrator should have prior knowledge or else consult the customer's carrier or service provider to determine how the carrier delivers the CID name end-to-end and, therefore, whether the display method is required. (See also Configuring an ISDN Profile for CID Name on page 266.) Furthermore, although the Voice Switch sends the caller ID name when configured to do so, Mitel cannot guarantee the results at the far end. Mitel cannot guarantee that carriers or service providers deliver caller ID names at the far end or that they support overwriting of the user name with a user-specified word. Also, in some cases, parameters on 3rd-party gateways might require modification before the caller ID name can be delivered.

To enable outbound CID name for SGT1-PRI:

1. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
2. In the **Name** column, click the name of the SGT1 Voice Switch with the PRI trunk that is to send the CID name.

Note:
The **General** tab in the details pane displays parameters for the switch.

3. Select the **Switch** tab.
4. Under **Layer 3**, in the **Protocol type** list, select **ISDN User**.
5. In the **Central office type** list, select **NI-2**.
6. Select the **Enable outbound calling name** check box. (This check box is just above the area labeled Layer 1).

11.6.3 Configuring an ISDN Profile for CID Name

This section defines the ISDN profile for Caller ID Name on SGT1-PRI and describes how to configure an ISDN profile for a SGT1-PRI trunk.

In most deployments, the default ISDN system profile is already part of the configuration and the default ISDN system profile has already been associated with the trunk group. The ISDN profile for CID Name on SGT1-PRI specifies the method used for delivering a CID name to the carrier or service provider.

The following list shows the possible methods related to CID:

- CallerIDSendMethod – display
- CallerIDSendMethod – displaypcc
- CallerIDSendMethod – facility
- CallerIDSendMethod – facilitypcc

As has been emphasized, the customer must know what the carrier or service provider expects for the ISDN message method. However, even when the expected method is known, an administrator might have to perform a simple experiment to determine which of the two possible categories of each method is required. In all deployments, the facility method is enabled by default. However for some WANs, a different method is required. To use one of these message methods, a new ISDN profile must be created.

Note:

The choice for using the “pcc” version of a method is not based on information that the carrier provides. For example, if a customer has settled on the display method (CallerIDSendMethod = display) in the ISDN profile and correctly applied the profile to the pertinent trunk group but the CID name is not received at the far end, then an alternative ISDN profile (with CallerIDSendMethod = displaypcc) must be applied to the trunk group.

11.6.3.1 Creating ISDN Profile for Specifying DM for CID Name

To meet the interoperability requirements for CID name as needed in some environments, the system administrator creates an ISDN profile that specifies one of two display methods for sending CID names. (If the need for the display method is uncertain, refer to Introduction to ISDN Profiles on page 262 and other conceptual descriptions of the CID name on SGT1-PRI function in this section.)

To create an ISDN Profile for specifying the Display Method (DM) for CID Name, perform the following steps:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **ISDN profiles**.
3. Click **New** to create a new ISDN profile.

Note:
The **General** tab in the **Details** pane displays parameters for the ISDN profile.

4. In the **Name** field, enter the name for the ISDN profile.

> **Note**:
> The name of the default profile SystemISDNTrunk is reserved and cannot be used for new profiles. The SystemISDNTrunk profile cannot be edited.

5. Select the **Enable** check box.
6. In the **Custom parameters** field, enter the following:

   CallerIDSendMethod – display (or **displaypcc**, as needed)
7. Click **Save**.

11.6.4 Enabling Caller ID Name for a Trunk Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups**. The **Trunk Groups** page opens.
3. In the **Name** column, click the name of the trunk group for which to enable CID name.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the trunk group.

4. Select the **Enable caller ID name** check box.
5. Optional: To overwrite all outbound CID names, enter the label to use as the CID name in the **When Site Name is used for the Caller ID, overwrite it with** field.
6. Click **Save**.

11.7 Configuring an ISDN Profile for SETUP Message

In Europe, a SETUP message with up to 25 digits may be required for ISDN BRI and PRI trunks. To provide 25 digits when necessary, a Voice Switch can add 5 digits to the 20 digits it normally sends in the U.S.

After the terminal equipment (TE) initially receives the SETUP ACK (Setup Acknowledge) message from the network terminal (NT), the Mitel TE can send five digits to the network terminal in the subsequent INFO message if the situation requires those digits.

For the implementation of this messaging, the switch indicates when the extra 5 digits are not needed (thus, a 25-digit SETUP message is the default). As the configuration steps illustrate, a message named Sending Complete indicates that the additional 5 digits are not needed. Note that, by itself, the Sending Complete message does not directly pertain to the European requirement for 25-digits in a SETUP message. It simply indicates that, for no specific reason, more digits are not required. This message is delivered in 1 of 2 ways:

- The Sending Complete message can go out after the SETUP ACK message arrives. This behavior is the default and does not involve an ISDN profile.
- The Sending Complete message can go out in the SETUP message. This requires an ISDN profile.

11.7.1 Creating an ISDN Profile for a 20-Digit SETUP Message

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **ISDN Profiles**. The **ISDN Profiles** page opens.
3. Click **New** to create a new ISDN profile.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the ISDN profile.

4. In the **Name** field, enter the name for the ISDN profile.

> **Note**:
> The name of the default profile SystemISDNTrunk is reserved and cannot be used for new profiles. The SystemISDNTrunk profile cannot be edited.

5. Select the **Enable** check box.
6. In the **Custom parameters** field, do one of the following:
   - Enter **OVLSendCmpWithSetup – yes** to carry the *Sending Complete message* in the SETUP message.
   - Enter **OVLSendCmpWithSetup – no** to transmit the *Sending Complete message* through the Voice Switch after the switch receives the SETUP ACK message.
7. Click **Save**.

Note:
After it is configured, the ISDN profile must be applied to the appropriate trunk group. See Associating an ISDN Profile with a Trunk Group on page 277 for information about assigning an ISDN profile to a trunk group.

11.8 Configuring Euro-ISDN Channel Negotiation

A Voice Switch can be configured in Connect Director to allow a central office (CO) to negotiate the choice of an outbound ISDN channel on a PRI or BRI.

This feature is supported for Euro ISDN for PRI and BRI.

Note:

This feature does not apply to inbound calls. Also, this feature is not supported for North America ISDN protocols (for example, NI2, DMS, and ESS).

11.8.1 Configuring ISDN Channel Negotiation

A Mitel system selects the outbound ISDN bearer channel and does not negotiate with the central office (CO) for the choice of channel. This behavior is called exclusive mode.

In Europe (or in any ETSI-compliant network), an ISDN profile can be configured in Connect Director to enable the Voice Switch to allow the CO to negotiate the channel.

The behavior that supports negotiation is called preferred mode. Although this function is available to BRI, it is more relevant to PRI.

The following steps are required to configure Connected Number Display for outside callers:

1. Configure an ISDN profile for ISDN Channel Negotiation. See Creating an ISDN Profile to Enable ISDN Channel Negotiation on page 271 for more information.
2. Associate the ISDN profile for Connected Number Display with the desired trunk group. See Associating an ISDN Profile with a Trunk Group on page 277 for more information.
3. Configure the switch for ISDN channel negotiation. See Configuring a Switch for Euro-ISDN Channel Negotiation on page 271for more information.The following trunk and switch settings are available in Connect Director after an ISDN profile is created:

11.8.1.1 Creating an ISDN Profile to Enable ISDN Channel Negotiation

For backwards compatibility, the default for channel negotiation remains exclusive mode. Therefore, ISDN channel negotiation must be enabled through an ISDN profile that enables the preferred mode.

1. In the navigation pane, click **Administration** > **Trunks** > **ISDN Profiles**. The **ISDN Profiles** page opens.
2. Click **New** to create a new ISDN profile.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the ISDN profile.

3. In the **Name** field, enter the name for the ISDN profile.

> **Note**:
> The name of the default profile SystemISDNTrunk is reserved and cannot be used for new profiles. The SystemISDNTrunk profile cannot be edited.

4. Select the **Enable** check box.
5. In the **Custom parameters** field, enter the following:

   ChannelPreferredMode=yes

> **Note**:
> Custom Parameters are case sensitive.

6. Click **Save**.

11.8.1.2 Configuring a Switch for Euro-ISDN Channel Negotiation

This section describes how to configure a switch parameters that apply to ISDN channel negotiation.

1. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
2. Do one of the following:

   - To edit an existing switch, click the name of the switch in the **List** pane.
   - To create a new switch, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing switch.

3. Select the **Switch** tab.
4. Under **Layer 3**, in the **Protocol type** list, select **ISDN User**.
5. In the **Central office type** list, select **Euro-ISDN**.

Note:
For information about configuring the remaining parameters for the switch, see Configuring Primary Voice Switches and Service Appliances on page 162.

6. After setting all desired parameters for the switch, click **Save**.

11.9 Configuring Connected Number Display for Outside Callers

An ISDN profile can be created in Connect Director to allow an outside caller to see the number of a Mitel user that answers the call.

This feature is supported for carriers or service providers configured with Euro-ISDN PRI or BRI.

Note:

This feature is not supported for Mitel deployments for North America Protocol (for example, NI-2, DMS, and ESS). Also, this feature is not supported for ISO QSIG or ECMA QSIG.

When an outside caller calls a Mitel user and the Mitel user answers the call, the phone number of the Mitel user is sent back to the outside caller through the CONNECT message. The phone number of the Mitel user can be the user's DID or the BTN associated with the trunk group.

The following steps are required to configure Connected Number Display for outside callers:

1. Configure an ISDN profile for Connected Number Display. See Configuring an ISDN Profile for Connected Number Display on page 273 for more information.
2. Configure the BTN for the trunk group that the ISDN profile will be associated with. See Purpose of the Billing Telephone Number for Caller ID on page 260for more information.
3. Associate the ISDN profile for Connected Number Display with the desired trunk group. See Associating an ISDN Profile with a Trunk Group on page 277 for more information.
4. Configure the switch for ISDN channel negotiation. See Configuring a Switch for Euro-ISDN Channel Negotiation on page 271 for more information.

11.9.1 Configuring an ISDN Profile for Connected Number Display

An ISDN profile for controlling the display of the Mitel user’s number on the caller’s phone can have one of three possible keyword settings and results, as follows:

- **useBTN** - The Voice Switch sends only the BTN specified for the trunk group in the CONNECT message to the service providers or carrier. The outside caller sees the Connected Number Display (the BTN specified for the trunk group).
- **present** - The Voice Switch sends the user’s DID or the BTN specified for the trunk group in the CONNECT message to the service providers or carrier. The outside caller sees the Connected Number Display (the user’s DID or the BTN specified for the trunk group).
- **restrict (default)** - The Voice Switch sends neither the user’s DID nor the BTN specified for the trunk group in the CONNECT message to the service providers or carrier. The outside caller does not see the Connected Number Display.

11.9.1.1 Creating an ISDN Profile for Connected Number Display

To create an ISDN profile in Connect Director that allows a caller to see the Mitel user’s DID (keyword –present), perform the following steps:

1. In the navigation pane, click **Administration** > **Trunks** > **ISDN Profiles**. The **ISDN Profiles** page opens.
2. Click **New** to create a new ISDN profile.

Note:
The **General** tab in the **Details** pane displays parameters for the ISDN profile.

3. In the **Name** field, enter the name for the ISDN profile.

Note:
The name of the default profile SystemISDNTrunk is reserved and cannot be used for new profiles. The SystemISDNTrunk profile cannot be edited.

4. Select the **Enable** check box.
5. In the **Custom parameters** field, enter the following:

ConnectedLine – present

Note:
The Custom parameters are case sensitive.

6. Click **Save**.

11.10 Configuring an ISDN Profile for RNIE

This section defines the ISDN profile for the Redirecting Number Information Element (RNIE). The purpose of this profile is to ensure delivery of an original caller ID to a remote device when the carrier or service provider does not validate the caller ID fields and, therefore, has no strategy for delivering the caller ID. Specifying an ISDN profile for RNIE is an advanced task for a network scenario where the default state of the trunk group is not appropriate after original caller ID is enabled (See Enabling Original Caller Information on page 261 for information about enabling original caller information).

Note:

No consultation with the carrier is necessary for the use of an ISDN profile for RNIE even though, in general, knowledge of how the carrier or service provider communicates at the trunk level is helpful.

11.10.1 Sequencing Numbers in the Q.931 SETUP Message

The ISDN profile for RNIE determines which of two possible sequences the Voice Switch uses to send the caller ID and the RNIE in the outbound Q.931 SETUP message. The sequence needed depends on how the carrier processes the SETUP message. Rather than depending on operational information from the provider, the customer decides which ISDN profile to use based on whether the original caller ID is reaching the far-end destination after a call-forwarding feature sends the calls out an ISDN trunk.

If the original caller ID does not reach the far-end device after trying both sequences in the ISDN profile, the customer should ensure that the other requirements of caller ID are configured correctly. As described later in this section, even if the Voice Switch is correctly forwarding the original caller ID outside the local network, conditions in the WAN might obstruct the successful arrival of caller ID at the destination.

The outbound Q.931 SETUP message has two caller ID fields, as follows:

- The caller ID. This number is either of the following:
  - The Mitel user's DID or the contents of the Billing telephone number (BTN) field
  - The number of the outside caller who called the Mitel user and whose call was subsequently forwarded out the trunk
- The redirecting number—the Mitel number that forwarded the original call, if call-forwarding was performed. (If the call was not forwarded, there is no redirecting information.) This number is either of the following:
  - The DID of the Mitel user who forwarded the call (if the user has a DID)
  - When necessary, the contents of the Billing telephone number (BTN) field

This redirecting number can be the base number in a trunk's DID range, the Mitel customer's BTN, or the CESID. These alternatives to the DID are described in Purpose of the Billing Telephone Number for Caller ID on page 260.

Note:

- If a carrier forwards an original caller ID to another provider, such as a CLEC, the subsequent provider might reject the call. This call rejection could be due to the subsequent provider utilizing the caller ID and RNIE in the opposite sequence of the first provider to transport the call. In this case, when the customer has determined that forwarded calls are being rejected at the far end and has consulted with Mitel TAC, an ISDN profile cannot help. The way to re-establish delivery of the forwarded calls through the CLEC—but without original caller ID—is to clear the **Enable original caller information** check box (see Enabling Original Caller Information on page 261) until carriers and service providers find a way to interoperate in a way that ensures delivery of caller ID.
- Different carriers or carrier regions can use different call parameters. Therefore, we recommend that a unique ISDN profile be created for each trunk group.

11.10.2 Creating an ISDN Profile for RNIE

An ISDN profile for RNIE can have one of two lines that specify its effect. The line must be typed according to the following syntax:

- **SEND_BTN_AS_RNIE = yes (default)**

Note:
The caller ID is presented to the calling party. The BTN is sent as the number to which the call must be redirected (if the **Enable original caller information** option is enabled).

- **SEND_BTN_AS_RNIE = no**

Note:
The BTN is presented to the calling party. The caller ID is sent as the number to which the call must be redirected (if the **Enable original caller information** option is enabled).

To create an RNIE ISDN profile:

1. Do one of the following:
   - In the navigation pane, click **Administration** > **Trunks** > **ISDN Profiles**.
   - In the navigation pane, click **Administration** > **Trunks** > **SIP Profiles**.
2. Do one of the following:
   - To edit an existing profile, click the name of the profile in the list pane.
   - To create a new profile, click **New**.
3. In the **Name** field, enter the name for the ISDN profile.

Note:
The name of the default profile SystemISDNTrunk is reserved and cannot be used for new profiles. The SystemISDNTrunk profile cannot be edited.

4. Select the **Enable** check box.
5. In the **Custom parameters** field, do one of the following:
   - Enter **SEND_BTN_AS_RNIE = no** to specify that the switch presents the BTN associated with the trunk group.
   - Enter **SEND_BTN_AS_RNIE = yes** (default) to specify that the switch presents the caller ID.
6. Click **Save**.

Note:
After it is configured, the ISDN profile must be applied to the appropriate trunk group. See Associating an ISDN Profile with a Trunk Group on page 277 for information about assigning an ISDN profile to a trunk group.

11.11 Associating an ISDN Profile with a Trunk Group

After an ISDN profile with the desired display method for CID name is created, the ISDN profile must be associated with the trunk group.

Note:
ISDN profiles are only valid for PRI and BRI trunk groups.

Many companies might choose to hide the personal name of the caller and instead insert the company name. As the following steps show, the system administrator can specify a label to overwrite all outbound CID names (and thus mask the call initiator's name).

Associating the ISDN profile with a trunk group:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups**. The **Trunk Groups** page opens.
3. In the **Name** column, click the name of the trunk group to which to associate the ISDN profile.

Note:
The **General** tab in the **Details** pane displays parameters for the trunk group.

4. In the **Profile** list, select the desired ISDN Profile.
5. Click **Save**.

11.12 Support for Mexico National Numbering Plan

Overview

This section describes the requirements for MiVoice Connect support for the new Mexico National Numbering plan.

The new Mexico National Numbering plan requires all subscriber numbers to be 10 digits. Combining the former areas codes with the local numbers gives the new national 10-digit number. Dialing a national number always requires 10 digits, whether for local calls or for long-distance calls.

11.12.1 Principal Numbering Plan Changes

Prefixes

The former numbering plan required the use of several prefixes. The new plan does not require these prefixes for all intra-Mexico dialing. Prefixes used in the former plan are listed in the following table:

Table 74: Prefixes (Earlier Plan)

Prefix	Description
01	Long distance.
044	Fixed line to local mobile; local calling party pays.
045	Fixed line to distant mobile; national calling party pays.
01	For non-geographic numbers such as 800- or 900-n umbers.

Note:

These prefixes are followed by 10 digits—area code + local number.

11.12.1.1 Service Numbers

For special services, the 3-digit special services numbers remain unchanged. These numbers are of the form 0nx. These are non-routable numbers that will be passed to the PSTN from the local switch.

For emergency service numbers, 911 remains the emergency number and does not change.

Note:
No other number can begin with 911.

11.12.1.2 International Calling From Mexico

International calls from Mexico to other countries are prefixed with “00” followed by the country code and destination national number. An international number might contain an arbitrary number of digits. The “00” prefix identifies the number as an international number.

11.12.1.3 Calling Party Pays (CPP) Mobile Numbers

Calls involving mobile numbers are charged by the minute (compared with fixed line calls, which are charged per call). Mobile numbers might be set up as Mobile Party Pays or Calling Party Pays. The earlier numbering plan used prefixes to designate Calling Party Pays mobile numbers; the new numbering plan removes these prefixes.

In addition, numbers in the new plan are managed in large numbers of small blocks, making a rules-based approach to CPP determination prohibitive. The *Instituto Federal de Telecomunicaciones* (IFT) regularly maintains and publishes a list of national numbers indicating which blocks are CPP.

11.12.1.4 Dialing PSTN Numbers From Systems Located in Mexico

Any numbers dialed after the Trunk Access Code must conform to Mexico's new national numbering plan to be recognized as properly formed by the PSTN. Properly formed numbers are either directed out at the local switch over trunks to the PSTN or they are further processed by routing tables for redirection to the PSTN through other locations within the MiVoice Connect system.

There are no longer any prefixes except for international long distance calls to other countries, which are prefixed by "00".

A properly formed number passed from the PBX to the PSTN must be in one of the following three forms:

- 3 digits
  - 911
- 3 digits
  - First digit must be 0
  - Second digit must be 2 - 9
  - Third digit must be 0 - 9
- 10 digits
  - First digit must be 2 - 9
  - Second digit must be 1- 9
  - Third digit through must be 0 - 9
  - First three digits must not be 911

Any number that meets any of these requirements is complete and might be immediately processed as a PSTN number. Under the new numbering plan, a normal Mexico national subscriber number or a non-geographic number will always be 10 digits, regardless of location or whether or not it is a fixed line or mobile line. The exceptions are 911 and the 3-digit special service numbers.

An international number dialed from Mexico will be prefixed by "00"" (after the Trunk Access Code) and might contain an arbitrary number of digits after the "00". The completeness of the dialed number will be determined within the expiration of the interdigit timer that starts after the user stops entering digits, or after the user presses **#** to signal the end of the dialed string.

11.12.2 MiVoice Connect Requirements

This section describes the Mexico Dial Plan requirements for MiVoice Connect

Note:
There are no changes to any internal system calling involving extension or internal numbers.

11.12.2.1 Calls to PSTN

Generally, accommodation for the new Mexico National Numbering Plan will make use of existing facilities in MiVoice Connect, with some additional requirements. The areas that are affected involve defining numbers for various purposes and implementing permissions and restrictions for trunk groups and user classes of service.

Call permissions and restrictions in MiVoice Connect are as follows:

- Internal only
- Local only
- National long distance
- National mobile
- International long distance
- All calls

Normally restrictions are rules-based. For the new Mexico numbering plan, this continues to be the case except for National mobile calls.

Local Area Code Requirements for MiVoice Connect

The **Local Area Code** fields must permit entry of Mexico's 2-digit and 3-digit area codes. Mexico's largest population centers such as, Mexico City, Guadalajara, and Monterrey have 2-digit area codes; all other areas have 3-digit area codes.

The following local area code fields must permit 2- and 3-digit area codes:

- Sites
  - Local area code
  - Additional local area codes

- Trunk Groups/Outbound/Network call routing
  - Local area code
  - Additional local area codes
  - Nearby area codes

Note:
These fields are used for network call routing and digit manipulation.

Permissions and Restrictions

Trunk groups and User class of service allow administrators to select restrictions based on level categories. The following Connect Director pages allow the setting of restrictions:

- **Trunk Group** > **Outbound** > **Trunk Services**
- **Users**> **Class of Service** > **Telephony Feature**
- **Users** > **Class of Service** > **Call Permissions**

11.12.2.2 National Mobile CPP Treatment

If the **COS - Call Permissions** option is selected for the **National Mobile** field in Connect Director, then calls to national mobile numbers will be permitted without any checking. If the **Local only** or the **Long Distance Calling** option is selected, then calls to Mobile CPP will be restricted. The dialed number will then be examined to determine whether it is a CPP number on the IFT's published list. If the number is listed as a CPP number, then the call will not be allowed (including, for example, call forwarding in the case of Telephony Feature Permissions).

11.12.2.3 Using the Mitel Outbound Call Blocker Application

For Mexico, the Mitel Outbound Call Blocker application is available separately for installation on the HQ Server to restrict the Mobile CPP numbers.

Note:
For Mexico, there is no license fee for the Mitel Outbound Call Blocker application.

11.12.3 Mitel Outbound Call Blocker Application

Overview

Note:
The Mitel Outbound Call Blocker application is intended only for users of Mexico Dial Plan.

The Mitel Outbound Call Blocker application prevents outgoing calls to numbers listed in the call block list. For an Outbound Trunk call, If the called number is present in the call block list the call is disconnected. The service is configured to compare all the digits of the blocked number.

Mitel Outbound Call Blocker application is provided as a standard Windows server application and can be run as needed. The application must be installed only on the Headquarters (HQ) server. It provides a user interface to specify a list of numbers to be blocked (provided by *Mexican Instituto Federal de Telecomunicaciones (IFT)*) and to enable stopping and starting the Outbound Call Blocker application service.

For instructions to install and configure the Mitel Outbound Call Blocker application, see the *Mitel Outbound Call Blocker Advanced Application – App Note* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform

Configuring IP Phones 12

This chapter contains the following sections:

This chapter discusses how to configure IP phones.

12.1 Overview

MiVoice Connect supports IP phones connected through voice switches. After installing the phones, configuring IP phones is a straightforward process that involves defining settings in Connect Director.

Supported IP and DECT Phones

The following IP phones are supported in MiVoice Connect:

- IP100-, IP200-, IP500-, and IP600-Series phones
- 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones

Note:

Currently, 6970 phones are supported as third-party SIP devices.

- DECT 112

Note:

- The SIP transport supported on DECT 112 is UDP.
- MiVoice Connect does not support **SRTP Auth**. This option should be disabled always.

Note:

- MiVoice Connect and DECT 112 supports SRTP and RTP.
- MiVoice Connect does not support TLS and TCP connections for third-party phones.
- Currently, MiVoice Connect supports TLS 1.2 connection.
- 6900-Series IP phones support the download of configuration files from MiVoice Connect using HTTPS with TLS 1.2.
- Mitel 6970 IP phones only support firmware version 6.0 with MiVoice Connect 19.2 SP1 or higher versions. MiVoice Connect Release 19.2 or previous releases is not supported with firmware version 6.0.
- Beginning with MiVoice Connect Release 19.3 and phone firmware Version 6.2.0, 6900-Series (6910, 6920, 6930, and 6940) phones have teleworker support (with InGate). This will allow 6900-Series phones that are in remote locations to communicate with the MiVoice Connect server hosted in a customer on-premises location.

12.1.1 Prerequisites

Before configuring IP phones through Connect Director, be sure that you've addressed the following prerequisites which involve setting up your network and installing the phones:

- Add and configure voice switches to support IP phones. For information on allocating switch ports for IP phone support, see Configuring Primary Voice Switches and Service Appliances on page 162.
- Set IP address ranges. For more information, see the *MiVoice Connect Planning and Installation Guide*.
- If you are using static IP addresses, set the boot parameters in the individual IP phones. For more information, see the *MiVoice Connect Planning and Installation Guide*.

When you have completed the installation process, connect the IP phones to the network. Phones connected to the network register themselves with the MiVoice Connect system.

12.1.2 IP Phone Configuration Overview

Configuring IP phones involves the following steps, many of which are optional:

- Configure system settings
- Add IP phones to the system
- View and edit IP phones
- Customize ringtones
- Customize wallpaper
- Specify custom applications for user groups
- Specify automatic off-hook for wireless headsets
- Configure programmable IP phone buttons
- Configure VPN phones
- Configure simultaneous ring and call move

12.2 Configuring System Settings for IP Phones

In addition to configuring the IP address range for phones, which you did as part of the installation process, you need to set IP phone options.

12.2.1 Reviewing the IP Phone Address Map

All IP phones are assigned to Headquarters by default. If Headquarters is your only site, you do not need to set IP address ranges. If you have more than one site with IP phones, you must set an IP address range for each site other than Headquarters. Details about the parameters on the IP Phone Address Map page are provided in IP Phone Address Map.

The following are the IP address mappings that you can create:

- IP address range based: This is used to determine the site the phone is registered to and also to derive the CESID/callback number.
- MAC based entry: This is used only to derive the CESID/callback number.

For teleworker phones, MAC address based entry is mandatory for RAY BAUM conformance. If an administrator wants a teleworker phone to register to a particular site, then an IP based address map must be created based on the EGW private IP range with following conditions:

- No CESID number must be assigned to this entry.
- No callback number must be assigned to this entry.

Example:

If the private IP range configured in EGW is in the range 192.168.1.1 to 192.168.1.10, the teleworker phone MAC address will be 00:01:02:03:04:AA and 00:01:02:03:04:BB. In this scenario, the IP address range for the entries will be as shown in the following tables.

Table 75: IP Address Range Entries - Part 1

Low IP	High IP	MAC	CESID
192.168.1.1	192.168.1.10	Blank	Blank
Blank	Blank	00:01:02:03:04:AA	ID_1
Blank	Blank	00:01:02:03:04:BB	ID_2

Table 76: IP Address Range Entries - Part 2

Callback	TeleworkerEnable	Site
Blank	FALSE	US_Site
CB_1	TRUE	US_Site
CB_2	TRUE	US_Site

Note:
Based on the requirement, the IP address entry can be split to similar individual entry.

Table 77: IP Phone Address Map

Parameter	Description
Site	If you are setting the IP address range for a site other than the one shown in the Site drop-down list, select it from the list.
Low IP address	This is the lowest IP address in the range of addresses.
High IP address	This is the highest IP address in the range of addresses.

Parameter	Description
Caller's emergency service identification (CESID)	Enter the Caller's Emergency Service ID to be used for IP phones in this IP address range. For example, enter **+14085555555**. For US sites, this feature is also applicable to SIP trunks if you select the **Enable RAY BAUM** option in the **Administration** > **Sites** > **General** tab page. For non-US sites, this feature is applicable only to ISDN PRI trunks. **Note**: • Whenever you enter the CESID, it will be saved in the database as entered and will not be formatted as per the Country-specific numbering plan. • (For US customers) If the third-party vendor trunks are not used for RAY BAUM conformance, then the CESID will be the telephone number that will identify the location and the callback number.
Use remote IP phone codec list	When this option is enabled, the receiving site adjusts the bandwidth of teleworkers' calls at the receiving end.
Teleworker User	Select this option for teleworker users. If this option is enabled, the **Caller's emergency service identification (CESID)**, **MAC Address** and **Call-Back Number** fields are mandatory.
MAC Address	Enter the MAC address of the endpoint.
Callback Number	Enter the callback number for IP-address-based or MAC-address-based mapping.

Parameter	Description
Ignore CID/DID for Callback	Select this option to use the callback number entered in the **Callback Number** field. If this option is selected, the CID/DID will not be used as a callback number. **Note**: If you select this field, then it is mandatory that you enter the callback number in the **Callback Number** field.

12.2.2 Exporting the IP Phone Address Map

To export IP phone address map information, follow these steps:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page opens.
3. Click **Export**. The information for the IP address map is downloaded as a Microsoft Excel file to your local machine.

Note:
You can use this Microsoft Excel file to import the IP address map data.

12.2.3 Importing the IP Phone Address Map

To import IP phone address map information, follow these steps:

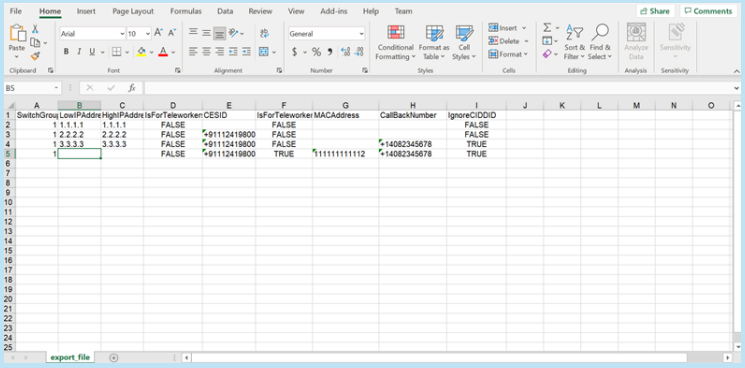
1. Launch Connect Director.
2. Export the Microsoft Excel file using the steps in Exporting the IP Phone Address Map on page 289.
3. Open the Microsoft Excel file that is saved on your local machine and edit the file.

Note:

- The IP Phone Import table only uses the numeric **SwitchGroupID** to identify the site location, also known as the **SwitchGroupName**. To assist the administrator in identifying the SwitchGroupIDs, a cross-reference list is provided at the top of the exported spreadsheet. These rows are for reference only, and must be deleted before re-importing the file.
- Ensure that the header row (first row) of the Microsoft Excel file is **SwitchGroupID** and columns across the row are in the following order:
  - **SwitchGroupID**
  - **LowIPAddress**
  - **HighIPAddress**
  - **IsForTeleworkers**
  - **CESID**
  - **IsForTeleworkersSupport**
  - **MACAddress**
  - **CallBackNumber**
  - **IgnoreCIDDID**

  Example:

Figure 8: Microsoft Excel file example



- While adding new entries in the **CESID** and **CallBackNumber** columns, ensure that the format of the entries is the same across the **CESID** and **CallBackNumber** columns. The entries must be in text format only. If not, the import of the *.xls* file will fail.

4. Launch Connect Director.
5. In the navigation pane, click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page opens.

6. Click **Import** and upload the Microsoft Excel file from your local machine.
7. In the dialog box that opens, click **Import**.

Note:

- After you click **Import**, all existing IP address entries will be deleted automatically and after that the new Microsoft Excel file will be imported.
- You can import the Microsoft Excel file only in *.xls* format.

12.2.4 Setting IP Phone Options

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Options**. The **Telephone Options** page is displayed.
3. Enter values or accept the defaults for the parameters, which are described in Parameters on the Telephone Options Page.
4. Click **Save**.

Note:

The **Server to Manage Switch** option is disabled for IP Phone Configuration Switches.

Table 78: Parameters on the Telephone Options Page

Parameter	Description
IP phone configuration switch 1	The switch designated to handle initial service requests from IP phones in the MiVoice Connect system. The switch communicates with the Mitel server to determine which switch manages calls for a particular IP phone. The IP addresses of these switches are downloaded to the IP phones whenever the IP phones are booted. If you do not assign a switch, the MiVoice Connect system automatically assigns the first two voice switches added to the system that are managed by the Headquarters server. This setting does not apply to IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones because these phones automatically receive the IP addresses of all switches in the system that support IP phones.The phones use any one of the switches in this list for initial contact before they are assigned to a particular switch.
IP phone configuration switch 2	An optional second configuration switch designated to handle initial service requests from IP phones in case the first configuration switch fails. This setting does not apply to IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones because these phones automatically receive the IP addresses of all switches in the system that support IP phones.
User group for unassigned IP phones	Unassigned IP phones are available for users configured for Any IP Phone. From the drop-down list, select the user group that has the call permissions you want unassigned IP phones to have.

Parameter	Description
IP phone announcement	A message that appears on all supported IP phones in the system. The text can be up to 19 characters long. For IP200-, IP500-, and IP600-Series phones, the message appears left-justified on the phone. To center the message, insert leading spaces in the text. For IP480, IP480g, and IP485g phones, the message is centered. The message does not appear on the IP420 or IP420g and 6900-Series (6910, 6920, 6930, and 6940) IP phones.
IP phone password	This field sets the administrative password for IP phones in the MiVoice Connect system. It is used only with IP phones that require a password. The default is **1234**. It can be 1–8 digits long.
Enable IP phone failover	For all IP100-, IP200-, IP500-, and IP600-Series phones, when this check box is selected the phones receive a keep-alive message from their call manager voice switch every four minutes. If a message is not received, the IP phone attempts to contact an alternate switch. Changing the state of this field requires these phones to be rebooted, which can take several minutes. Phones could drop calls because of the reboot process. For IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones, when this check box is selected, the phones failover to a new voice switch if their current switch fails. These phones do not require a reboot when you change the state of this field. For more information about failover behavior of IP phones, see Call Continuation During Failover on page 294.

Parameter	Description
Delay after collecting digits	The timeout period, in milliseconds, for operations that involve transferring calls. This setting applies to all users and can be set only once for the entire system. You cannot configure different timeout periods for different features or for different users, and users cannot configure the timeout period through the Connect client or the IP phone interface. This delay behavior applies to the following features: blind transfer operations related to conference calls, dialing from the Directory, intercom, on-hook dialing, park, pickup, redial, transfer, and unpark. Users aren't required to press a soft key to initiate these operations. Instead, the operations occur automatically at the expiration of this timeout period. After all of the necessary digits (which could vary based on the site's dialing plan) have been entered, digit collection stops and the timeout period begins counting down. At the end of the countdown, which can be as short as one second, the call is transferred. The default is 3 seconds.
User group for anonymous phones	The user group to which all Anonymous phones are assigned. From the drop-down list, select the user group that has the call permissions you want anonymous IP phones to have.

12.2.5 Call Continuation During Failover

Mitel provides the **Enable IP Phone Failover** option to enable a phone to move from a failed switch to another switch automatically rather than waiting for the current switch to come back up or for the administrator to manually move the phone to another switch. This feature is applicable to IP phones, third-party SIP extensions, and service appliances. SoftPhone does not support continuation of calls through failover.

The **Enable IP phone failover** option is enabled on the Telephone Options page, as described in Configuring System Settings for IP Phones on page 286.

When the **Enable IP phone failover** option is enabled and the voice switch handling a call becomes unavailable during a call, the phone goes through two failover stages:

- **Pending Failover** is the period between when the phone does not receive the expected acknowledgement signal from its voice switch until the time that an alternate

switch is assigned to perform call management tasks for the phone. This period typically lasts 2 to 4 minutes after the switch becomes unavailable.

- **Failover** is the period after the alternate switch is assigned to perform call management tasks for the phone.

12.2.5.1 Behavior of IP400-Series and 6900-Series Phones During Failover

For 400-Series IP phones and 6900-Series (6910, 6920, 6930, and 6940) phones, when the **Enable IP phone failover** option is selected, switch failover is relatively transparent to phone users. If a switch fails, active calls remain active, and the phone automatically hunts for a new switch to bind to. If the user tries to make a call during Pending Failover stage, the phone hunts for a new switch to use for the outbound call. A “No Service” message is displayed on the phone only if the phone is unable to bind successfully with a different voice switch.

The amount of time it takes for failover to occur depends on whether the phone is idle when the switch failure occurs:

- If the phone is idle, the failover happens approximately 4 minutes after the switch failure is detected.
- If the user tries to make a call during the switch failure, the failover is initiated 5 seconds from the time the call is dialed so that the call can be completed.

Regardless of the setting for the **Enable IP phone failover** option, the phones detect the switch failure and try to hunt for a new switch. The Headquarters server dynamically manages phone failover, redirecting the phones to an available voice switch, but an actual failover to the new switch occurs only if the **Enable IP phone failover** option is enabled.

12.2.5.2 Behavior of IP100-, IP200-, IP500-, and IP600-Series Phones During Failover

When a phone enters the Pending Failover stage, calls in progress remain active. Call control options, including soft key operation, are unavailable during this time. Users cannot initiate new calls, and the phone display remains frozen during pending failover.

When **Enable IP phone failover** is not enabled, all active calls remain active when the phone enters the Failover stage, but the phone does not move to another voice switch. When a phone is in this state, the user cannot make new outgoing calls or receive new incoming calls until the voice switch is again operational or the administrator moves the phone to another voice switch.

When **Enable IP phone failover** is enabled, active calls are maintained through the beginning of the failover stage until the normal completion of the call. All pending

failover restrictions remain in place after the phone enters the Failover stage until calls maintained through Failover initiation are completed.

12.2.5.2.1 IP Phones – Local Endpoint

A local endpoint is the source (calling) IP phone that is controlled by the failed switch during a failover. During the Pending Failover stage, the telephone user interface displays a “No Service” message until the phone is assigned to a new switch. Call control operations are not available on surviving calls. All inbound calls to the local endpoint are routed to the destination specified by the current availability state.

During the Failover stage, the telephone user interface displays “Failover Mode” while surviving calls remain active. Pressing phone keys generates a “No Service” message on the phone interface. Call control operations on surviving calls remain unavailable. All inbound calls to the local endpoint are routed to the destination specified by the current availability state. After the surviving call is concluded, the IP phone returns to normal operation.

12.2.5.2.2 IP Phone – Remote Endpoint

A remote endpoint is the target (called) endpoint that the functioning switch controls during failover. During failover, remote endpoint IP phones can hang up the call, place the call on hold, or retrieve the call from hold. All other soft key operations are unavailable for the duration of the call. The IP phone continues displaying call information until the end of the call. Call control operations on other calls remain available.

12.2.5.3 Behavior of Third-party SIP Phones During Failover

This feature causes no changes to messages displayed by SIP devices. Failover procedures and restrictions are applicable to third-party SIP phones. Call control operations initiated from third-party SIP phones on failover calls are not available.

12.2.5.4 Behavior of Trunks During Failover

Mitel releases the trunk only after the remote side goes on hook. System cleanup procedures, executed every two hours, release trunks that were left hanging.

12.2.6 Moving an IP Phone to a Different System

If you plan to move 400-Series IP phones from one MiVoice Connect system to another, you must clear each phone’s configuration by using MUTE 25327# (CLEAR).

12.3 Adding IP Phones to the System

After you add IP phones to your MiVoice Connect system they are in the **Available** state. You can then configure them for specific users or as anonymous phones.

12.3.1 Adding IP Phone Users

You can add IP phone users to the system using one or both of the following methods:

- Use the Any IP Phone method to add users by allowing users to assign their own phone from their desktop and voice mail. This method simplifies the setup of multiple new users.
- Assign a specific IP phone to a user.

Note:
When a user (mailbox) is moved from one server to another server, the softphone will de-register.

12.3.1.1 Using the Any IP Phone Method to Add Phones for Multiple Users

This procedure describes how to configure a user to use any IP phone. For information about creating users, see Configuring User Groups on page 481.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page appears.
3. Add a new user or select an existing user as follows:
   - To add a new user, click **New**.
   - To select an existing user, click the user's name.

Note:

The **Extension** pane for the new or existing user is displayed on the bottom of the page.

4. On the **General** tab, in the **User Group** field select a user group from the drop-down list.

> **Note**:
> Select a user group with a Class of Service telephony profile that allows extension reassignment. For more information about extension reassignment, see Configuring a COS for Telephony Features Permissions on page 461.

5. Scroll to the **Primary phone port** field, and do the following:
   - Click the **IP Phone** radio button.
   - In the drop-down list, select **Any IP Phone**.
6. Click **Save**.
7. To use this profile to create another user, click **Copy** and repeat steps 4 and through 5.
8. Instruct users to assign their extension to their phone by logging in to the voice mail system or using the phone interface.

12.3.1.2 Assigning an IP Phone to a Specific User

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Add a new user or select an existing user as follows:
   - To add a new user, click **New**.
   - To select an existing user, click the user's name.

> **Note**:
> The **Extension** pane for the new or existing user is displayed on the bottom of the page.

4. Scroll to the **Primary phone port** field, select **IP phone**, and select the specific IP phone's MAC address from the drop-down list.
5. Complete the user profile. (For information about user settings, see Configuring User Groups on page 481.)
6. Click **Save**.

12.3.2 Adding or Deleting Anonymous Phones

Anonymous phones provide flexibility within the MiVoice Connect system by making additional ports or IP phones available without assigning them to any particular user extension. When configured as anonymous telephones, these ports and IP phones cannot receive calls but do have access to dial tone. If users have the proper Class of Service (COS) permissions, they can assign their extensions to these phones through the voice mail system or the telephone user interface. When a user assigns a port or IP phone to an extension, it receives calls until the user unassigns it. For more information on how to use the Extension Assignment feature, see Configuring Extension Assignment on page 549.

To configure anonymous telephone ports and IP phones:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Anonymous Phones**. The **Anonymous Phones** page opens.
3. Do one of the following:
   - To add a new anonymous phone, click **New** and fill in the fields on the **General** tab on the bottom pane of the page. See Anonymous Phones Page: General Tab for details.
   - To delete an anonymous phone from the MiVoice Connect system, select the phone, click **Delete**, and then click **OK** in the confirmation dialog. (Deleting an anonymous phone disconnects any calls that are in progress on the port.)
4. Click **Save**.

Table 79: Anonymous Phones Page: List Pane

Field Name	Description
Jack #	The name of the telephone jack associated with the anonymous phone. This is typically the physical telephone jack that the telephone plugs into.
Name	The name of the phone. By default, this is the phone's MAC address.
Switch	The switch that the vacated telephone port is associated with.
Current User	The name of the user who is currently using the anonymous telephone port or IP phone.
Current Extension	The extension of the user who is currently using the anonymous telephone port or IP phone.

Table 80: Anonymous Phones Page: General Tab

Field Name	Description
Jack #	The name of the telephone jack associated with the anonymous phone. This is typically the physical telephone jack that the telephone plugs into.

Field Name	Description
Automatic message forwarding	The forwarding destination for any messages received by an anonymous phone. You can select a particular IP phone or a particular port on a switch by selecting the appropriate radio button and selecting the specific phone or port in the drop-down list.

12.3.3 Viewing Vacated Phones

A vacated telephone is a telephone that is configured as the home port or IP phone of a user on the system, but that user is currently assigned to another telephone and no other user is assigned to the vacated phone.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Vacated Phones**.

Note:

The **Vacated Phones** page, which displays the fields described in Vacated Phones Page, is displayed.

Table 81: Vacated Phones Page

Field Name	Description
Jack #	The name of the telephone jack associated with the vacated phone. This is typically the physical telephone jack that the telephone plugs into.
Name	The name of the phone. By default, this is the phone's MAC address.
Switch	The switch that the vacated telephone port is associated with.
Home User	The name of the user who was initially assigned to the phone before assigning his or her extension to another phone.

Field Name	Description
Home Extension	The extension of the user who was initially assigned to the IP phone.

12.4 Viewing and Editing IP Phones on the System

To allow you to manage IP phones, Connect Director includes pages for viewing and editing IP phones on the system:

- You can view and edit IP phones on the Telephones page. For more information, see Viewing IP Phones on page 301.
- You can view the status of IP phones through the Maintenance menu. For more information, see Monitoring IP Phone Status on page 801.

IP phones are assigned to the Headquarters site if they are not assigned to another site through IP address mapping, but you can move IP phones to a different site. When you assign a specific IP phone to a user, the user belongs to the site where the IP phone is located.

For details about editing user information, see Configuring User Groups on page 481.

Note:

For 6900-Series (6910, 6920, 6930, and 6940) phones, if the phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

12.4.1 Viewing IP Phones

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Telephones**. The **Telephones** page opens.

   The Telephones page, which shows all phones in the system, is displayed.

Note:
For details about the columns on the **Telephones** page, see Telephones Page: List Pane.

Note:
Mitel Technical Support does not perform troubleshooting on any model of IP phone (such as IP210) that has a designation of “Unsupported.” The designation appears in the “Phone Type” column on the **Telephones** page.

Table 82: Telephones Page: List Pane

Parameter	Description
command check box	Allows you to select one or more phones to which to apply the selected command.
Name	The configured name of the phone. By default, this is the phone’s MAC address.
Site	The name of the site where the phone resides.
Switch	The name of the switch that manages the phone.
MAC Address	The MAC address of the phone.
IP Address	The IP address of the phone.
Current User	The name of the user who is currently assigned to the phone.
Home User	The name of the user who was initially assigned to the phone before assigning his or her extension to another phone.

Parameter	Description
Phone Type	The model number of the phone or button box. **Note**: In this parameter, when the phone type is changed from Soft Phone to Desk phone (for example, IP485g), the client will send a clean up request to the Client Application Server (CAS). CAS will mark this request as **IPPHONES_UNOCCUPIED**. The clean up request will be initiated every night by the DB update service.
Assign To	For a BB24 button box, the name of the telephone that the button box is connected to.
Button Box Count	The number of BB424 button boxes connected to the phone.
Expiration	For IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones, this value shows when a phone will refresh its certificate. Certificate refresh happens once every hour. Phones also refresh their certificate when they are rebooted or powered on after being powered off.

Table 83: Telephones Parameters: General Tab

Parameter	Description
Name	Specifies the name of the telephone.
Switch	The name of the switch that manages the phone
Site	The name of the site where the phone resides
MAC Address	The MAC address of the phone

Parameter	Description
IP Address	The IP address of the phone
Current User	The name of the user who is currently assigned to the phone
Home User	The name of the user who was initially assigned to the phone before assigning his or her extension to another phone
Phone Type	The model number of the phone or button box
Assign To	For a BB24 Button Box, specify the name of the telephone the BB24 is assigned to.
Button box order	For a BB24 Button Box, specify where in the sequence of four possible button boxes this BB24 Button Box should reside.

12.4.2 Renaming an IP Phone

You can change the name of an IP phone from the **Telephones** page in Connect Director. By default, IP phones are listed by MAC address in the **Name** column of the **List** pane on the **Telephones** page.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Telephones**.

Note:

The **Telephones** page is displayed.

3. In the **List** pane at the top of the page, click the name of the phone you want to rename.

Note:
The **General** tab in the **Details** pane at the bottom of the page displays the details for that phone.

4. In the **Name** field, enter a new name for the phone.
5. Click **Save**.

12.4.3 Deleting an IP Phone from Connect Director

Note:

- If you use MUTE 25327# (CLEAR) to clear a phone's configuration, the phone is automatically deleted from Connect Director.
- For 6900-Series (6910, 6920, 6930, 6940, and 6970) phones, if you use the **Reset** (factory-default) option in the **Advanced** menu, the phone is automatically deleted from Connect Director.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Telephones**. The **Telephones** page opens.
3. If you want to filter the list of phones, click and enter text in one or more filter boxes.

Note:
The filtered list of IP phones is displayed.

4. Select the check box for the IP phone that you want to delete.

Note:
Ensure that you have the selected the correct phone and that no other phones are selected.

5. Click **Delete**.

A dialog box requests confirmation.

6. Click **Yes** to delete the phone.

Note:

- If you want to add the IP phone back into the system, you must reboot the IP phone. The phone is reconfigured during the boot process and becomes available again.
- 400-Series IP phones and 6900-Series (6910, 6920, 6930, 6940, and 6970) phones automatically re-register with the system and display the Available state and a user must be assigned, without rebooting.

Note:

Available state is not displayed for 6970 IP phone.

12.4.4 Moving an IP Phone to a Different Voice Switch

To move an IP phone to a destination switch at a remote site, the remote site must have an IP address range defined. You may not move an IP phone to a switch on a remote site if the IP address of the phone is not within the IP address range defined for the destination site.

The IP address range restrictions apply only to switches at remote sites. You can move an IP phone across switches at the Headquarters site without entering an IP address range for the Headquarters site. However, if the phone's IP address is within a range mapped to a remote site, you cannot move that phone to a switch at the Headquarters site.

Clearing a phone's configuration while the phone is connected to the MiVoice Connect system automatically removes the phone from Connect Director. If you clear a phone's configuration while the phone is not connected to the system, you must manually remove the phone from Connect Director.

To move one or more IP phones:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Telephones**. The **Telephones** page opens.

3. If you want to filter the list of phones, click and enter text in one or more filter boxes.

Note:

The filtered list of IP phones is displayed.

4. Select the check boxes for the IP phones you want to move.
5. In the drop-down list at the top of the page, do the following:
   - If you want to move the phone to a different site, select the new site in the **Move to site** drop-down list.
   - Select the switch you want to move the phone to in the **and switch** drop-down list.
6. Click **Move**.

Note:
A dialog box requests confirmation.

7. Click **OK** to move the phone.

12.4.5 Overriding DHCP 156

For 400-Series IP phones, follow these steps to override DHCP Option 156:

- If your installation uses DHCP Option 156, follow these steps:

1. Go to **Settings** .
2. Do either of the following:
   - Select **Advanced** > **Reset**.
   - Press the **MUTE** option followed by **25327#** on the phone's keypad.

   The phone will clear the factory settings and reboot.
3. During reboot, the **Press Skip to Bypass Provisioning** option might appear. Selecting this option will skip DHCP option. Therefore, do not select this option so that the phone can clear and reboot the factory settings with the Configuration server set by DHCP Option 156.

- If your installation does not use DHCP Option 156, follow these steps:

  1. Go to **Settings**  .
  2. Do either of the following:

     - Select **Advanced** > **Reset**.
     - Press the **MUTE** option followed by **25327#** on the phone's keypad

     The phone will clear the factory settings and reboot.
  3. During reboot, the **Press Skip to Bypass Provisioning** option might appear. If this option appears, select this option. The Home page opens.
  4. Go to **Settings** > **Voice Services** > **MiVoice Connect** and enter the fully qualified domain name (FQDN) of the Configuration server or the IP address of your Headquarters server. The phone will reboot and apply the manually entered server address instead of the one received from the DHCP option.

Before you move 6900-Series (6910, 6920, 6930, and 6940) phones from one MiVoice Connect system to another, you must perform either of the following:

- If your installation uses DHCP Option 156, perform these steps:

  1. Go to **Settings**  .
  2. Select **Advanced** > **Reset**. The phone will clear the factory settings and reboot.

Note:

- During reboot, the **Press Skip to Bypass Provisioning** option might appear. Selecting this option will skip the DHCP option and take you to the**Voice Services** page. In the **Voice Services** page, select **MiVoice Connect** and enter the **Configuration Server** (fully qualified domain name (FQDN) or IP address of your Headquarters server). The phone will reboot and apply the manually entered server address and not the one received from DHCP option.
- You can register a 6900-Series phone with out-of-the box MiNet firmware only with a MiVoice Connect system that uses a certificate signed by a well-known Certificate Authority (for example, VeriSign, GoDaddy, and GeoTrust) or a UC certificate Authority (ShoreTel UC CA). This is because 6900-Series phones cannot authenticate a certificate signed by a third-party Certificate Authority as the root certificate of third-party CA is not available in the trusted store on 6900-Series phones. If the root certificate of third-party CA were available in the trusted store on 6900 series phones, the phones would have authenticated the certificates as expected. This feature will be supported in a future release.

- If your installation does not use DHCP Option 156, perform these steps:

1. Go to **Settings**  .
2. Select **Advanced** > **Reset**. The phone will clear the factory settings and reboot.

12.4.6 IP Phone State Display

IP phones display the following states:

- **Available:** The phone has no user assigned to it. Calls can be placed from the phone, but it does not receive calls. The Caller ID is “Unknown”.
- **<User Name> <User Ext>:** The phone is assigned to <User Name>.
- **Anonymous:** The user can make a call but cannot receive calls. The Caller ID is “Caller ID Unknown.” The phone can be in this state for either of the following reasons:
  - The assigned user has activated the Extension Assignment feature on another phone.
  - The Mitel administrator has explicitly configured anonymous phones that do not have assigned users.
- **Unavailable:** The phone was once in the MiVoice Connect system but has been removed through Connect Director. The phone has no dial tone and is not functional.

Note:

This state does not apply to 400-Series and 6900-Series (6910, 6920, 6930, 6940, and 6970) phones.

12.4.7 Displaying IP Phone Settings

You can display a phone's current IP parameter settings by entering a key sequence from the phone's keypad.

12.4.7.1 On IP100-, IP200-, IP500-, and IP600-Series Phones

1. With the phone on hook, press the MUTE key followed by **4636#** (INFO#).

Note:

The phone displays a parameter or group of parameters.

2. Press **#** to advance the display or * to exit.

Note:

The phone resumes normal operation after the last parameter or group of parameters has been displayed.

12.4.7.2 On 400-Series and 6900-Series Phones

Follow these steps to display the IP phone settings for 400-Series phones:

1. With the phone on hook, press the **MUTE** key followed by **4636#** (INFO#).

Note:

The **Admin Options** menu opens.

2. Use the navigation keypad and the selector button to scroll through and open the submenus as necessary to view the phone's settings.

Note:

For descriptions of the parameters, see the *MiVoice Connect Maintenance Guide*.

3. To close the **Admin Options** menu, do one of the following:

   - On IP480, IP480g, and IP485g phones, press the **Exit** soft key.
   - On IP420 and IP420g phones, with **Exit** selected press the selector button on the navigation keypad.

Follow these steps to display the IP phone settings for 6900-Series (6910, 6920, 6930, 6940, and 6970) phones:

1. Go to **Settings**  .
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**. The settings for the phone are displayed

12.4.8 Resetting an IP Phone

You can reset a phone by entering a key sequence from the phone's keypad.

12.4.8.1 On IP100-, IP200-, IP500-, and IP600-Series Phones

1. With the phone on hook, press the MUTE key followed by **73738#** (RESET#).

Note:

The phone displays the **Reset Phone?** prompt.

2. Press **#** to reboot.

Note:

The phone reboots and applies settings.

12.4.8.2 On 400-Series and 6900-Series IP Phones

Follow these steps to reset the 400-Series IP phones:

1. With the phone on hook, press the **MUTE** key followed by **73738#** (RESET#).

Note:

The phone displays the **Reset phone** screen.

2. Do one of the following:

- On IP480, IP480g, and IP485g phones, press the **Reset** soft key.
- On IP420 and IP420g phones, with **Reset** selected, press the selector button on the navigation keypad.

Note:

The phone reboots and applies settings.

Follow these steps to reset the 6900-Series (6910, 6920, 6930, 6940, and 6970) phones:

1. Go to **Settings**  .
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Restart** to reset the phone.

Note:

For 6970 IP phone, select **Reset** to reset the phone.

12.5 Customizing Ringtones

IP phones offer multiple sets of different ringtones that users can select on their phones. Each set has one tone for internal calls and one tone for external calls. IP phones also support the ability to load custom ringtones on an IP phone so that users can distinguish the sound of their phone's ringtone from their neighbors' ringtones.

To use custom ringtones, you must save them to the proper location on the server. The default directory for ringtones is `<drive>:\inetpub\ftproot\wav\ringtone`. In addition, for 400-Series IP phones, WAV files must be converted to PCM files, as described below.

After the custom ringtones are saved on the server, the way that you specify the ringtone file names depends on the phone model:

- For the IP655 and the 400-Series IP phones, you specify custom ringtones for a particular user group through the User Groups page in Connect Director. When custom ringtones are assigned in this manner, the existing sets of Mitel ringtones are preserved.
- For IP100-, IP200-, and IP500-Series phones, you specify custom ringtones through a configuration file. When ringtones are customized through configuration files, the custom ringtone set displaces one of the existing sets of Mitel ringtones.

Note:

The 6900-Series (6910, 6920, 6930, 6940, and 6970) phones does not support the download of custom ringtones. It supports only the built-in ringtones provided in the phone firmware.

The ringtones are downloaded to the IP phone through FTP, HTTP, or HTTPS.

Custom ringtones have the following requirements or restrictions:

- Custom ringtones must be in Waveform audio file format (.wav). Mitel does not offer custom ringtones, nor does it provide tools for creating or managing the custom WAV files, but numerous web sites offer free WAV downloads.
- Phones support the following formats:
  - µ-law: 8-bit, 8 kHz, 16 kHz, monaural
  - a-law: 8-bit, 8 kHz, 16 kHz, monaural
  - 16-bit, 8 kHz, monaural -or- 16-bit, 16 kHz, monaural
- Most Mitel phone models can have up to two custom tones. Their combined size must be less than 750 KB. IP400-series phones can have up to 10 pairs of custom ringtones, without this size restriction.
- Connect Director imposes ringtone size restrictions for IP655 and IP400-Series models. Custom ringtones for ring pairs 5-8 can be up to 100 KB each. Custom ringtones for ring pairs 9-14 (available only for the 400-Series phones) can be up to 300 KB each.
- WAV files can be any time length within the size restrictions. If a WAV file is less than six seconds, the phone pads the ring out to a six-second length before it repeats the WAV file. WAV files longer than six seconds are repeated.

Custom ringtones for IP400-Series phones use PCM audio format (.pcm) rather than WAV format (.wav). Custom ringtone WAV files are converted to PCM format automatically or by running a batch file, as follows:

- During the Mitel installation or upgrade process, any existing custom ringtone WAV files in the `\wav\ringtone` subdirectory are automatically converted to PCM, and they are available for use by the 400-Series phones.
- If you add WAV files for custom ringtones after the Mitel installation or upgrade process, WAV files must be converted to PCM audio format before you can download them to the 400-Series phones. To convert WAV files to PCM format, run `wav2pcm.bat`, which resides in `<drive>:\inetpub\ftproot\wav\ringtone`. Running wav2pcm.bat converts all WAV files in the `\wav\ringtone` subdirectory to PCM format and stores the new ringtone files in `<drive>:\inetpub\ftproot\pcm\ringtone`.

When you select custom ringtones for 400-Series phones on the Edit User Groups page in Connect Director, the system automatically uses the corresponding .pcm file for the .wav file you select.

12.5.1 Loading Custom Ringtones through Connect Director

For the IP655 and IP400-Series phones, you specify custom ringtones for a particular user group through Connect Director.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page is displayed.
3. Do one of the following:
   - To edit options for an existing user group, click the user group name.
   - To create a new user group, click **New**.
4. On the **Details** pane, click the **Profile** tab, and then click the **Ringtones** subtab.
5. For one or more ringtones, in the **Name** field specify a name and then select audio files in both the **Internal** and **External** drop-down lists.

Note:

The IP655 phone can use ringtones through Ring Pair 8. IP400-Series phones can use ringtones through Ring Pair 14.

6. Click **Save**.

12.5.2 Loading Custom Ringtones through a Custom Configuration File

For IP100-, IP200-, and IP500-series phones, you can specify custom ringtones through a configuration file. Following is a high-level description of the process:

1. Identify the WAV files you want to use as ringtones. You can either create the files yourself or obtain them from another source, such as a website. Put the files on a server that is accessible to the IP phone by anonymous FTP. (This server does not have to be the same as the host of the configuration files.) The default directory for ringtones is `<drive>:\inetpub\ftproot\wav\ringtone`.
2. Create or edit the custom configuration file for a specific phone or a phone model.

3. Reboot the phone so that it retrieves the information in the configuration file and downloads the WAV files. At boot time, the phone indicates the success or failure of phone-specific configuration download and the WAV download.

To specify that a phone use custom ringtones, you must insert two configuration parameters, WaveRinger1 and WaveRinger2, in a custom configuration file. These two parameters identify the name and location of the custom ringtones that the IP phone downloads (by FTP or HTTPS) to its RAM at boot time. The WaveRinger1 and WaveRinger2 Configuration Parameters table below provides more details.

For example, to load one of the custom ringtones, you could replace **L/r14** (Ring 4 External) and **L/r15** (Ring 4 Internal) with the name and location of the file containing the new custom ringtone, using the symbols shown in the following Ringtones and Symbols table.

Replacing internal and external ringtones in separate sets (for example, Ring 2 external and Ring 4 internal) is also possible, but only one set of ringtones can be active at a time. Activating either set of ringtones activates only one of the custom ringtones at a time.

Table 84: WaveRinger1 and WaveRinger2 Configuration Parameters

Parameter Name	Value	Notes
WaveRinger1 WaveRinger2	Up to 64 ASCII Characters	Used to assign one Wave File to any of the ringtones defined in the below table. The first value is the ringtone, and the second value is the location of the file on the FTP server. Examples: WaveRinger1 L/rg 192.168.0.20/audio/dave.wav WaveRinger2 L/r1 192.168.0.20/audio/dave.wav

Table 85: Ringtones and Symbols

Ringtone	Symbol
Standard - External ring	L/rg

Ringtone	Symbol
Standard - Internal ring	L/r1
Ring 2 - External ring	L/r10
Ring 2 - Internal ring	L/r11
Ring 3 - External ring	L/r12
Ring 3 - Internal ring	L/r13
Ring 4 - External ring	L/r14
Ring 4 - Internal ring	L/r15

You can add the parameters listed in WaveRinger1 and WaveRinger2 Configuration Parameters to the custom configuration file for a specific phone or all phones of a certain model:

- For a specific phone, create a phone-specific custom configuration text file and store it in the same directory as the standard IP phone configuration files. The name of the phone-specific file contains the MAC address of the phone that you want to receive the custom ringtone. You can find the MAC address on the sticker on the back of the phone. The name of the phone-specific configuration file is as follows:

  `shore_AABBCCDDEEFF.txt`

  where “AABBCCDDEEFF” is the MAC address and all the letters in the MAC address should be in upper case.
- To load the same custom ringtone onto several IP phones at the same time, edit the custom configuration file for a particular phone model. (For example, the custom configuration file name for the IP560 is S6custom.txt.) Be aware that loading ringtones on all phones of a certain model could cause ringtone confusion if the phones are concentrated in one area of a building.

The default location for custom configuration files is `<drive>:\inetpub\ftproot\phoneconfig`. For more details about using custom configuration files, see the *MiVoice Connect Maintenance Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

12.6 Customizing Wallpaper on Color Phone Displays

The IP265, IP485g, IP565g, and IP655 phone models offer color displays. These phones include default images that you can specify for the wallpaper on the phone display, but you can also configure these phones to display custom wallpaper images that you download from a server.

Note:

The 6900-Series (6910, 6920, 6930, 6940, and 6970) phones does not support customization or download of the wallpaper image.

The process and graphics specifications for using custom wallpaper images vary based on the IP phone model.

12.6.1 For IP485g and IP655 Phones

To use a custom wallpaper image on a IP485g or IP655 phone, you create the image, add the image file to the server, and use the User Groups page in Connect Director to assign the image to a particular user group. The particular wallpaper image that is displayed can be set in the user's personal options in Connect Director or through the phone's **Options** menu. This section describes how to create and assign custom wallpaper images.

In addition, this section explains how to modify the "Standard" wallpaper image that IP485g phones include. To change the default wallpaper image for this "Standard" file, you specify the new image in a custom configuration file for the phone.

12.6.1.1 Creating Custom Wallpaper Images

Wallpaper images need to be in the Portable Network Graphics (.png) file format in the following dimensions:

- For the IP485g, wallpaper images are 480x272 pixels.
- For the IP655, wallpaper images are 640x480 pixels.

You can create .png files using Microsoft Paint or any other graphics editing program. A simple approach for creating a custom image that is the correct size is to use one of the wallpaper images provided by Mitel as a template.

Note:

Because wallpaper images for the IP485g and IP655 are different sizes, it is recommended that you save images in both sizes with the same name in the appropriate directories. With images available in both sizes, after you specify the image in Connect Director, the phone can access the image in the correct size.

If an image of the proper size for the phone model is not available, the following happens:

- If you select an image that was created for the IP485g to use on the IP655, the image does not display.
- If you select an image that was created for the IP655 to use on the IP485g, a cropped and resized version of the image is displayed. Therefore, it might not look the way you expect it to look.

To create a graphic file that can be used as a wallpaper image:

1. Locate the wallpaper images that were loaded on your system when you installed the MiVoice Connect server by looking in one of the following default directories:

   `<drive>:\inetpub\ftproot\Wallpaper\480x272c\`

   `<drive>:\inetpub\ftproot\Wallpaper\640x480c\`

   Note:

   Depending on how your system was installed, the root path for these directories might be different.

2. Open one of the .png files in this directory by using MS Paint or another graphics editing program.
3. Verify that the image has the following attributes:

   - For IP485g
   - Width – 480 pixels
   - Height – 272 pixels
   - For IP655
   - Width – 640 pixels
   - Height – 480 pixels

4. Save a copy of the image, or use Save As to save a new file.
5. Verify that the old file and the new file exist in one of the following locations, as appropriate:
   - `<drive>:\inetpub\ftproot\Wallpaper\480x272c\`
   - `<drive>:\inetpub\ftproot\Wallpaper\640x480c\`
   - wherever your custom wallpaper images are stored
6. Change the image to create your custom image, while retaining the size of the original image.
7. Click **Save**.

12.6.1.2 Assigning Custom Wallpaper Images to a User Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page opens.
3. Do one of the following:
   - To edit options for an existing user group, click the user group name.
   - To create a new user group, click **New**.
4. On the **Details** pane, click the **Profile** tab, and then click the **Wallpapers** subtab.
5. For one or more wallpaper images, specify a name and select an image from the drop-down list.
6. Click **Save**.

12.6.1.3 Specifying a Custom Wallpaper Image for a User

After wallpaper images are assigned to a particular user group, they can be assigned to any user in that user group.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Do one of the following:
   - To edit options for an existing user, click the user's name.
   - To create a new user, click **New**.

     The **Details** pane is populated with the existing user's parameters or shows default parameters for a new user.

4. On the **Details** pane, click the **Telephony** tab.
5. In the **Wallpaper** field, select a wallpaper image from the drop-down list.
6. Click **Save**.

12.6.1.4 Specifying a Wallpaper Image from the Phone Interface

Users can select from the provided wallpaper images by using the Options menu on the IP485g or the User Options menu on the IP655. Details are provided in the phone user guides.

12.6.1.5 Specifying a Custom Image for the Standard Wallpaper Image

In general, you configure the custom wallpaper images through Connect Director. However, if you want to specify a custom image for the Standard image, you do that by adding text to the configuration file in the phone configuration directory on the Headquarters server.

The following procedure uses the default directories. Depending on how your system was installed, your root path might be different.

1. Save the custom wallpaper image file on the Headquarters server in the following directory, as appropriate for the phone model:

   `<drive>:\inetpub\ftproot\Wallpaper\480x272c`

   `<drive>:\inetpub\ftproot\Wallpaper\640x480c`
2. Access the `<drive>:\inetpub\ftproot\phoneconfig` directory on the Headquarters server, and edit the configuration files as follows to specify an image to use as the Standard wallpaper image:

   - For the IP485g phone, add the following lines to custom_IP485g.txt:

     ```
     [user]

     wallpaperStandardFilename= <image file name>.png
     ```
   - For the IP655 phone, add the following line to swecustom.txt:

     `wallpaper1Phone` *“<image file name>.png”*

     When you use this method, the image’s label on the phone is Standard. You cannot modify the label.

Note:

For example, if you want to replace the Standard wallpaper image (standard.png) on the IP485g with your company logo (logo.png), add the following lines to the custom configuration file:

```
[user]

wallpaperStandardFilename=logo.png
```

This file name will not be overridden by other configuration settings.

3. Reboot the phones so that they apply the new setting.
4. Verify that the phones display the new wallpaper file for the Standard wallpaper setting.

12.6.2 For IP265 and IP565g Phones

To use a custom wallpaper image, you must first create the image and then specify it in a custom configuration file.

12.6.2.1 Creating Custom Wallpaper Images

For IP265 and IP565g phones, the wallpaper is 320x240 pixels and uses an uncompressed 256-color.bmp file format. Each of the 256 colors is defined by a 24-bit RGB value. Bitmap files can be composed using MS Paint or any other editor that can create Paint-compatible files.

To create a graphic file that can be used as a wallpaper image:

1. Open the image in Microsoft Paint.
2. Verify that the image has the following attributes:
   - Width – 320 pixels
   - Height – 240 pixels
   - Colors – Colors
3. Click **OK** to close the dialog box.
4. Click **File** > **Save As**.

   The Save As dialog box appears.
5. In the **Save as type** field, select **24-bit Bitmap (*.bmp;*.dib)**.

6. In the **File Name** field, enter the name to use for the file.
7. Click **Save**.

12.6.2.2 Downloading the File to Several Color-Screen IP Phones

The wallpaper file that each IP phone displays is specified in configuration files located in the phone configuration directory on the Headquarters server. In standard Mitel installations, the phone configuration directory is `<drive>:\Inetpub\ftproot`.

Mitel specifies one text file for each phone model that defines default characteristics for all phones of that model type on the system. You specify the default wallpaper for phones of a specific model by adding a line to its corresponding configuration file.

To load a custom wallpaper image on all phones of a specific model type:

1. Save the wallpaper file on the Headquarters server in the following directory:

   `<drive>:\Inetpub\ftproot`
2. Access the `<drive>:\Inetpub\ftproot` directory on the Headquarters server.
3. Open the custom configuration file for the phone model:
   - For IP265, open `s36custom.txt`
   - For IP565g, open `s6ccustom.txt`
4. Add the following line to the open file: `Wallpaper2pixmap abc.bmp`, entering the name of the wallpaper file in place of abc.bmp, and then save and close the file.

Note:

For example, if the wallpaper file is name `logo.bmp`, enter **Wallpaper2pixmap logo.bmp** in the configuration file.

5. Open the configuration file for the phone model:
   - IP265: open `shore_s36.txt.`
   - IP565g: open `shore_s6c.txt.`
6. Verify that the file contains the one of the following lines, or add the line if it is not present:
   - IP265: Include `s36custom.txt`.
   - IP565g: Include `s6ccustom.txt`.

7. Reset the phones.
8. Verify that each phone displays the new wallpaper file.

12.6.2.3 Downloading a Custom Wallpaper Image to a Single Phone

The individual configuration files for a phone override the default settings for individual IP phone models. You can assign custom wallpaper files to individual IP phones by modifying the corresponding phone configuration file.

1. Save the wallpaper file on the Headquarters server in the following directory:

   `<drive>:/Inetpub/ftproot`
2. Access the `<drive>:/Inetpub/ftproot` directory on the Headquarters server.
3. Create a text file named shore_xxxxxx.txt, where xxxxxx is the MAC address of the phone. Use lower case text when naming the file.

   The MAC address is a 12-digit number that uniquely identifies each device. This address is printed on the white bar code located on the bottom of the phone.

> **Note**:
>
> For example, if the MAC address of an IP565g is 00104907020C, then create a file named `shore_00104907020c.txt`.

4. Add a line in the open file with the following format: `Wallpaper2pixmap abc.bmp`, where **abc.bmp** is the name of the wallpaper file, then save and close the file. For example, if the wallpaper filename is `logo.bmp`, enter **Wallpaper2pixmap logo.bmp**.
5. Reboot the phone.
6. Verify that the phone displays the wallpaper file.

12.7 Specifying Custom Applications for User Groups

For certain phone models, such as the IP655, in addition to specifying ringtones and wallpaper, you can specify configuration options for applications through the **User Group** page in Connect Director.

1. Launch Connect Director.
2. Click **Administration** > **Users** > **User Groups**. The **User Groups** page opens.

3. Do one of the following:
   - To configure applications for an existing user group, click the user group name.
   - To create a new user group, click **New**.
4. On the **Details** pane, click the **Profile** tab, and then click the **Phone Applications** subtab.
5. In the **On idle** field, select an application from the drop-down list.
6. To make other applications available to users in that user group, in the **Available applications** field, use the drop-down lists to select applications that reference URLs.
7. Click **Save**.

12.8 Automatic Off-Hook and Headset Preferences

You can set a user's automatic off-hook preference in Connect Director, and users can set this preference through the interface on some phone models. In Connect Director and the Connect client, the automatic off-hook preference is combined with the headset type, but some phone models provide the headset type as a separate option, which leads to the following differences in behavior:

- For the IP480, IP480g, and IP485g phones, the automatic off-hook preference (speaker or headset) and the headset type (wired or wireless) are separate options that a user can set in the phone interface. As a result, the headset type preference remains in effect regardless of the automatic off-hook setting. In other words, a user can select the speaker phone as the automatic off-hook setting while still specifying a preference for headset type.
- The IP420 and IP420g phone interface does not provide the capability to change the preferences for automatic off-hook or headset type. If a user's headset type is set to wireless headset and the user assigns his or her extension to a phone that does not have a wireless headset attached, the user cannot use the headset button or automatic off-hook on the phone. Alternatively, the speaker phone or handset could provide audio path. In addition, on IP420 and IP420g phones, after a user has unassigned his or her extension from a phone and the phone returns to an Available or Anonymous state, the headset type always reverts to the wired headset preference.
- For IP phone models other than the IP400-Series models, the automatic off-hook preference includes the headset type, just as in Connect Director. As a result, if you or the user change a user's automatic off-hook preference from wireless headset to speaker on these models, the phone reverts to a wired headset setting.

Note:

This setting does not apply to 6900-Series (6910, 6920, 6930, and 6940) phones. The configuration settings are managed on the phone.

12.9 Specifying Automatic Off-Hook for Wireless Headsets

Mitel has incorporated electronic automatic off-hook functionality into various IP phone models. These IP phones work with the **Plantronics CS50** wireless headset. Users who have purchased this supported headset model can answer or end calls by pressing the activation button on their headset when they hear their phone ring. If they are too far from their phone to hear it ring, the headset will generate an audible cue to announce incoming calls.

This feature is supported on the following IP phone models:

- IP565g
- IP560g
- IP560
- IP485g
- IP480g
- IP480
- IP420g
- IP420
- IP265
- IP230
- IP212k

Using this feature defeats auto on-hook and off-hook behaviors.

You can configure the automatic off-hook feature through the phone, or Connect Director. The procedure for using Connect Director is as follows:

1. Launch Connect Director.
2. Click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the user whose automatic off-hook option you want to modify.

   Information for that user appears in the **Details** pane.
4. On the **Details** pane, click the **Telephony** tab.
5. In the **Automatic off-hook preference** field, select **Wireless headset**.

6. Click **Save**.

12.10 Configuring Programmable IP Phone Buttons

An administrator or user can change the functions associated with programmable buttons on IP phones or button boxes. These programmable buttons function as shortcuts for operations that would normally require pressing two or three buttons to accomplish the same task. For example, the bottom button on an IP560 could be configured to speed dial a particular extension or external number. The button above that could be set to perform overhead paging, and so on.

Supported Programmable Button Functions lists the supported functions that can be programmed through Connect Director. Not all programmable functions apply to all phone models.

All of the custom buttons are configurable except for the top right button, which is permanently set to provide call appearance information (that is, the ringing indicator and call timer information). After a function is assigned to a button, users can enter a label that appears on the display next to the custom button. The length of the label depends on the phone model, and labels might be truncated on certain phone models.

You can configure custom buttons through Connect Director on behalf of a user, or you can enable permissions for an individual user so that the user can modify the custom buttons on the IP phone through the telephone interface. The functions that a user can assign to a programmable button using the telephone interface vary depending on the phone model. On IP230, IP480, IP480g, and IP485g models, these functions are limited to Dial Number and Call Appearance.

The programmable button feature is supported on all Mitel multiple-line models except the IP420 and IP420g.

Note:

- The 6910 IP phones does not support user modification of programmable buttons through the **Phone Settings** menu.
- For 6920, 6930, and 6940 IP phones, you can configure Dial Number, Call Appearance and Mobile Line programmable button types through the **Phone Settings** menu.

Table 86: Supported Programmable Button Functions

Function	Parameter	Comments
Agent Login	None	Log in as a workgroup agent.
Agent Logout	None	Log out as a workgroup agent.
Agent Wrap-Up	None	Enter agent wrap-up status.
Barge In	Extension or none	Join an in-progress call (“barge in”) as a conferenced participant. This feature is useful for operators, executive assistants, trainers, and workgroup supervisors. Included in this feature are some visual cues such as LED colors and a subset of simple icons that allow you to monitor the extension to a limited extent.
Bridged Call Appearance	Extension, Call stack position, and Ring delay before alert	See call activity and interact with calls for another extension. This bridged information, which provides more detailed information than the Monitor Extension functionality, offers faster call handling between users. The call appearance button assigned to the targeted extension displays various icons and LED colors and blink patterns according to the type of call.
Call Appearance	None	Represents a phone call on your extension. **Note**: Call Appearance is not supported on Button Box.

Function	Parameter	Comments
Call Move		Switch a call from one phone to another without disrupting the conversation. **Example:** If a user is participating in a conference call, the user can move the call from a desk phone to a cell phone and leave the office, without disrupting thecall. For more information, see Configuring Simultaneous Ringing and Call Move on page 346.
Centrex Flash	None	See Configuring Centrex Flash on page 253.
Change Availability	Availability state	Change the availability state on the phone. You can configure the button to change the availability state to one of the following: • Available • In a Meeting • Out of Office • Vacation • Custom • Do Not Disturb For more information about availability states, see Configuring Availability States on page 559.
Change Default Audio Path	Audio Call Path	Change the default audio path on the phone. You can configure the button to change the default audio path to one of the following: • Speaker • Headset • Wireless Headset • Bluetooth Headset

Function	Parameter	Comments
Conference Blind	Extension or external number	Join a party into a conference call without first consulting the user on the extension or external number to which you are joining the other party.
Conference Consultative	Extension or external number	Join a party into a conference call after first consulting the user on the extension or external number to which you are joining the other party.
Conference Intercom	Extension or none	Join a party into a conference call after first using intercom to consult the user on the extension to which you are joining the other party.
Dial Mailbox	Extension or none	Call another person's voice mailbox directly without ringing their phone.
Dial Number (Speed Dial)	Extension or external number	Dial an extension or an external number.
Group Pickup	Extension	Answer an incoming call to an extension in a pickup group.
Hotline	Extension	Initiate a hotline call. A hotline is a ringdown circuit between two extensions; for example, an executive and an assistant. Hotline calls can be configured as speed dial or intercom calls.
Intercom	Extension or none	Use a programmed button to connect to another user. When you intercom another user, instead of their phone ringing, the called party will hear a tone then you will be connected to their speaker phone.
Malicious Call Trace	Mailbox	Event logs are sent to the specified mailbox. For more information, see Implementing Malicious Call Trace on page 337.
Mobile Line	None	Switch the call audio from your Bluetooth-paired mobile phone to your Mitel desktop IP phone. This feature is available if your mobile phone is synchronized with your desk phone through the Mitel Mobilelink feature.
Monitor Extension	Extension or none	Monitor the extension of another user so that you can help answer calls on behalf of that extension. You can also configure the Monitor Extension button for multiple functions, depending on the status of the monitoring party's phone. For more information, see Monitoring Extensions from an IP Phone on page 571.
Page	None	Access the overhead paging system or page a group of phones.
Park	Extension or none	Park a call on another extension.
Park and Page	Extension or none	Park a call on another extension and simultaneously page a group of phones.

Function	Parameter	Comments
Phone Application	Application	This feature is not supported for button box.
Pickup	Extension or none	Pick up an incoming call for another extension.
Pickup Night Bell	None	Pick up a call from an extension that rings on an overhead s peaker. This feature can be convenient for off-hours when a caller needs to speak with anyone at a site.
Pickup/Unpark	Extension or none	Pick up an incoming call for another extension or unpark a c all that is parked on another extension. Uses internal prese nce to determine which operation to perform
Record Call	Mailbox	Record an active external call on your extension; only external calls can be recorded. Pressing the programmed button a second time stops the recording. Call recordings can be saved in the mailbox of the initiating client (by leaving the mailbox field blank) or can be routed to an alternate mailbox by typing a mailbox number in the field.
Record Extension	Extension or mailbox	Record an active external call on another person's extension; only an extension involved in an external call can be recorded. Call recordings can be saved in the mailbox of the initiating client (by leaving the mailbox field blank) or can be routed to an alternate mailbox by entering a mailbox number in the field.
Send Digits Over Call	Digits	The Mitel system allows users to send a preconfigured se t of DTMF tones out during a call. This feature is useful for quickly navigating external interactive voice response (IVR) systems as well as external systems requiring an account code.
Silent Coach	Extension	Listen to and coach someone during a call without the ou tside party hearing.

Function	Parameter	Comments
Silent Monitor	Extension or none	Silently monitor a call on another extension. You are added to the existing call without being heard or seen by any party. This feature is useful for users such as workgroup supervisors. Included in this feature are some visual cues such as LED colors and a subset of simple icons that allow you to monitor the extension to a limited extent.
Toggle Handsfree	None	Toggle between enabling and disabling handsfree mode. When handsfree mode is enabled, dial tone is disabled so t hat the user can use a headset or speakerphone to answer or make calls from the IP phone.
Toggle Lock/Unlock	None	A BCA user can override the default privacy setting using the Toggle Lock/Unlock programmable button. For example, the user can lock the call to make the call private and prevent other BCA users from joining the call. **Note**: Toggle Lock/Unlock is not supported on Button Box.
Transfer Blind	Extension or external nu mber	Transfer a call to another party without first consulting that p arty.
Transfer Consultative	Extension or external nu mber	Transfer a call to another party after first consulting that par ty.
Transfer Intercom	Extension or none	Transfer a call to another party after first using intercom to c onsult that party.
Transfer to Mailbox	Extension or none	Transfer a call directly to another user's voice mailbox.
Transfer Whisper	Extension or none	Transfer a call to another party after first using whisper p age to consult that party. Whisper page allows a user to joi n a call on another user's extension and speak to that user without the other call participant hearing. The user can spe ak back to the user that initiated the whisper page privately using the whisper page mute feature.
Unpark	Extension or none	Unpark a call that is parked or on hold on another exten sion.

Function	Parameter	Comments
Unused	None	
Whisper Page	Extension or none	With this feature, while on a call, you can make a whisper c all and speak to a person without the other call participant s hearing the conversation between you and the person on the whisper call. A whisper call to a person does not need that person's acceptance to become active.
Whisper Page Mute	None	Respond privately to the person who initiated a whisper page without the other call participant hearing.

12.10.1 Configuring Programmable Buttons through Connect Director

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page opens.
3. Click the name of the user whose phone buttons you want to program.

Note:
The **IP Phone Buttons** tab for that user is displayed in the details pane.

4. Click the subtab for the phone or button box for which you want to program buttons.
5. For each button that you want to configure, do the following:

   a. In the first **Function** field, select the category for this button from the drop-down list.
   b. In the drop-down list in the second field, select the function to associate with a particular button. (For descriptions of the functions, see Supported Programmable Button Functions.)
   c. In the **Long Label** and **Short Label** fields, enter a label to appear next to the button on the phone LED display to remind the user of the button's function, as follows:

      - The **Short Label** field applies to most Mitel multiple-line phones and can be up to 6 characters, but only the first 5 characters display on most phones; the BB24 and IP212k can display 6 characters.
      - The **Long Label** field applies to the IP655, IP480, IP480g, IP485g, BB424, IP6910, IP6920, IP6930, IP6940, and M695 PKM models.

Note:
If you leave either the **Long Label** or **Short Label** field blank, the text you enter for one of the labels is automatically propagated to the blank field. **Long Label** text is truncated to fit the space allotted for the **Short Label**.

d. When applicable, enter the appropriate information in the fields that appear in the Target section.

e. Certain functions require a destination, but for other functions (such as speed-dial or blind transfer) a destination is optional. Some functions take only extensions, and some functions take any type of phone number.

6. Click **Save**.

12.10.2 Copying Programmable Button Configurations

You can copy the programmable button configuration from one user to another, thus reducing the tedious work of configuring IP phone buttons.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. In the **List** pane, select the **command** check box for the user whose programmable buttons you want to use as the source from which to update other users' configurations.

Note:
The selected user's information is displayed in the details pane.

4. Click **Bulk Edit**. The **Bulk Edit** tab is displayed in the details pane.
5. Use the **command** check boxes to select the user or users whose programmable buttons you want to update with the source information.
6. Scroll to the bottom of the **Bulk Edit** tab and select the check boxes for the devices (IP Phones and/or one or more button boxes) whose programmable buttons you want to copy.
7. Click **Save**.
8. Click the **Results** tab to check the status of the copy operation.

12.10.3 Enabling a User to Program Buttons on a IP Phone

Note:

The default for new Class of Service (Telephony) profiles is to have this feature disabled, thus preventing users from modifying their own programmable buttons.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the user whose profile you would like to modify to enable the user to customize IP phone buttons.

Note:
The **Details** pane displays the information for that user.

4. On the **General** tab, scroll down to the **User group** field and click the **Go to this user group** link.

Note:
The **User Groups** page for the user is displayed.

5. In the **COS – Telephony** field, click **View Class of Service**.

Note:

The **Telephony Features Permissions** page is displayed.

6. In the **Details** pane, select the **Allow customization of IP phone buttons and client monitor windows** check box.
7. Click **Save**.

12.10.4 Customizing Buttons on a Phone or Button Box via the Telephone Interface

Through the telephone interface, users can customize programmable buttons on IP phones, and the BB24, and BB424 phones. The IP230, 400-Series, 6900-Series (6910,

6920, 6930, and 6940) and the BB424 phones support a limited set of programmable buttons. The other IP phones support a broad set of functions to be programmed. For details about customizing programmable buttons from the telephone interface, see the user guide for the particular phone model.

Note:

- The BB424 IP485g phone supports the BB424.
- The 6900-Series (6910, 6920, 6930, and 6940) phones supports Programmable Key Modules (PKMs). For more information about PKMs, refer to the *Mitel M695 Programmable Key Module Installation Guide*.

12.11 Configuring a Hotline Button

A Hotline is a bi-directional ringdown circuit accessed through IP phone or Connect client buttons. A hotline call is initiated by pressing the assigned button. Hotline calls can be configured as speed dial or intercom calls.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page is displayed.
3. Click the name of the user for whom you want to program a hotline button.

Note:
The **IP Phone Buttons** tab for that user is displayed in the details pane.

4. Click the subtab for the phone or button box where you want to configure a hotline button.

Note:
The subtab displays the buttons for that device.

5. Identify the button # that you want to configure, and do the following:

   a. In the first **Function** field, select **All** or **Telephony**.
   b. In the second field, select **Hotline**.
   c. In the **Long Label** and **Short Label** fields, enter a label to appear next to the button on the phone or button box LED display to remind the user of the button's function.

   Note:
   For details about labels, see Configuring Programmable Buttons through Connect Director on page 333.

   d. In the **Extension** field, enter the extension to which you want the call to connect.
   e. In the **Call Action** field, select the method you want to use for making the connection.
6. Click **Save**.

12.12 Implementing Malicious Call Trace

Mitel provides organizations with the ability to report a malicious call by requesting the Connect client trace and record the source of the incoming call. Organizations can provide users with the Malicious Call Trace (MCT) capability to initiate a sequence of events that trace a call when malicious intent is suspected.

MCT enables the Mitel phone user to identify the source of malicious calls. A user, who receives a malicious call from the PSTN over an ISDN trunk supporting MCT, can initiate a MCT on the phone by pressing a programmable button, entering a star code sequence, or using the Connect client toolbar button.

After the user initiates the MCT process, the Mitel Windows Event Log is notified and the user receives an urgent email confirming the action along with an audible tone. The system provider is notified through the PSTN of the malicious nature of the call. This allows the system provider to take action, such as notifying legal authorities.

Note:

MCT is an ISDN feature. It is implemented on BRI and PRI trunks to ISDN service providers that support the feature. The Mitel implementation of MCT supports the ETSI standard that is configurable on switches that support Euro-ISDN. Trace information is not provided to or displayed on the Mitel user phones.

12.12.1 Configuring a Programmable Button for Malicious Call Trace

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page is displayed.
3. Click the name of the user for whom you want to configure a programmable button for Malicious Call Trace.

Note:

The **IP Phone Buttons** tab for that user is displayed in the **Details** pane.

4. Click the subtab for the phone or button box where you want to configure the button for Malicious Call Trace.

Note:

The subtab displays the buttons for that device.

5. Identify the button # that you want to configure and do the following:

   a. In the first Function field, select **All** or **Telephony**.
   b. In the second field, select **Malicious Call Trace**.
   c. In the **Long Label** and **Short Label** fields, type a label to appear next to the button on the phone or button box LED display to remind the user of the button's function.

(For details about labels, see Configuring Programmable Buttons through Connect Director on page 333.)

d. In the **Mailbox** field, enter the user mailbox where the event logs should be sent.

e. In the **Call Action** field, select the method to use for making the connection.

6. Click **Save**.

12.12.2 Initiating a Malicious Call Trace

You can initiate a malicious call trace through a star code, a programmable button, or the Connect client.

12.12.2.1 By Using a (*) Star Code

On a IP phone, third-party SIP phone, analog phone, or Extension Assignment device, the user must place the suspected malicious call on hold and then enter the MCT star code (***21**) to start the tracing process.

Example: The user receives an incoming malicious call. Using an IP phone, third-party SIP phone, Analog phone or Extension Assignment device the user presses the hold button and then enters ***21** to start the trace sequence. Once the trace sequence starts, a confirmation tone will be played prior to returning to the call to indicate that an MCT request has been initiated, an event is logged in Connect Director, record call is attempted to the local extension's mailbox, and an urgent email is sent to the recipient of the call.

12.12.2.2 By Using a Programmable Button

On a IP phone, the user presses the programmed button to start the tracing process.

Example: The user receives an incoming malicious call. Using a IP phone with programmable keys, the user presses the programmable key which will start the trace sequence. Once the trace sequence starts, a confirmation tone will be played to indicate that an MCT request has been initiated, an event is logged in Connect Director, record call is attempted to the configured extension's mailbox, and an urgent email is sent to the recipient of the call.

12.12.2.3 By Using the Connect Client Toolbar Button

Using the Connect client, select the **Toolbar** button to start the tracing process.

Using Softphone, press the **IP Programmable Button** to start the tracing process. The signal requesting MCT initiation is sent to the switch through TMS.

Note:

The Connect client does not support the initiation of MCT using the star code.

12.12.2.3.1 Example

The user receives an incoming malicious call through the Connect client or a softphone, the user can press the programmable toolbar key which will start the trace sequence. Once the trace sequence starts, a confirmation tone will be played to indicate that an MCT request has been initiated, an event is logged in Connect Director, record call is attempted to the configured extension's mailbox, and an urgent email is sent to the recipient of the call.

12.12.3 Considerations for Using Malicious Call Trace

When setting up your system, keep the following considerations in mind:

- The Mitel MCT feature will only work with carriers supporting ETSI standard EN 300 130-1 V1.2.4.
- Mitel switches support the malicious call identification originating function (MCID-O) only. They do not support the malicious call identification terminating function (MCID-T). If the switch receives a notification from the network of a malicious call identification, it ignores the notification.
- The MCT feature is supported only for incoming calls from the ISDN network.
- The service provider must have MCID functionality enabled for the feature to work.
- Mitel ISDN interface on the SGE1/BRI switches must have the Protocol Type set to ISDN User with the Central Office Type set to Euro ISDN. When MCID is initiated on a third-party SIP phone by putting a call on hold and initiating the star code *21 sequence, after the successful initiation of the signal the previous call continues to be held. User needs to manually unhold the call. For IP phones and analog phones, the held call is connected back after MCT initiation.
- Malicious Call Trace confirmation tone is not given to third-party SIP phones. Calls on third-party SIP phones are not automatically taken off hold.
- Connect client and Softphone do not support initiation through the star code sequence.
- The Connect client for mobile platforms does not support the Malicious Call Trace feature.
- Malicious Call Trace confirmation tone signals an invocation attempt. It does not signal that the MCT request was successfully received at the connected network (CO). The MCT response is not processed by the ISDN stack.

- Malicious Call Trace phone programmable button may configure a target mailbox for recording the call, but MCT initiated via star code will always be recorded to the initiating user's mailbox (no way to specify target).
- Malicious Call Trace attempt can only be issued once per call.
- Malicious Call Trace invocation is only valid while the call is established.
- Malicious Call Trace is not supported on conference calls created on a MiVoice Connect system.
- Intercommunication/Networking considerations. MCID caller info on calls between different networks is subject to agreement between the service providers.

12.13 Configuring VPN Phones

The VPN phone capability allows remote workers to have a full and familiar IP phone experience. For remote IP phones using the MiVoice Connect system, secure audio communication between the remote phone and the Headquarters site is provided through VPN tunnels.

A virtual private network (VPN) is a computer network in which some internode links are facilitated via open connections or virtual circuits through a larger network instead of via physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network. One common application is secure communications through the public Internet.

The feature includes an Open SSL VPN client in the IP phone and an Open SSL VPN Gateway. The Open SSL structure allows the traversal of firewalls implemented by many enterprises for blocking VPN tunnels.

The method used to provide VPN capability differs depending on the phone model:

- For IP400-Series phones, VPN access is enabled through the Edge Gateway appliance. For details about enabling VPN access for 400-Series phones, see Implementing VPN Access for 400-Series Phones on page 341.
- For IP phones IP655, IP565g, IP560g, and IP230g, VPN access is enabled through a VPN concentrator. For details about enabling VPN access for these phone models, see Implementing VPN Access for IP655, IP565g, IP560g, and IP230g Phones on page 342.

12.13.1 Implementing VPN Access for 400-Series Phones

Enabling VPN access on 400-Series phones involves the following high-level steps:

- Set up the Virtual Edge Gateway appliance.
- Configure the VPN settings on each 400-Series phone that you want to provide to users as remote phones.

12.13.1.1 Setting up the Edge Gateway Appliance

The Edge Gateway appliance uses the Remote Access Secure Tunneling (RAST) protocol to provide VPN access. You must install and configure this virtual appliance before you can configure VPN on a phone. This involves first using Connect Director to add and configure the Virtual Edge Gateway appliance and then using the Connect Edge Gateway Administration Portal to specify other necessary parameters. For complete details, see the *Edge Gateway Administration Guide*.

12.13.1.2 Enabling VPN Access on a Phone

1. On the phone's key pad, press the **MUTE** button and dial the numbers corresponding to **SETUP#** (73887#).

> **Note**:
>
> The **Admin options** menu and **Admin password** fields are displayed.

2. Enter the Administrative password following by **#**. The **Admin options** menu is displayed
3. Scroll to VPN, and press the **Open** soft key.
4. With the **Use VPN** field highlighted, press the **Toggle** soft key to change the setting to **On**.
5. In the **VPN gateway** field, enter the IP address of the Edge Gateway appliance.
6. In the **VPN gateway port** field, accept the default port (443) or change the value to a different port number.
7. Press the **Back** soft key.
8. Press the **Apply** soft key. The phone reboots and then prompts you for user credentials.
9. At the prompt, enter your extension and voicemail password.
10. Press the **OK** soft key.

12.13.2 Implementing VPN Access for IP655, IP565g, IP560g, and IP230g Phones

To implement VPN phone support on these phone models requires two components – a VPN Concentrator and an IP phone capable of communicating over a VPN.

Mitel offers two VPN Concentrator models:

- **VPN Concentrator 5300LF/5300LF2** – supports a capacity of 100 calls.
- **VPN Concentrator 4500/4550** – supports a capacity of 10 calls.

The VPN Concentrator is located at Mitel's Headquarters site, connected to the same LAN as local switches and the Headquarters server. For specific deployment options based on the router and firewall configuration of the Mitel network, refer to the *VPN Concentrator 4500/5300 Installation and Configuration Guide*.

The SSL-based VPN Concentrator enables remote IP phones to establish secure voice communications with through the local Mitel PBX through SSL VPN tunnels. For every tunnel, a virtual PPP interface is created on VPN Concentrator and a peer PPP interface is created on the remote IP phone. Signaling and media streams go through the PPP interface and are secured by SSL encryption.

For IP655, IP565g, IP560g, and IP230g phones, Mitel licenses VPN phone usage on a stunnel basis. A stunnel provide SSL tunnels between a remote device and a VPN gateway. Establishing a stunnel requires an available VPN phone license. If the number of active stunnels equals the number of available licenses, the VPN Concentrator will not establish new stunnels until an existing stunnel is disconnected.

Each remote device is assigned a user name and password that is recognized by the VPN Concentrator. Phone logging into the Concentrator are authenticated through the verification of its user name and password. When the phone is successfully authenticated, the Concentrator establishes a stunnel to that phone, after which it can receive and make phone calls through the MiVoice Connect system. The stunnel remains in place until the phone sets the VPN parameter to off or the Concentrator times out all stunnel connections.

After a stunnel is established from the IP phone to the Concentrator, VPN phone calls are performed from the IP phone in the same manner as if the phone is located on the same LAN as the VPN Concentrator. The VPN Concentrator manages the connection from the phone to the MiVoice Connect system.

12.13.2.1 Implementing VPN Support

Implementing VPN support for IP655, IP565g, IP560g, and IP230g phones involves the following high-level steps:

1. Install and configure the VPN Concentrator.
2. Modify system settings in Connect Director.
3. Configure the IP phone.

The following sections provide details for these steps.

12.13.2.1.1 Installing and Configuring the VPN Concentrator

Refer to the *VPN Concentrator 4500/5300 Installation and Configuration Guide* for instructions on physically inserting the VPN Concentrator into the network. The guide also describes web browser pages that configure the VPN concentrator. The following sections describe the pages and fields in this interface that require configuration.

The VPN Concentrator is shipped with the pre-configured IP address 192.168.1.1 for the LAN port.

To access the VPN Concentrator web interface pages:

1. Assign static IP address 192.168.1.2 with subnet 255.255.255.0 to the Ethernet interface of the computer that is connected to the LAN port.
2. Launch a web browser and access the following URL: http://192.168.1.1.
3. Enter the following parameter values to log into the system:
   - **Username**– root
   - **Password**– default
4. Select Network in the blue Configuration Menu on the left side of the page, and then enter the appropriate values in the following fields:
   - **LAN Interface Settings:** Enter the IP address by which other LAN devices will access the VPN Concentrator.
   - **WAN Interface Settings:** Enter the IP address by which remote devices can access the VPN Concentrator.
5. Select **Stunnel** in the blue **Configuration Menu** on the left side of the page, and verify that the following parameters are set properly:
   - **Stunnel Enable** is selected.
   - **Stunnel Server IP Address** is set to the LAN address of the VPN Concentrator, as specified on the Network page.
   - **Stunnel Server Port Number** is set to **443**.
6. Select **System** > **Route** in the blue **Configuration Menu** on the left side of the page, and add any desired static routes to networks or servers on the LAN as follows:
   a. Enter the subnet address and mask in the **IP Network** and **Netmask data** fields, respectively.
   b. Enter the IP address that accesses the Gateway server of the added network.
   c. Click **Submit**.

7. To add a user account for Stunnel access to the VPN Concentrator, select **Stunnel > Username Database** in the blue Configuration Menu on the left side of the page and do the following:

   a. Enter the username and password for the user in the **Username** and **Password** data fields, respectively.
   b. Re-enter the password in the **Confirm Password** data entry field.
   c. Click **Submit**.

12.13.2.1.2 Modifying System Settings in Connect Director to Support VPN Phones

Connect Director assigns codecs on the basis of the site assignment of the IP phone's IP address. Assigning the IP address block allocated to the VPN Concentrator to a specific site assures that the switch uses the proper codec when handling VPN Calls.

To set the IP address range:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page appears.
3. Click **New**. The **General** tab, which includes blank fields for the new IP address range, is displayed.
4. In the **Site** field, select the VPN site.
5. In the **Low IP address** field, enter the lowest IP address of the block allocated to VPN calls. The IP address must be valid for the network where the site is located.
6. In the **High IP address** field, enter the highest IP address of the block allocated to VPN calls.
7. Click **Save**.

Note:
See E911 Configuration Options for configuration recommendations for Emergency 911 related features on VPN phones.

12.13.2.1.3 Configuring IP Phones to Make VPN Calls

You must manually configure IP phones to establish a tunnel with the VPN concentrator. After the phone is configured and placed on a WAN port (such as the Internet), it

attempts to communicate with the Concentrator. Mitel does not provide DHCP options for automatically setting these parameter values at startup.

To configure VPN on the phones:

1. Press the **MUTE** button, and then enter the numbers for **SETUP#** (73887#).
2. Enter the administrative password, followed by **#**.
3. Press **#** to step through the phone options and configure the following parameters:

- **VPN Gateway:** This parameter specifies the WAN IP address of the VPN Concentrator to which the IP phone connects. Default value is 0.0.0.0.
- **VPN Port:** This parameter specifies the port number of the VPN Concentrator to which the IP phone connects.
- **VPN:** This parameter, when set to On, enables VPN Phone on the IP phone. Default setting is Off.
- **VPN User Prompt:** This parameter, when set to On, programs the IP phone to prompt the user for a VPN user name after completing a power cycle.
- **VPN Password Prompt:** This parameter, when set to On, programs the IP phone to prompt the user for a VPN password after completing a power cycle.
- **FTP:** This parameter specifies the IP address of the RTP server from which the phone requests VPN Phone software upgrades. When set to the default value of 0.0.0.0, the phone solicits upgrades from the IP address of the VPN Gateway.

12.13.2.1.4 Configuring the VPN User Name and Password

The user name and password is stored in non-volatile RAM on the phone. Power cycling and normal phone operations have no effect on the stored name and password. The VPN Concentrator authenticates the IP phone when the phone attempts to establish a stunnel by verifying that the phone's username and password is included in the user accounts on the Users list page.

New IP phones are shipped with this memory location vacant. The first time a user power cycles the phone with the VPN parameter set to On, the phone prompts the user for a username and password. The phone prompts for these values if the VPN User Prompt and VPN Password Prompt parameters are set to On; otherwise, the IP phone continues using the previous memory contents when attempting to establish a stunnel.

12.14 Configuring Simultaneous Ringing and Call Move

Simultaneous ringing allows a Mitel user to configure up to two additional phones to ring in addition to their assigned phone. You can configure simultaneous ringing for a user

from their user page in Connect Director, or a user can configure it through the Connect client. The feature can also be configured from some phone interfaces.

When the feature is configured, calls to the Mitel extension of the user ring the primary phone and all additional configured phones simultaneously. For convenience, the user can turn the feature on or off to stop the simultaneous ringing at any time.

Incoming calls to simultaneous ringing devices are presented as standard calls with standard ringtone. A ring delay can be configured for additional destinations that allows the preferred phone to ring first.

After a simultaneous ringing call is established, the user may move the call between the simultaneous ringing devices. The Call Move mechanism can be initiated through a IP phone soft key, a programmed button, the Connect client, or star code ***23**.

12.14.1 Implementing Simultaneous Ringing

Administrators can enable simultaneous ringing through the Class of Service Edit Telephony Features Permissions page. Any Mitel user's profile may be configured for simultaneous ringing. After a Mitel user's profile is configured for simultaneous ringing, their extension becomes preferred. This extension can be configured as a standard system extension, external Extension Assignment, SoftPhone, VPN phone, or third-party SIP phone.

Before users can enable simultaneous ringing of their phones, you must first modify the default Class of Service to provide the necessary permissions.

12.14.1.1 Modifying Class of Service

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**. The **Telephony Features Permissions** page is displayed.
3. Do one of the following:

   - To modify an existing set of telephony features permissions, in the **List** pane click the name of the set of permissions.
   - To add a new set of telephony features permissions, click **New** to create a new Class of Service.

Note:

The **Details** pane displays the **General** tab, which lists information for the new or existing feature set.

4. Select the **Allow external call forwarding and find me destinations** check box.
5. Select the **Allow additional phones to ring simultaneously and to move calls** check box.
6. In the **Scope** section, click a radio button to specify the type of calls for which users of this class of service can use these features.
7. Click **Save**.

12.14.1.2 Configuring Simultaneous Ringing in Connect Director

You can configure simultaneous ringing for a user through Connect Director, and users can configure this feature through the Connect client or the phone interface.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page appears.
3. Click the name of the user whose profile you want to modify. The **Details** pane displays information for that user.
4. Click the **Routing** tab, and then click the **Phones** subtab.
5. For each additional phone you want to configure, do the following:

    a. Enter a label for the phone.
    b. Enter the phone number of the additional phone in the appropriate row.
    c. In the **Activation** field, select the method the user is to use to answer calls:

        - **Accept call by answering:** Requires the user to remove the phone from the hook and speak.
        - **Accept call by pressing '1'**: Requires the user to press 1 on the phone keypad to signal that they are answering.

    d. In the **Number of Rings** field, enter the number of times you want the phone to ring before the call is rerouted.
6. Click the **Ring Me** subtab.

7. For each phone you want to configure to ring simultaneously, do the following:

   a. Select which availability states the simultaneous ringing applies to.
   b. In the **Simultaneously ring** drop-down list, select which phone should ring simultaneously.
   c. If you want to specify another phone to ring simultaneously, select a phone from the **Also ring** drop-down list.

> **Note**:
> For details about device types allowed for additional extensions, see Other Considerations for Call Move on page 350.

8. Click **Save**.

12.14.2 Disabling/Enabling Additional Phones

Through the Connect client or the phone interface, users can turn Additional Phones on or off as needed. Consult the Connect client documentation or the phone user guides for details.

12.14.3 Implementing Call Move

Connect supports call move, which allows users to switch from one phone device to another without disrupting the conversation. For instance, if a user is participating in a conference call, the user can easily move the call from the desk phone to a cell phone and leave the office, without disrupting the conference.

12.14.3.1 Call Move from an IP Phone or the Connect Client

The user can move a call as follows:

- When the call is on the assigned phone and the user presses the **Move** soft key on the phone or uses the Move Call action in the Connect client, the following events happen:
  - The call goes on hold. Simultaneous ringing on idle phone(s) lasts until the user picks up one of the phones. (The preferred phone does not ring.) Until the user picks up the call, the caller hears silence.
  - Additional phones start ringing with no ring delay.
  - Ringing on Additional phones stops after the user answers the call on the Additional phone.
  - When the user answers the Additional phone, the call is moved to that Additional phone.
- When the call is on one of the Additional Phones and the user presses the **Move** soft key on the assigned phone or uses the Move Call action in the Connect client, the conversation is immediately switched to the assigned phone.

12.14.3.2 Call Move Using Star Code on a Mobile Phone

To activate Call Move, dial ***23** (at the dial tone).

Simultaneously ringing idle phones ring until the user answers one of them. Until then, the caller hears silence.

Additional destinations will ring.

When the call is answered on the additional phone, the call is moved to the new device.

12.14.3.3 Cancelling Call Move

- Unhold the call, or execute ***23** code again.
- If the Cancel is successful, the call is retrieved.

12.14.3.4 Other Considerations for Call Move

- Only SIP extension type phones (including the 400-Series and 6900-Series (6910, 6920, 6930, and 6940) IP phones), external numbers, or off-system extension (OSE) devices can be configured as additional devices.
- If a conference call is in progress, the call move operation is not allowed.
- Call Move pull functionality is not supported from additional destinations.
- Call Move push functionality is supported on SIP trunks only if they support DTMF signaling using SIP INFO.
- Call Move or configuring simultaneous ringing is supported on the Connect client.
- The only supported star code sequences from additional destinations is *23.
- The Connect client only displays calls on the assigned phone.

- Call Move or configuring simultaneous ringing is not supported from Mobility Client.
- When OSE is configured as additional phone, care should be taken to make sure the call is directly placed to OSE and not AA.
- When a cell phone is configured as an additional phone, care should be taken to set the activation mode to 'answer by pressing 1' so that when the call is redirected to cell phone voicemail, other simultaneous ringing destinations do not stop ringing.
- If the preferred user is a workgroup agent, the **WrapUp** soft key is displayed instead of the **AddOn/ AddOff** soft key (or the **Add'l phone** soft key on the IP485g). However, if the user receives a personal call (not a WorkGroup/Contact Center call), the **Move** soft key is displayed

Note:

For 6900-Series (6910, 6920, 6930, and 6940) phones, unlike 400-Series IP phones, the location of the agent related softkeys does not collide with the **Simultaneous ring** and **Call Move** softkeys.

Setting Call Control Options 13

This chapter contains the following sections:

This chapter provides information about configuring the system-wide call control features of the MiVoice Connect system.

13.1 Configuring Account Codes

Account codes are typically used to assist Mitel users in the billing of their clients. For example, if a law firm wants to keep track of the length of calls to their clients so that they may later bill those clients for services rendered, they can enter an account code that corresponds to that client before dialing the client's phone number. At the end of the call, the call length, time, and date are entered in a record, thus helping the firm to keep track of the calls made to each of their clients.

Account codes can vary in length and be flexibly formatted. In addition, account codes can be configured so that an account code is optional or required for users placing outbound calls. In this way, the account code can also function to prevent unauthorized employees from dialing long-distance numbers.

Mitel supports wildcard characters in account codes. This enhancement allows the system to surpass the previous limit of 50,000 account codes so that an almost unlimited number of account codes can be supported. The wildcard character – a question mark

– can be entered in place of DTMF digits in the account code. Each wildcard character matches any numbered DTMF digit.

The use of wildcards introduces less strict validation of the account code entered by the user. Rather than checking each individual code, a length check is performed. The introduction of wildcards into the account codes does not impact the ability of the system to assign an account code to an individual client. Account codes with and without wildcards can be configured on the same system. However, a single account code cannot contain a mix of digits and wildcard characters.

You can create account codes with non-numeric characters, but these characters are discarded during code collection. The following table shows example account codes and describes how the Account Codes Service interprets the code.

Table 87: Sample Account Codes

Sample Account Code	Recorded Code
Sales 200	200
1001-3	10013
1.234A	1234
3000 Exec 2	30002

Account code collection is enabled based on selections made in the user groups settings; the collection of account codes is set to one of the following states:

- None
- Optional
- Required

For information about account codes and user groups, see Adding or Editing a Bridged Call Appearance on page 361.

Call Detail Record (CDR) reports include account code details associated with outbound calling. Account Codes are associated with a configurable extension and have a dedicated user group, named “Account Code Services” that defines ultimate call permissions and trunk group access.

A new user group named “Account Code Service” is created, by default, for use by the Account Codes Service. Because this user group is intended only for use by the Account Codes Service, it does not appear in User group drop-down lists for assignment to users or other objects such as workgroups. You can, however, change all the parameters of the

Account Codes Service user group except for the fields indicating whether account codes are disabled, optional, or required.

13.1.1 Collecting Account Codes

When account code collection is enabled or required for a user group, calls placed through the telephone or through Connect client are routed to the account code extension. The Account Codes Service prompts the user to enter an account code followed by the “#” key. If the account code entered does not match the digits in a stored account code, an explanation message is played and the user can enter an account code again. When a matching account code is collected, the call is placed according to the originally dialed number.

For user groups configured with account codes, call permissions define which dialed numbers are directed to the Account Codes Service. Calls that are redirected to the account codes extension are completed with the trunk access and call permissions of the Account Codes Service.

This structure imposes two sets of permissions on outbound calls:

1. The call permissions applied to the user group to which the user who places the call is assigned determine whether an account code must be collected or not.
2. The call permissions applied to the Account Code Service user group determine whether calls are finally placed or if the intercept tone is played.

Account code restrictions do not affect calls that are forwarded to external numbers. Instead, the Class of Service (COS) settings control the forwarding of calls to external numbers. For more information, see Specifying a Class of Service on page 461.

The Account Codes Service applies to the system extensions on the SoftSwitch running on the Headquarters server only. If the Headquarters SoftSwitch is not reachable by the originating voice switch, the call is processed according to the settings for the user group associated with the user who places the call.

Specifically, during loss of connectivity, the originator's assigned user group configuration determines the following call routing:

- For end users who have optional account code collection, the system places the calls.
- For users who have forced account code collection, the system automatically rejects the call attempts.

13.1.2 Viewing Account Codes

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Account Codes**. The **Account Codes** page is displayed.

13.1.3 Adding or Editing Account Codes

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Account Codes**. The **Account Codes** page opens.

Note:
The **Filter Account Code** section allows you to search for an existing account code by name or account code. To search, enter the beginning string of the name or account code in the Name or Account Code field and click **Find Now**. To display the entire list, leave both fields blank and click **Find Now**.

3. Do one of the following:

- To edit an existing account code, click the name of the account code in the **List** pane.
- To create a copy of an existing account code, click **Copy**.
- To create a new account code, click **New**. The **General** tab in the details pane displays parameters for the new or existing account code.

4. In the **Name** field, enter the name for the account code.
5. In the **Account code** field, enter the account code.

Note:
Account codes can include up to 20 alpha-numeric characters and must include at least one digit. Digits are significant characters and may not be replicated in multiple account codes. For example, the system identifies 8888, p88q88, and abc8de8fg8hij8 as the same code: 8888.

6. Click **Save**.

Note:
For information about enabling account codes for a user group, see Configuring User Groups on page 481.

13.1.4 Configuring Multi-Site Account Codes

Many organizations need to track calls made to clients so that they can bill the clients for the time they spend on the call. The Multi-Site Account Codes feature allows the Headquarters server, a Distributed Voicemail Server, or a voicemail switch to validate account codes. This feature is beneficial because it distributes the processing of the account code validation load, thus eliminating any single point of failure for account code validation.

Account code validation is performed by the Headquarters server by default. Outbound external calls are redirected to the Headquarters server for account code validation. Once the account code is validated, the call is redirected to the originally dialed external number.

The Multi-Site Account Codes feature adds the capability of allowing a Distributed Voicemail Server or voicemail-enabled switch to validate account codes. In addition, if the Distributed Voice Server or voicemail-enabled switch is unavailable, the Account Code validation migrates to another server or voicemail-enabled switch (following the site's hierarchy). This process helps account code validation to be more reliable in a multi-site environment.

To configure multi-site account codes, you need to do the following:

- Review the system wide account code extension and change it if it conflicts with the existing dial plan.
- Change the account code local extension for the Headquarters server.
- Add the account code local extension to the DVS.
- Add the account code local extension to the voicemail-enabled switch.
- Change users' call permissions to restrict outbound external calls.

13.1.4.1 Changing the System-wide Account Code Extension

The system-wide Account Code Extension is populated by default when the Mitel software is installed on the Headquarters server. If the system-wide Account Code Extension conflicts with the existing customer dial plan, the administrator can change the Account Code Extension.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Dialing Plan** > **Systems Extensions**. The **System Extensions** page is displayed.
3. Under **Account codes**, in the **Extension** field, enter the new system-wide account code extension.
4. Click **Save**.

13.1.4.2 Changing the Account Code Local Extension for HQ Server

The account code local extension is populated by default for the Headquarters server only.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. In the **Name** column, click **Headquarters**. The **General** tab in the **Details** pane displays parameters for the Headquarters server.
4. Select the **Voice Application** tab.
5. In the **Account code local extension** field, enter the new account code local extension for the Headquarters server.
6. Click **Save**.

13.1.4.3 Adding Account Code Local Extension to the DVS

The Account Code Local Extension is not populated by default for distributed voicemail servers (DVSs). The administrator must manually enter the extension.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. In the **Name** column, click **Headquarters**. The **General** tab in the **Details** pane displays parameters for the Headquarters server.
4. Select the **Voice Application** tab.
5. In the **Account code local extension** field, enter the account code local extension for the server.
6. Click **Save**.

13.1.4.4 Adding Account Code Local Extension to Voicemail-Enabled Switch

The Account Code Local Extension is not populated by default for voicemail-enabled switches. The administrator must manually enter the extension.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.

3. In the **Name** column, click the name of the desired voicemail switch (50V or 90V).

> **Note**:
>
> The **General** tab in the **Details** pane displays parameters for the voicemail switch.

4. Select the **Voice Application** tab.
5. In the **Account code local extension** field, enter the account code local extension for the server.
6. Click **Save**.

13.1.4.4.1 Additional Configuration Requirements

Once the system has been configured to validate account codes, the MiVoice Connect system administrator must restrict the users' call permissions so that outbound external calls are not permitted. See Call Permissions on page 475 for details.

13.1.5 Using Account Codes

To use account codes, the user picks up the phone and dials an external number. The call is redirected to a Server or voicemail-enabled switch, and the user is prompted to enter an account code. The person enters the account code and presses the # key. If the user enters a valid account code, the call is recorded in the database and redirected to the external destination. The MiVoice Connect system administrator can then run account code reports to show the time, date, and length of the call.

If the user repeatedly dials an incorrect account code, and the MiVoice Connect system administrator has configured the caller's user group such that it is mandatory to enter an account code (Forced), the call will be dropped.

If the user repeatedly dials an incorrect account code, and the MiVoice Connect system administrator has configured the caller's user group such that it is optional to enter an account code (Optional), the call will proceed to the external number, but it will not be recorded in the database and made available to Account Code reports.

13.2 Configuring Bridged Call Appearances

A Bridged Call Appearance (BCA) is an extension that is shared among multiple users. A BCA has an internal extension number and call stack depth. Each user with the same BCA sees the same BCA extension number, and the number of calls that can reside on

that BCA is its call stack depth. The maximum BCA stack size is 24 or 36, depending on the type of switch.

Some characteristics of a BCA are as follows:

- It does not require a license.
- It is assigned to a voice switch.
- It supports Availability States.
- It cannot be controlled by a schedule.

A user answers a BCA call by pressing a IP phone button that is assigned to a BCA call stack position. Calls to a BCA occupy distinct call appearance buttons and are identified by their position in the call stack. IP phone buttons that answer calls are configured to handle calls to a specific call stack position of a BCA. A button can be programmed for each position in the call stack.

13.2.1 Example BCA Scenario

The system administrator configures a BCA with an extension of 118 and a call stack depth of 3. The IP phones of three users are configured to handle calls to the BCA as follows:

- User One has one button that answers calls from Stack Position #1.
- User Two has one button that answers calls from Stack Position #2.
- User Three has three buttons configured to answer BCA calls. The first button answers calls to Stack Position #1, the second button answers calls to Stack Position #2, and the third button answers calls to Stack Position #3.

The first incoming call to the BCA arrives on Stack Position #1. User Two cannot answer this call. A second call to the BCA will arrive on Stack Position #2 if the first call is still active. User One cannot answer that call. User Three is the only user that can answer calls that arrive on Stack Position #3.

When a call stack position on a BCA receives a call, the button on each phone configured for that stack position flashes green to indicate an incoming call. When the call is answered, the LED on the phone of the person that answers it turns solid green while the other BCA stack buttons are red (without BCA conferencing) or orange (when BCA Conferencing has been enabled for the BCA).

A user places a call from a BCA by pressing a programmed IP phone button. The LED on the outbound caller's phone becomes solid green, and the buttons associated with the BCA stack position on all other phones become solid red. If the call is placed on hold, the button LED for the applicable call stack position on all phones indicates a call on hold.

Pressing the top-most BCA custom button for outbound calls does not necessarily access trunk 1. No one-to-one correlation exists between the custom buttons

programmed for BCA extensions and a particular trunk. The system administrator can associate trunks with BCA extensions through a variety of approaches.

A caller ID number can be associated with a BCA. The following rules determine which caller ID number is displayed at the far end for an outbound BCA call:

- Outbound to an internal extension – one of the following is sent, depending on the configuration of the Call Control Options (see Call Control Options Parameters on page 427 for more information):
  - The name and number of the user that initiated the BCA call. If the user's extension is private, the caller ID is blank.
  - The name and extension of the BCA. If the BCA extension is private, the caller ID is blank.
- Outbound to an external number – the system sends the first number in the following list that is available:
  - Outbound caller ID number that is assigned to the BCA
  - DID number assigned to the BCA
  - External identification or caller ID number of the user who initiates the BCA call
- Outbound to an external emergency number (such as 911) – the emergency identification or the user's CESID number is sent.

The system can be configured to display the caller ID on inbound calls. It can also be configured to enable, disable, or delay inbound call ringing.

13.2.2 Switch Support for Bridged Call Appearances

Mitel one-rack unit (1-U) Half Width and 1-U Full Width voice switches support BCAs with the following limits:

- Up to 24 BCA extensions can be configured on a switch.
- Up to 128 BCA extensions (on other switches) can be monitored.
- A maximum of 32 phones can be configured to point to the same BCA extension.

Note:

It is recommended that users of the BCA feature be moved to the same managing IP Phone appliance that the BCA extension is assigned to. Administrators should monitor these assignments because the managing appliance can change after maintenance or a hardware failure.

13.2.3 Viewing Bridged Call Appearances

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Bridged Call Appearances**. The **Bridged Call Appearances** page opens.

Note:
For descriptions of the columns in the list pane on the Bridged Call Appearances page, see Bridged Call Appearances Page: List Pane.

Table 88: Bridged Call Appearances Page: List Pane

Column Name	Description
Name	Name of the BCA.
Extension	Extension number for the BCA.
Switch	The IP host name of the Mitel voice switch to which the BCA is connected.

13.2.4 Adding or Editing a Bridged Call Appearance

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Bridged Call Appearances**. The **Bridged Call Appearances** page opens.
3. Do one of the following:
   - To edit an existing BCA, click the name of the BCA in the **List** pane.
   - To create a copy of an existing BCA, click **Copy**.
   - To create a new BCA, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing BCA.
4. Review the parameters on all of the tabs in the **Details** pane, and specify values as appropriate.

Note:
For more information about all of the BCA parameters on the various tabs of the details pane, see BCA Parameters on page 362.

5. Click **Save**.

13.2.5 BCA Parameters

A bridged call appearance has many details. You configure BCA parameters on the following tabs, which you can access on the details pane for a particular BCA:

- General Tab
- DNIS Tab

13.2.5.1 General Tab

General information about new and existing BCAs is provided on the **General** tab in the details pane of the Bridged Call Appearances page.

Bridged Call Appearances Page: General Tab describes the parameters on the **General** tab of the **Bridged Call Appearances** page.

Table 89: Bridged Call Appearances Page: General Tab

Parameter	Description
Name	Specifies the name of the BCA.
Extension	Specifies the extension on which the BCA receives calls.
Show References	Click to display a list of everywhere this extension is used.

Parameter	Description
Backup extension	Specifies the extension that receives calls for the BCA when the switch that supports the BCA is out of service. **Note**: If another BCA serves as the backup extension, the two BCAs must be assigned to different switches.
DID Settings	Click change settings to display the following DID settings: • Enable DID • DID Range • DID number
Enable DID	Select this check box to authorize a BCA to use a DID number. See Configuring DID on page 239 for additional information about DID numbers and ranges.
DID Range	If a BCA is authorized for a DID, in the drop-down list select a DID range for the BCA.
View System Directory for DID usage	Click this link to view the System Directory page, with directory details for this BCA.
DID number	Specifies the DID number for the BCA.

Parameter	Description
Outbound caller ID	Specifies the caller ID number that the system sends on an outbound BCA call to an external number. **Note**: When placing an outbound BCA call to an internal number, one of the following is sent, depending on the configuration of the Call Control Options. See Call Control Options Parameters on page 427 for more information. • The name and number of the user that initiated the BCA call. If the user's extension is private, the caller ID is blank. • The name and extension of the BCA. If the BCA extension is private, the caller ID is blank.
Include in System Dial by Name directory	Select this check box to enable the BCA extension to appear on a IP phone display when a user presses the Directory button.
Make extension private	Select this check box to make the BCA extension private. See Configuring Private Extensions on page 547 for more information about private extensions.
Switch	In the drop-down list, select the voice switch to which to assign the BCA.

Parameter	Description
Call stack depth	Specifies the maximum number of simultaneous calls that can be “stacked” on the BCA. When this number is met, additional inbound calls are routed to the call forward destination specified for Call stack full.
Forward after	Specifies the number of times to ring the BCA before sending the call to the call forward destination.
Call forward destinations	Specifies the numbers to forward inbound BCA calls to when the calls are not answered before the specified number of rings or because the specified call stack depth has been reached. • **Call stack full** - Specifies the number to forward calls to when the specified call stack depth has been reached. • **No answer** - Specifies the number to forward calls to when the call is unanswered after the specified number of rings.
Allow bridge conferencing	Select this check box to allow conferencing on the BCA.

Parameter	Description
Default privacy settings	Specifies whether to initially allow other users of the BCA to join active BCA conference calls. • **Other parties can't join** (default) - Select this option to initially prevent other users of the BCA from joining active BCA conference calls. • **Other parties can join** - Select this to initially allow other users of the BCA to join active BCA conference calls. **Note**: These options are only available if bridge conferencing is enabled for the BCA.
Provide tone when parties join	Select this check box to play a tone whenever another party joins a conference call on the BCA. **Note**: This option is only available if bridge conferencing is enabled for the BCA and other parties are allowed to join.

13.2.5.2 DNIS Tab

Bridged Call Appearances Page: DNIS Tab describes the parameters on the **DNIS** tab of the **Bridged Call Appearances** page.

Table 90: Bridged Call Appearances Page: DNIS Tab

Parameter	Description
Add	To associate the BCA with a DNIS, click **Add** and provide details for the DNIS mapping in the displayed fields.
Trunk group name	From the drop-down list, select the trunk group for the DNIS mapping.
Digits	Enter the DNIS number.
Description	Provide a description for the DNIS number. This description is seen by call recipients and in call detail reports (CDRs). The description length can be up to 26 characters.
Music on Hold	From the drop-down list, select a file-based MOH resource.
Remove	If you want to remove a DNIS system that is configured for this BCA, click **Remove**.

13.2.6 Bulk Editing BCA

You can use the Bulk Edit feature to change the switch for multiple BCAs at the same time.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Bridged Call Appearances**. The **Bridged Call Appearances** page opens.
3. In the **List** pane, select the check box for each BCA you want to include in the bulk edit.
4. Click **Bulk Edit**. The **Bulk Edit** tab in the **Details** pane displays the Switch parameter for editing.
5. Select the **Include in change** check box.
6. In the **Switch** list, select the switch to assign all selected BCAs to.
7. Click **Save**.
8. Click the **Results** tab to check the status of the bulk edit operation.

13.2.7 Configuring an IP Phone Button for a BCA Extension

This section describes how to configure an IP Phone button for a BCA extension. Users answer BCA calls by pressing programmed IP phone button. BCA buttons are configured to answer calls at a specific stack position of a BCA extension.

Note:

- IP phone buttons can also be configured so that a BCA call is answered when the user lifts the handset or presses either the speaker or headset button.
- Admins and BOSS do not receive BCA notifications if the BCA call is answered using the Client toolbar while logged in to the Connect client in Deskphone mode. To prevent this, configure the same call stack of BCA programmable buttons on the phone and on the BCA client toolbar of the Connect client for the administrator.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page opens.
3. In the **First Name** column, click the name of the user you want to configure BCA answer options for.

Note:
The **IP Phone Buttons** tab in the **Details** pane displays parameters for the user's IP phone buttons.

4. Select the subtab for the device the user will use to answer BCA calls; **IP Phones** or **Button Box**.
5. In the first column for the button to configure, select **All** or **Telephony.**
6. In the **Function** column, select **Bridged Call Appearance**. The **Bridged Call Appearance** options are displayed.
7. In the **Long Label** and **Short Label** fields, enter a label to appear next to the button on the phone LED display to remind the user of the button's function.

Note:
For details about phone button labels, see Configuring Programmable Buttons through Connect Director on page 333.

8. In the **Extension** field, enter the BCA extension to assign to the button.
9. In the **Call stack position** list, select the individual calls to the BCA extension that the IP Phone Button can access.
10. In the **Ring delay before alert** list, select one of the following:

    - **None** - to start ringing the phone audibly on the first ring.
    - **1, 2, 3**, or **4** - to ring the phone silently for the selected number of rings before ringing the phone audibly.
    - **Don’t Ring** - to not ring the phone audibly.
11. Under **Show caller ID on monitored extensions**, select one of the following:

    - **Never** - to not show caller ID for inbound BCA calls.
    - **Only when ringing** - to show caller ID for inbound BCA calls only when the phone is ringing.
    - **Always** - to show caller ID for inbound BCA calls when the phone is ringing and as long as the call is connected.
12. Do one of the following:

    - Select the **Enable Auto-Answer When Ringing** check box to enable the user to answer a BCA call by picking up the handset, hook-flashes, or by pressing the programmed IP phone button, speaker button, headset button, or an unused call appearance button.
    - Clear the **Enable Auto-Answer When Ringing** check box to enable the user to answer a BCA call only by pressing the programmed **IP phone** or the **Answer** option.

Note:

- For the **Allow Auto Answer** of a BCA call to work, the Delay Before Audibly Ringing parameter must be set to a value other than **Don't Ring**.
- If you are using headset with a 6900-Series IP phone, ensure that the **Audio** mode on the phone is set to either **headset**, **headset/speaker**, or **speaker/ headset**.
- The **Allow Auto Answer** of a BCA call is not supported on 6900-Series IP phones running firmware earlier than version 6.1.
- If the **Show caller ID** option is set to **Never** and **Auto answer** is enabled, the Call 1 CID will be displayed for incoming BCA calls only (while in **Ringing** state).
- If the **Show caller ID** option is set to **Never** and **Auto answer** is disabled, NO CID will be displayed on the phones for BCA calls in **Ringing**, **Active**, or **Held** states.

13. Under **No connected call action**, select one of the following ringdown behavior options for the BCA button:

    - **Answer only** - to disable ringdown.
    - **Dial tone** - to configure the phone as the recipient on a ringdown circuit.
    - **Dial extension** - to configure the button as the initiating end of a ringdown circuit when the recipient is an IP phone on the Mitel network; type the desired extension in the field.
    - **Dial external** - to configure the button as the calling end of a ringdown circuit when the recipient is a device that is not on the Mitel network; type the desired external number in the field.

    Note:
    For more information about configuring ringdown, see Configuring Automatic Ringdown Circuits on page 447.

14. Click **Save**.

13.3 Configuring Bridged Call Appearance Conferencing

This section describes BCA conferencing. BCA conferencing is available to regular BCA users and SCA users (and their assistants).

Bridged Call Appearances are set up to be private by default, so a BCA or SCA user with a call in progress cannot be joined by other BCA users on the same extension. However, the default setting can be changed to allow others to join, and an override on the phone lets the owner of the call lock or unlock the conference regardless of the default.

When a call is made to the BCA line, the flashing orange BCA button turns green when the user answers the BCA call. Other BCA users see either of the following on this line:

- A solid orange LED if conferencing is allowed: If the button is orange, the BCA user can press the button to join the BCA call in progress.
- A solid red LED if conferencing is disallowed: If the button is red, users cannot join the active BCA call unless the owner of the call presses the Unlock button on his or her phone.

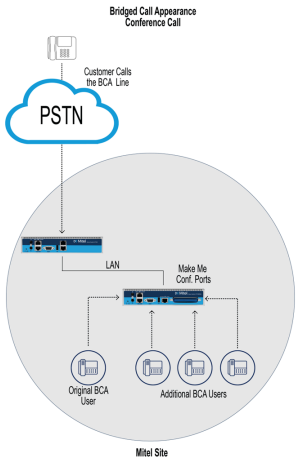
With permission, a BCA user can join the active BCA call by pressing the orange BCA button on the phone. Bridged Call Appearance Conference Call shows that other BCA users have joined a BCA call. In the figure, note that the caller directly connects to the original BCA users' IP phone. The phone of each additional BCA user is transferred to a voice switch with available Make Me Conference ports that directly connects each additional BCA user.

13.3.1 Answering and Joining a BCA Call

When a call comes in to a BCA line, the color of the BCA button indicates if the BCA call is ringing, has been answered, is private, or allows conferencing.

- When the BCA line is ringing, the BCA button programmed on each IP Phone blinks green.
- The first user who picks up the line sees a solid green button labeled for the BCA.
- Other users of the BCA see either an orange or red button, as follows:
  - If the button is orange, the user can press the button to attempt to join the call. If enough Make Me Conference ports are available and the maximum number of allowed conferenced parties has not been reached, the user is added to the active bridged call.
  - If the BCA button is red and the user presses the button, an error message displays on the phone and the user is not able to join the conference call.

Figure 9: Bridged Call Appearance Conference Call



13.3.2 Enabling BCA Conferencing for BCA and SCA Users

For the selected BCA user, the entire window is active. For an SCA user, only the conference area of the BCA edit window is activate. The reason is that BCA parameters for the SCA user are inherited from the SCA account.

The SCA user always owns the conference call and can decide when other BCA users are admitted to the conference. An SCA user can override the default privacy setting by toggling the **Lock/Unlock** soft key on the phone. The text above the soft key describes the action to be applied to the active call; the soft key text label toggles between **Lock** and **Unlock**. For example, to make the call private, the user with the call presses the **Lock** soft key. To make the call available for conferencing, the user presses the **Unlock** soft key.

Note:

SCA users are differentiated in the Bridged Call Appearances list pane using the format *<first name>_<last name>_<extension>*, where the following is true:

- *first name* represents the first name of the user
- *last name* represents the last name of the user
- *extension* represents the user's extension

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Bridged Call Appearances**. The **Bridged Call Appearances** page opens.
3. Do one of the following:

   - To edit an existing BCA or SCA user, click the name of the BCA or SCA user in the **List** pane.
   - To create a copy of an existing BCA or SCA user, click **Copy**.
   - To create a new BCA, click **New**.

   Note:
   The **General** tab in the **Details** pane displays parameters for the new or existing BCA or SCA user.

4. Select the **Allow bridge conferencing** check box.
5. Under **Default privacy settings**, select one of the following:

   - **Other parties can't join** (default) - to prevent other users of the BCA from joining active BCA conference calls.
   - **Other parties can join** - to initially allow other users of the BCA to join active BCA conference calls.

6. Select the **Provide tone when parties join** check box to play a tone whenever a party joins the BCA conference.
7. Click **Save**.
8. Program an IP phone button for the BCA for each of the appropriate IP phones.

Note:
For more information about assigning the BCA to IP phone buttons, see Configuring an IP Phone Button for a BCA Extension on page 368.

9. Configure the appropriate number of Make Me Conference ports on a voice switch that is available to the site.

13.4 Configuring Shared Call Appearance

The Shared Call Appearance (SCA) feature provides call appearances that are shared between an executive (the SCA user) and an assistant (configured as a regular BCA user). The assistant can monitor the SCA user's call appearances to facilitate call routing and conferencing needs. With SCA, an assistant can help executives with their communication needs by making or answering calls on behalf of the executive and by setting up phone conferences. The assistant is not restricted to supporting an executive and can receive other telephony capabilities through Connect Director. The system has the flexibility to support multiple executives and assistants for different call routing arrangements.

For telephone conferences, the SCA user and assistant have the following:

- BCA conferencing
- Blind conferencing
- Regular conferencing abilities that all IP phone users have

BCA conferencing allows an assistant or executive to set up conference calls so that when the executive is ready he or she can enter the conference by pressing the SCA button on the IP phone. The assistant can stay in the conference, leave the conference, or be locked out of the conference by the executive.

SCA relies on BCA as an underlying technology to support its functionality. All IP phone models except IP420, IP420g, IP115, IP110, and IP6910 phones support SCA. Analog phones do not support SCA.

13.4.1 SCA Feature Components

This section describes the main feature components of SCA. It divides components into different non-conference and conference-related areas.

13.4.1.1 Associated Bridged Call Appearance

An Associated Bridged Call Appearance (aBCA) is a bridged call appearance that is associated with an executive extension. Associated BCAs differ from other BCAs as follows:

- In Connect Director, an aBCA is specified in the **Edit User** page instead of the **Bridged Call Appearance** page.
- aBCAs are created when a Mitel extension is converted to an executive extension.

13.4.1.2 Non-Conference Functionality

When a regular user is enabled for SCA, the system automatically creates an associated BCA (aBCA) and gives it an aBCA extension number.

Nearly all the BCA parameters that could be selected for the regular BCA user are fixed. Only the label for each SCA button can be specified.

The settings for SCA IP programmable buttons are fixed at the following values:

- Ring Delay before Alert: None
- Show Caller ID on Monitored Extensions: Always
- Button push actions default: (unused)
- No Connection Call Action: Dial tone
- Call Stack Position: Automatically ordered (no manual ordering allowed)

The SCA call stack positions are automatically set and not manually configurable in Connect Director. However, call stack positions are automatically reordered if a button is specified to be other than an SCA. The SCA buttons are reconfigured around the new button type.

Note:

For a button box, the system does not auto-shift call stack positions.

When a regular user is enabled for SCA, each regular call appearance converts to an SCA. Standard call appearances do not exist for the SCA user, and no SCA button can be converted back to a regular call appearance unless the SCA configuration is removed by disabling SCA.

13.4.1.3 BCA Conferencing

The BCA conference parameters are configured on the Bridged Call Appearances page. For information about setting up BCA conferencing, see Enabling BCA Conferencing for BCA and SCA Users on page 371.

13.4.2 Enabling SCA for a User

This section outlines a sequence of steps that a system administrator might follow to set up a new SCA user and assistant and enable BCA conferencing. The purpose of this outline is to promote smoother execution of the configuration steps. Readers who are already very familiar with BCA and SCA can go directly to the steps for specifying the accounts for SCA users and assistants as well as BCA conferencing for the executive.

The tasks required for enabling SCA for a user are as follows:

1. Create the new regular user account that is intended for the SCA user. For information about adding users, see Adding or Editing a User on page 489.
2. Convert the new user to an SCA (executive) user by enabling SCA. For information about creating a new SCA user, see Creating a New Executive User on page 375.
3. Configure the IP phone buttons that the SCA user's account calls for. For information about configuring IP phone buttons for BCA, see Configuring an IP Phone Button for a BCA Extension on page 368.
4. Enable BCA conferencing. See Enabling BCA Conferencing for BCA and SCA Users on page 371Enabling BCA Conferencing for BCA and SCA Users.
5. Program IP phone buttons on the assistant user's device for the aBCA associated with the SCA (executive) user. See Programming an Assistant's IP Phone Button for aBCA on page 378.

13.4.2.1 Creating a New Executive User

The configuration tasks in this section apply to a new executive (SCA) user and a new administrator (regular BCA) in a subsequent section. Other types of steps for configuring a new user apply to the executive and administrator accounts, but they are largely omitted here. For details on user accounts, see Configuring User Groups on page 481.

Note:
If the executive and assistant need to manage SCA calls in Connect client, the Access License for each of these users must be Operator.

Creating a new user with SCA enabled:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Do one of the following:

   - To edit an existing user, click the name of the user in the **List** pane.
   - To create a copy of an existing user, click **Copy**.
   - To create a new user, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing user.

4. In the **First name** and **Last name** fields, enter the first and last name of the new user.
5. In the **Access license** list, select **Professional** or **Operator**. Connect client requires the Operator license to display the BCA Window.
6. In the **Primary phone port** section, select **IP phone**, and then select the specific phone in the drop-down list.

Note:
If an IP phone model of sufficient capability is not recognizable in the list of MAC addresses, the correct phone can be determined by matching the IP phone model number to a MAC address on the **Telephones** page in Connect Director (**Administration > Telephones > Telephones**).

7. Click **Save**.

Note:

Before enabling SCA for a new user, the system administrator must save the user parameters after entering the basic user parameters. The Enable SCA check box becomes active only after this intermediate save.

8. Select the **Telephony** tab in the details pane.

Note:
The telephony features parameters for the user are displayed.

9. Select the **Enable shared call appearances** check box.

> **Note**:
> The associated BCA extension is populated automatically.

10. Optional: Enter a different associated BCA extension in the **Enable shared call appearances** field.

    The next available extension number is automatically generated when shared call appearances is enabled. If the system administrator has an organized scheme for extension numbers, manual entry of the extension number may be desired. Manually entering the extension can also be valuable in case an auto-generated number is outside the number management scheme.

> **Note**:
>
> A number must be deemed acceptable before saving the SCA parameters. After the SCA parameters have been saved, the associated BCA extension can only be changed by first disabling and then again enabling SCA for the user.

11. In the **Call stack depth** field, type a value for the depth of the call stack.

    This is the number of SCA buttons that the executive has. This number is subsequently reflected on the IP Phones subtab of the IP Phone Buttons subtab for programming IP phone buttons. The system default is 8, but some planning for resource usage is recommended. For example, some executives might need only two or three SCA buttons while others might need eight or more, and planning should have been completed for button boxes and how many executives one assistant might have to support.
12. Click **Save**.
13. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page opens
14. In the **First Name** column, click the name of the user you just created.

> **Note**:
> The **IP Phone Buttons** tab in the **Details** pane displays parameters for the user's IP phone buttons.

15. Select the subtab for the device the user will use to answer SCA calls; **IP Phones** or **Button Box**.

16. In the **Long Label** and **Short Label** fields for each SCA button, type a label to appear next to the button on the phone LED display.

Note:
All other parameters are fixed for an SCA button. However, you can also program non-SCA buttons for other functions, such as speed dial, hotline, and so on.

17. Click **Save**.

The executive account has been created, but conferencing and default privacy settings for the SCA user still need to be configured. To configure the conference-related details for the SCA user, see Enabling BCA Conferencing for BCA and SCA Users on page 371.

13.4.3 Programming an Assistant's IP Phone Button for aBCA

Note:
When the SCA feature is used, the executive and associated assistants should be managed by the same IP Phone appliance. Administrators should monitor these assignments because the managing appliance might change after maintenance or a hardware failure.

This section describes how to allow a regular BCA user to monitor an executive's call appearances. In order to do this, the BCA user must have an IP phone button programmed for the aBCA associated with the executive.

The number of executives who can be monitored by a single assistant should be limited to a maximum of six (six aBCA's with no more than three stack buttons each, for a maximum of 18 aBCA buttons). The number of assistants who can monitor a particular executive user should not exceed four.

Making all the executive's call appearances visible to the assistant is not required. If an executive wants one or more lines to be hidden from the assistant, the administrator omits the requested number of hidden lines from the assistant's configuration.

For complete information about programming an IP phone button for a BCA, see Configuring an IP Phone Button for a BCA Extension on page 368.

Note: The No Answer Number of Rings and Call Forward Destination parameters reflect the initial values of these parameters. However, the real-time state of these parameters can change, based on the activity of the user. For a regular BCA user, these parameters are editable in the BCA window in Connect Director. In contrast, for an SCA user (tied

to an aBCA), these parameters are grayed out in the window because the SCA user inherits the parameters when the system creates the aBCA. Thereafter, if the SCA user is changing these parameters in real time, the changes are actually inherited in the aBCA, but the BCA page in Connect Director is not updated to reflect the changes. Put another way, Connect Director continues to reflect the initial value of these two SCA parameters.

13.4.4 Usage Guidelines for SCA

This section contains SCA usage scenarios and suggestions.

Note:

- The SCA feature is not recommended for executives or monitoring assistants who are remote (work from home) users.
- When an executive extension is routed to a phone that does not have programmable buttons, the executive extension behaves as a normal extension. Eventually, when the executive's calls are routed to a phone with programmable buttons, the behavior of the extension reverts back to an executive extension.

13.4.4.1 Bridged Call Appearance Monitoring

The Bridged Call Appearance Monitor is a Connect client window that displays all Bridged Call Appearances accessible to the user's extension through all devices assigned to the user. The BCA Monitor consolidates all of a user's aBCA activity into a single panel.

The Bridged Call Appearance Monitor is available in Connect client only if the Access License for the user is Operator.

In Connect client, because calls are tracked as BCA calls in the BCA monitor window, the active call cell disappears when a call is put on hold, and the held call can be viewed only in the BCA monitor window.

aBCA is hidden in the phone directory list so that users do not accidentally call an aBCA instead of the executive. However, as with regular BCAs, the system administrator can configure an aBCA as the destination of a trunk group or the targeted extension of a programmable button function. The system administrator has the discretion to decide how to use aBCA.

Placing an executive extension call on hold parks the call on the aBCA. Held calls on an executive extension are viewable in the Bridged Call Appearance Monitor in Connect client or in the IP phone display.

13.4.4.2 Assistant Users

Assistant accounts need no special configuration for the monitoring of the executive's call appearances other than the assignment of programmable buttons for IP phones. However, for monitoring of executive call appearances in Connect client, the assistant's Access License must be Operator.

An assistant should not be configured with the SCA feature. The SCA feature should be configured only for the executive user.

Note:

With bridge conferencing allowed, the practice of multiple assistant users barging into the same executive call is not recommended.

13.4.4.2.1 Hotline

A typical SCA setup includes a hotline circuit between an executive and assistant. They use a hotline circuit to communicate requests, responses, and status of calls.

To land a call on a hotline button for intercom or speed dial, both parties must have a hotline-programmed button. In the absence of this programming, the offered call is processed as a regular call.

Hotline calls and Extension Monitor calls to an executive extension that are picked up are not bridged. For details on how to configure a hotline button, see Copying Programmable Button Configurations on page 334.

Note:

- A hotline intercom call uses the intercom permissions of the user. Therefore, the rules that apply to that user's regular intercom also apply to a hotline-intercom call.
- To reduce system presence messaging, Dial Number (Speed Dial) buttons to the executive should not be configured for the assistant.

13.4.5 Inbound and Outbound SCA Calls

This section describes the typical actions that executives and assistants take when an assistant takes a call on behalf of an executive and when an assistant places a call on

behalf of an executive. In this section, blind conferencing is not used. Examples of blind conferencing are provided in Blind Conferencing and the SCA User on page 382.

13.4.5.1 Assistant Support for Inbound Calls

The following scenario describes a typical sequence of actions when an assistant takes a call on behalf of an executive.

1. The inbound call triggers a flashing orange light on the IP phone of both the assistant and the executive. If the Access License of the executive and assistant is Operator, Connect client also signals the incoming call. (The executive can pick up the call and preempt the assistant's involvement with the call).
2. The assistant answers the call on the flashing BCA button and can, for example, get the caller's name and purpose.
3. The assistant puts the call on hold.

Note:

The executive call timer is reset if the executive puts the call on hold.

4. The assistant presses the hotline button shared with the executive.
5. The assistant tells the executive of the call in progress (on hold) and gives pertinent information about the call.
6. The executive picks up the call by pressing the flashing orange SCA button.

Note:

Internal users who call an executive see the called party ID aBCA while the phone is ringing and the actual executive number after the call is picked up.

13.4.5.2 Assistant Support for Outbound Calls

The following scenario describes a typical sequence of actions when the assistant sets up a call for the executive.

1. The assistant accesses one of the executive's call appearances by pressing an appropriate IP phone or Connect client button.

2. The assistant calls the intended recipient of the executive's call.
3. The assistant places the called party on hold.
4. The assistant presses the hotline button to the executive.
5. The assistant tells the executive of the call in progress (on hold) and provides information about the call as needed.
6. The executive picks up the call by pressing the flashing orange button that the assistant has identified.

Note:

An executive extension's redial list shows only outbound calls.

13.4.6 Blind Conferencing and the SCA User

This section illustrates blind conferencing and the SCA user in two contexts. In one situation, the assistant receives a call on behalf of the executive while the executive is already on a call. In the other context, the executive is on a call but then asks the assistant to call someone and conference the called party into the existing call.

13.4.6.1 Blind Conferencing of an Inbound Call

1. The executive is currently on a call with party number one.
2. The assistant receives a call from a second party.
3. The assistant determines that the executive is on a call and wants the second party to join the executive's call.
4. The assistant hotlines the executive to say that the second party is on the line and ready to join the call.
5. The hotline call ends, and the executive is connected back to party one, and the assistant is connected back to party two.
6. The assistant initiates a conference and selects the executive's call into which party two must join.

After the conference connection is completed, parties one and two are in the same call.

13.4.6.2 Blind Conferencing of an Outbound Call

1. The executive is on the phone with party one and uses the hotline to ask the assistant to bring another party into the call.

2. The executive goes back on-line with party one.
3. The assistant calls party two.
4. The assistant hotlines the executive to say that party two is ready to join.
5. The assistant adds party two by initiating the blind conference and then pushing the button for the executive's active call appearance.

13.5 Configuring Silent Coach

Silent Coach is a Connect client feature that lets a user (the initiator) intervene in another user's active call and communicate with that user (the recipient). The initiator can speak to the recipient and listen to all other participants on the call. The recipient is the only call participant that can hear the initiator.

The right to use Silent Coach is set by the system administrator. The system administrator also specifies the users (recipients) whose calls the initiator can monitor. A Telephony Class of Service (COS) assigns Silent Coach rights. Silent Coach can be initiated through various IP Phone models or through Connect client.

The following are details about Silent Coach Behavior:

- Silent Coach lets the initiator switch between Silent Monitor, Barge In, and Silent Coach functions for the same call.
- Silent Coach sessions can be initiated through IP Phone or Connect client programmable buttons, Connect client menu options, and star code calls from other calling devices.
- The initiator of a Silent Coach session can change the session to a Silent Monitor or Barge In session. Silent Monitor sessions can be changed into a Silent Coach sessions.
- The recipient can place the original call on hold to engage in a two-way conversation with the Silent Coach initiator. At the end of this conversation, the user can resume or terminate the original call.
- Silent Coach cannot be initiated with users who are on conference calls.
- A call with an active Silent Coach session cannot be transferred or converted to a conference call.
- The recipient cannot record calls while Silent Coach is active.

Note:

The following devices do not support session transitions, coach consulting, or coach resumption.

- Analog phones
- IP110

13.5.1 Configuring Silent Coach Permissions

Silent Coach access is controlled through Telephony COS settings. Permissions for monitoring calls or having calls monitored are configured through the Silent Monitor/ Silent Coach option on the Telephony Class of Service Edit panel.

To configure Silent Coach for a Telephony Class of Service:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**. The **Telephony Features Permissions** page opens.
3. Do one of the following:

   - To edit an existing set of telephony features, click the name of one of the preconfigured COS profiles (Fully Featured, Minimally Featured, or Partially Featured).
   - To create a new class of service for telephony features, click **New**.

Note:
In the **Details** pane, the **Telephony Features Permissions** page for the new or existing class of service is displayed.

4. Under **Silent monitor / Silent coach other's calls**, do the following:

   a. Select the **Allow Initiation** check box.
   b. In the **Accept** section, select one of the following options:

   - **None** - to prevent users with this COS from having their calls monitored.
   - **All** - to allow users with this COS to have their calls monitored.
   - **Only From** - to allow only the specified users to monitor the calls of users with this COS

5. Click **Save**.

13.5.2 Enabling the Silent Coach Warning Tone

Mitel provides an option for playing a warning tone to all call participants when a Silent Coach session is initiated. The warning tone setting applies to all Silent Coach sessions on the system. When a user transitions between Silent Coach and silent monitor, the warning tones are based on the Silent Coach or silent monitor warning tone setting.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Options**. The **Call Control Options** page opens.
3. Select the **Enable Silent Coach warning tone** check box.

13.5.3 Configuring Silent Coach Buttons

IP Phone and Connect client programmable buttons can be configured to initiate a Silent Coach session with a specific user or to query the caller for a Silent Coach destination. The configuration processes for IP Phone and Connect client programmable buttons are almost identical.

To configure an IP Phone button to initiate Silent Coach:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page opens.
3. In the list pane, click the name of the user that you want to allow to initiate the silent coach feature.

Note:
The **IP Phone Buttons** tab in the **Details** pane displays parameters for the selected user.

4. Select the **IP Phone Buttons** tab in the **Details** pane.

Note:
The telephony features parameters for the user are displayed.

5. Select the **IP Phones** subtab.
6. In the first column for the button to configure, select **All** or **Telephony**.
7. In the **Function** column, select **Silent Coach**. The Extension field is displayed.
8. In the **Long Label** and **Short Label** fields, enter a label to appear next to the button on the phone LED display.

Note:
For details about phone button labels, see Configuring Programmable Buttons through Connect Director on page 333.

9. Optional: To program the button to monitor the calls of a specific user, enterthe user's extension in the **Extension** field.

Note:
If an extension is not supplied, the initiator is prompted to enter an extension number to monitor each time the button is pressed.

10. Click **Save**.

13.5.4 Performing Silent Coach Operations

A user can initiate silent coach functionality through any of the following methods:

- Connect client programmable button
- Connect client menu option
- IP Phone programmable button
- On any phone, enter ***22** and the target extension.

13.5.4.1 Initiating Silent Coach Operations with Connect Client

Connect client supports two methods of initiating Silent Coach operations:

- Clicking advance call menu drop-down in the contact card.
- Press a programmable button in the tool bar.

13.5.4.1.1 Performing a Silent Coach from Connect Client Menu

Perform the following:

1. Click **People** tab, select the required contact.

> **Note**:
>
> The contact card is displayed.

2. In the Contact card, click **Advanced Call Menu** drop-down next to the green call icon.

> **Note**:
>
> The **Advanced Call Menu** drop-down is displayed.

3. In the **Advanced Call Menu**, select **Silent Coach** option.

13.5.4.1.2 Performing a Silent Coach from a Connect Client Tool Bar Button

> **Note**:
>
> Before performing a silent coach from Connect client toolbar, you must configure the Silent Coach option on the toolbar in Director.

Note:

1. Click **Add Shortcut** button in the toolbar pane.

> **Note**:
>
> The programmable buttons configured for that user is displayed.

2. Select **Silent Coach** option to add the silent coach option as a programmable button in the toolbar.
3. Click the **Silent Coach** button.

> **Note**:
>
> - If the button specifies a Silent Coach recipient, the system immediately initiates a Silent Coach session with that user. Skip the remaining steps.
> - If the button does not specify a Silent Coach recipient, Connect client displays the **Silent Coach** dialog box. In this case, continue to the next step.

4. Enter an extension or select from the drop-down list.
5. Click the **Silent Coach** button.

13.5.4.1.3 Transitioning a Silent Coach Session into a Silent Monitor or Barge In Session

Click **Advanced Call Menu** drop-down next to the green call icon and select **Monitor** or **Barge In** option.

13.5.4.2 Initiating Silent Coach Operations from a IP Phone

To initiate Silent Coach from an IP Phone button that is programmed for Silent Coach, press the Silent Coach button.

- If the button specifies a Silent Coach recipient, the system immediately initiates a Silent Coach session with that user.
- If the button does not specify a Silent Coach recipient, enter the recipient's name or number in the Telephone User Interface.

13.5.4.3 Initiating Silent Coach from Any System Phone

- Enter the ***22** code, followed by the number of the target extension.

IP phones display soft key options while a Silent Monitor option is active.

Soft key options available to the Silent Coach initiator:

- **SilMon:** Transitions the session into a Silent Monitor session.
- **Barge:** Transitions the session into a Barge In call.
- **Show:** Displays all call participants in the Telephone User Interface.
- **Hangup:** Terminates the Silent Monitor session.

The soft key options available to the Silent Coach recipient are as follows:

- **Consul:** Places the active call on hold and establishes a two-way voice path with the Silent Coach initiator.

Note:

While the recipient consults with the initiator, soft key options include:

- **Resume:** Restarts the recipient's original call.
- **Show:** Displays all of the call participants.
- **HangUp:** Terminates the call.

- **Show:** Displays all call participants in the Telephone User Interface.
- **Hangup:** Terminates the Silent Monitor session.

13.6 Configuring Hunt Groups

Hunt groups allow a call to be offered to a limited set of user extensions with no reporting, queuing, sophisticated schedules, log-in, log-out, or wrap-up states.

Note:
You must be aware that configuring a hunt group to simultaneously ring all members may introduce short, but unexpected delay from the caller's perspective. Refer to the *Delay in Audio Up To 2 Seconds for Hunt Group Calls is Considered Normal* article on the Mitel support site for additional hunt group considerations that may ensure more efficient use of this feature.

You must be aware that each hunt group is composed of an ordered list of users as follows:

- SG-generation switches — A maximum of 8 hunt groups and a maximum of 16 hunt group extensions per group can be assigned to a single switch.

  You can have up to 8 hunt groups on a switch. Each individual hunt group can have up to 16 members, and each hunt group can have a call stack of 16. The maximum number of members across all groups on the switch is 16.
- ST-generation switches — A maximum of 24 hunt groups with a maximum of 16 members each can be assigned to a single switch. Each hunt group can have a call stack of 24.
- Virtual switches — A maximum of 24 hunt groups with a maximum of 16 members each can be assigned to a single virtual switch. Each hunt group can have a call stack of 16.

Note:

- Consider that the maximum group and member values listed here are subject to the overall capacity of the switch and must take into consideration all other features that use switch resources. Refer to the formulas in the *Real Time Capacity* section of the *MiVoice Connect Planning and Installation Guide* for more information about how switch resources are calculated.
- Other hunt groups can be added as hunt group members, but this is not recommended due to the possibility of creating call flow loops, other errors, and potential system instability. However, you can use another hunt group extension as the call stack full destination.

If your requirements are more complex, you should use workgroups.

Rather than being reliant on the Headquarters server, a hunt group can be assigned to the switch closest to the agents and/or trunks associated with it. The switch controls the hunting, with no dependency on the server. Hunt groups have an extension number and, optionally, can also have a DID and/or DNIS number. They can be call forward

extensions for users, workgroups, route points, personal assistants, site fax redirect extensions, site operator extensions, and the target for trunk groups. They are also allowed as the backup destination for workgroups and route points. This can be useful to allow some basic call routing when the workgroup server is not reachable.

The caller ID displayed for a hunt call is the external caller's ID.

A user may belong to more than one hunt group. In addition, a user assigned to a workgroup may also be assigned to hunt groups. Each call is hunted as a new call; that is, if the hunt mode is top down, each new call begins hunting from the top of the list. In this case, the person at the top of the list will get most of the calls.

13.6.1 Viewing Hunt Groups

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Hunt Groups**. The **Hunt Groups** page opens.

Note:
For descriptions of the columns on the Hunt Groups page, see Hunt Groups Page: List Pane.

Table 91: Hunt Groups Page: List Pane

Column Name	Description
Name	Name of the hunt group.
Extension	Extension number for the hunt group.
Switch	The IP host name of the Mitel voice switch to which the individual trunk is connected.
Members	Number of members in the hunt group.
On-Hours	The current On-Hours schedule used for the hunt group.
Holiday	The current Holiday schedule used for the hunt group.

13.6.2 Adding or Editing a Hunt Group

Note:

You can use the Bulk Edit feature to change the switch for multiple hunt groups at the same time. See Bulk Editing Hunt Groups on page 399 for more information.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Hunt Groups**. The **Hunt Groups** page is displayed.
3. Do one of the following:
   - To edit an existing hunt group, click the name of the hunt group in the **List** pane.
   - To create a copy of an existing hunt group, click **Copy**.
   - To create a new hunt group, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing hunt group.
4. Review the parameters on all of the tabs in the details pane, and specify values as appropriate. For more information about all of the hunt group parameters on the various tabs of the details pane, see Hunt Group Parameters on page 392.
5. Click **Save**.

13.6.3 Hunt Group Parameters

A hunt group has many details. You configure hunt group parameters on the following tabs, which you can access on the details pane for a particular hunt group:

13.6.3.1 General Tab

General information about new and existing hunt groups is provided on the **General** tab in the **Details** pane of the **Hunt Groups** page.

The following table describes the parameters on the **General** tab of the **Hunt Groups** page.

Table 92: Hunt Groups Page: General Tab

Parameter	Description
Name	Specifies the name of the hunt group.
Extension	Specifies the hunt group's extension. **Note**: Each hunt group must have a unique extension number.
Show References	Click to display a list of everywhere this extension is used.
Backup extension	Specifies the hunt group backup extension. The backup extension supports back-up call routing in case of a system failure. This extension can be another hunt group, a workgroup, a route point, or a user's extension. If a call is not answered by the hunt group because of a system malfunction such as an unavailable server or network problem, the call is routed to the backup extension.
DID Settings	Click **change settings** to display the following DID settings: • Enable DID • DID Range • DID number
Enable DID	Select this check box to authorize a hunt group to use a DID number.

Parameter	Description
DID Range	If a hunt group is authorized for a DID, in the drop-down list select a DID range for the hunt group. Before you can specify a DID range, DID services must be configured for the desired trunk group, which is enabled by default if a DID trunk group is configured.
View System Directory for DID usage	Click this link to view the System Directory page, with directory details for this hunt group.
DID number	Specifies the DID number for the hunt group.
Include in System Dial By Name directory	Select this check box if you want the hunt group to be included in the auto-attendant's dial-by-name directory.
Make extension private	Select this check box to remove this number from the system directory and call routing destination lists. For more information about private numbers, see Configuring Private Extensions on page 547.
Switch	The Mitel voice switch to which the hunt group is connected.
Call stack depth	Specifies the maximum number of simultaneous calls that can be "stacked" on the hunt group extension. When this number is met, additional inbound calls are routed to the call forward destination specified for Call stack full.

Parameter	Description
Distribution pattern	Select one of the following options for distributing incoming calls to members of the hunt group: • **Top Down** starts with the first member in the member list and sequentially searches through the list until an available member is found. • **Simultaneous** sends the call to all available members simultaneously. For information about changing the order of the member list, see Changing the Position of Member in the Member List on page 397.
Rings per member	Specifies the number of times to ring a member's phone before forwarding the call to the next member in the hunt group.
No answer number of rings	Specifies the number of times to ring the last member's phone before forwarding the call to the No answer Call forward destination.
Call member when forwarding all calls	Select this check box to offer a call to a hunt group member even if the member's availability state is set to Call Forward Always.
Skip member if already on a call	Select this check box to prevent calls from being offered to a member when the member's phone is busy or currently being offered a call, even if the member's call stack is not full.

Parameter	Description
Call forward destinations	Specifies the numbers to forward inbound hunt group calls to when the calls are not answered before the specified number of rings or because the specified call stack depth has been reached. • **Call stack full** - Specifies the number to forward calls to when the specified call stack depth has been reached. • **No answer** - Specifies the number to forward calls to when the call is unanswered after the specified number of rings.
Off-hours/Holiday destination	The destination for inbound calls during off-hours and holiday schedules.
On-hours schedule	The current On-Hours schedule used for the hunt group. Click **View schedule** to view details for the selected schedule.
Holiday schedule	The current Holiday schedule used for the hunt group. Click **View schedule** to view details for the selected schedule.
Current availability state	The current availability state.

13.6.3.2 Members Tab

On the **Members** tab of the **Hunt Group** page, you can add and remove members from a hunt group and change the order of the member list.

The following table describes the parameters on the **Members** tab of the **Hunt Group** page.

Table 93: Hunt Groups Page: Members Tab

Parameter	Definition
Available	Displays the extension and name for each member that is available to add to the hunt group.
Selected	Displays the extension and name for each member that is a member of the hunt group.

13.6.3.3 Adding or Removing a Member from the Hunt Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Hunt Groups**. The **Hunt Groups** page is displayed.
3. Do one of the following:
   - To edit an existing hunt group, click the name of the hunt group in the **List** pane.
   - To create a copy of an hunt group, click **Copy**.
   - To create a new hunt group, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing hunt group.
4. In the details pane, click the **Members** tab.
5. Do one of the following:
   - To add a member to the hunt group, select the member in the **Available** list and click the right arrow button to move the member to the **Selected** list.
   - To remove a member from the hunt group, select the agent in the **Selected** list and click the left arrow button to move the member to the **Available** list.
6. Click **Save**.

13.6.3.4 Changing the Position of Member in the Member List

If the call distribution pattern is Top Down, the position of the member in the hunt group list can affect how likely that member is to receive an incoming call.

When **Top Down** is selected, it is more likely that members closer to the top of list will be selected to receive a call. This is because for each new call, the hunt for a free member always begins at the top of the list.

For information about changing the call distribution pattern, see General Tab on page 392.

To change the position of a member in the member list:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Hunt Groups**. The **Hunt Groups** page is displayed.
3. Do one of the following:

   - To edit an existing hunt group, click the name of the hunt group in the **List** pane.
   - To create a copy of an existing hunt group, click **Copy**.
   - To create a new hunt group, click **New**.

   Note:
   The **General** tab in the **Details** pane displays parameters for the new or existing hunt group.

4. In the details pane, click the **Members** tab.
5. Select the member to move in the **Selected** list, and then do one of the following:

   - Click the up arrow button to move the member up in the list.
   - Click the down arrow button to move the member down in the list.

6. Click **Save**.

13.6.3.5 DNIS Tab

The following table describes the parameters on the **DNIS** tab of the **Hunt Groups** page.

Table 94: Hunt Groups Page: DNIS Tab

Column Name	Description
Add	Click **Add** to add a row to the DNIS tab.

Column Name	Description
Trunk group name	In the drop-down list, select the trunk group to assign the DNIS to. **Note**: Only trunk groups that have DNIS enabled appear in this list.
Digits	Specifies the DNIS number that the telephone company sends.
Description	Specifies a description of the DNIS identifier.
Music on Hold	Specifies the file-based MOH resource to use for the DNIS.
Remove	Click **Remove** next to the row to remove from the DNIS tab.

13.6.4 Bulk Editing Hunt Groups

You can use the Bulk Edit feature to change the switch for multiple hunt groups at the same time.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Hunt Groups**. The **Hunt Groups** page is displayed.
3. In the **List** pane, select the check box for each hunt group you want to include in the bulk edit.
4. Click **Bulk Edit**. The **Bulk Edit** tab in the details pane displays the Switch parameter for editing.
5. Select the **Include in change** check box.
6. In the **Switch** list, select the switch to connect all selected hunt groups to.
7. Click **Save**.
8. Click the **Results** tab to check the status of the bulk edit operation.

13.6.5 Setting the Hunt Group to Busy

When all members of a hunt group are unavailable, you can set the hunt group to busy. When the hunt group is set to busy, all calls to that hunt group are forwarded to the Call stack full Call forward destination specified for the hunt group. For information about setting the Call forward destinations for a hunt group, see Hunt Group Parameters on page 392.

The state of the hunt group can be changed to busy or normal from a telephone or from the Switches Maintenance page in Connect Director.

Note:

After a switch reboots, the hunt group is returned to a normal state and is available, by default.

To change the state of a hunt group from a phone:

- Press ***18**, and then enter the hunt group extension.

Note:

A confirmation prompt is played, confirming the state of the hunt group.

To change the state of a hunt group from Connect Director:

1. Launch Connect Director.
2. In the navigation pane, click **Maintenance** > **Status and Maintenance** > **Appliances**. The **Appliances** page is displayed.
3. In the **List** pane, click the switch that handles the hunt group.

Note:
The **Status** tab in the **Details** pane displays current status information for the switch.

4. In the **Hunt Groups** section, select the check box for the hunt group you want to set as busy.

5. In the **Command** list, select one of the following:
   - **Hunt group busy** - to set the hunt group to busy.
   - **Hunt group normal** - to set the hunt group to available.
6. Click **Apply**.

13.7 Configuring Music on Hold

All file-based Music on Hold (MOH) resources are uploaded using Connect Director and are stored on the Headquarters server. Whenever a new MOH resource is added to the Headquarters server, the resource is automatically distributed to all DVS/VMBs that have file-based MOH enabled. The MOH resource is then stored and accessed locally on each DVS/VMB.

Disk space usage of MOH files is shown on the Voice Mail Maintenance page in Connect Director.

The play time of the MOH is tracked for each call. When a caller is placed on hold, they will hear the MOH resource from the beginning. If the caller is taken off hold and put back on hold, the MOH file is paused and starts again where it left off.

For information about configuring file-based MOH for application servers and Voice Mail Model Switches, see Specifying Root and Administrator Passwords for CLIs on page 209.

13.7.1 Adding or Editing a Music on Hold Resource

You can add an audio file to use as a MOH resource. All MOH audio files must be CCITT µ-Law, 8 KHz, 8-bit, mono WAV formatted files.

Note:
The maximum size for a MOH file is 6835 KB. Files larger than 6835 KB cannot be distributed to the DVS servers.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Music on Hold** > **Files**. The **Music on Hold Files** page is displayed.

3. Do one of the following:
   - To edit an existing MOH resource, click the name of the MOH resource in the **List** pane.
   - To add a new MOH resource, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing MOH resource.
4. In the **Name** field, enter a name for the MOH resource.
5. Next to the **File name** field, click **Browse**.
6. Navigate to and select the file to add as a MOH resource, and then click **Open**.
7. Click **Save**.

13.7.2 Deleting a Music on Hold Resource

Deleting a MOH resource file deletes the file from the Headquarters server and all DVS/VMBs that the file was previously distributed to.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Music on Hold** > **Files**. The **Music on Hold Files** page is displayed.
3. In the **List** pane, click the MOH resource to delete.
4. Click **Delete**. A confirmation dialog box appears.
5. Click **OK** to delete the MOH resource.

13.7.3 Playing a Music on Hold Resource

You can play MOH resources from Connect Director, or you can play resources over a phone by calling the global or local MOH extension.

13.7.3.1 Playing MOH Resources from Connect Director

When you play a MOH resource from Connect Director, the resource is played through the PC speakers.

To play MOH resources from Connect Director:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Music on Hold** > **Files**. The **Music on Hold Files** page opens.
3. In the **List** pane, click the MOH resource to play.

Note:
The **General** tab in the **Details** pane displays parameters for MOH resource.

4. Click **Play File**.

13.7.3.2 Playing MOH Resources from a Phone

You can play a MOH resource from a phone by dialing the local or global MOH extension. For information about file-based MOH extensions, see the following:

- Configuring System Extensions on page 49
- Configuring Application Servers on page 115
- Configuration Parameters on page 155

To play MOH resources from a phone:

1. Dial the global or local MOH extension.

   The first MOH resource in the MOH resources list is played.
2. Press **#** to cycle through all MOH resources.

13.8 Configuring Paging Groups

As an alternative to using an in-house paging system, you can broadcast a message to a group of phones using the paging groups feature. This feature allows a system administrator to designate a group of extensions that can be paged by dialing a single system extension and recording your message. This feature can be a cost-effective alternative for environments that do not already have an overhead paging system installed.

For environments that have an overhead paging system, paging groups can be used to target your message to a select group of individuals within the organization while not exposing the message to everyone in the building, as would happen with an overhead page.

Note:

Group paging is an alternative to calling a paging number. Auto-Attendant can support group paging for internal users (if group paging meets the customer's paging needs). Group paging is not available to external callers.

13.8.1 Sending a Page to a Paging Group

Send a paging message to a paging group requires the following steps:

1. The paging group extension is dialed from a phone.
2. The paging message is recorded, and the call is ended.
3. The paging group server attempts to play the message on each affected extension.

Note:

To reduce the possibility of an audio delay when paging multiple phones in the same room, the MiVoice Connect system waits to verify that all affected extensions are ready to receive the page. This delay period is specified in the group paging group parameters. See Hunt Group Parameters on page 392for more information.

13.8.1.1 Delivering a Paging Message

- When a paging message is delivered to an on-hook IP phone, the message is played through the speaker on that phone.
- When a paging message is delivered to an IP phone or analog phone that is on an active call, the page is treated as a normal call.

Note:

If priority paging is enabled, the page is handled differently. See Priority Paging on page 410 for more information.

- Call routing does not apply to paging calls.
- The maximum number of extensions that can be paged at one time is 100.

- Paging is not available to external callers.
- Paging is not available on voice switches.

13.8.2 Viewing Paging Groups

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Paging Groups**. The **Paging Groups** page is displayed.

Note:
For descriptions of the columns on the Paging Groups page, see Paging Groups Page: List Pane.

Table 95: Paging Groups Page: List Pane

Column Name	Description
Name	Name of the paging group.
Extension	Extension number for the paging group.
Server	The name of the server that hosts the group paging.
Members	Number of members in the paging group.

13.8.3 Adding or Editing a Paging Group

Before a paging group can be implemented, an extension list must be created to specify the extensions to include in the paging group. For the purpose of paging, members of the extension list must belong to a user group that allows overhead and group paging. For information about creating extension lists, see Extension Lists on page 546.

Note:

You can use the Bulk Edit feature to change the group paging server for multiple paging groups at the same time. See Bulk Editing Paging Groups on page 408for more information.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Paging Groups**. The **Paging Groups** page is displayed.
3. Do one of the following:
   - To edit an existing paging group, click the name of the paging group in the **List** pane.
   - To create a copy of an existing paging group, click **Copy**.
   - To create a new paging group, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing paging group.

4. Review the parameters and specify values as appropriate. For descriptions of the paging group parameters, see Paging Group Parameters on page 406.
5. Click **Save**.

13.8.4 Paging Group Parameters

Table 96: Paging Groups Page: General Tab

Column Name	Description
Name	Specifies the name of the paging group.
Extension	Specifies the extension number for the paging group.
Show References	Click to display a list of everywhere this extension is used.

Column Name	Description
Group paging server	In the drop-down list, select the server to host the paging group paging.
Include in System Dial by Name directory	Select this check box if you want the paging group to be included in the auto-attendant's dial-by-name directory. **Note**: No name is recorded for a paging group. When a paging group is chosen, the extension is announced by a generic message.
Make extension private	Select this check box to remove this extension from the system directory and call routing destination lists. For more information about private numbers, see Configuring Private Extensions on page 547.
Enable priority paging	Select this check box to enable priority group paging. For more information about priority group paging, see Priority Paging on page 410. Select one of the following options to specify the phone output to use to play the priority paging message. • **Deliver group page via speakerphone** - plays the paging message on the phones speaker • **Deliver group page via active audio path** - plays the paging message on the active media source, such as a headset or handset

Column Name	Description
No answer number of rings	Specifies the number of times to ring an extension before ending the call. For analog phones, this parameter is always applied. For IP phones, this parameter is applied whenever the phone is busy.
Extension list	In the drop-down list, select the extension list to use as the paging group. For information about configuring extension lists, see Extension Lists on page 546.
Group paging synchronization delay	Specifies the amount of time the server waits to connect to all extensions in the paging group prior to sending the paging message to the phones. A synchronization delay reduces the perception of audio echo when paging large groups of phones.

13.8.5 Bulk Editing Paging Groups

You can use the Bulk Edit feature to change the group paging server for multiple paging groups at the same time.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** >**Call Control** > **Paging Groups**. The **Paging Groups** page is displayed.
3. In the **List** pane, select the check box for each paging group you want to include in the bulk edit.
4. Click **Bulk Edit**. The **Bulk Edit** tab in the **Details** pane displays the **Group paging** server parameter for editing.
5. Select the **Include in change** check box.
6. In the **Group paging server** list, select the server to host all selected paging groups.
7. Click **Save**.
8. Click the **Results** tab to check the status of the bulk edit operation.

13.8.6 Adding Overhead Paging to a Paging Group

You can add overhead paging to a paging group by including the paging extension for a site in the extension list that is applied to the paging group.

A paging extension is an extension that sends a page announcement to a site's overhead paging system when a user calls that extension. For information about configuring paging extensions, see Adding or Editing a Paging Group on page 405.

By adding a paging extension to a paging group, a user can broadcast a message to both of the following at the same time:

- A select group of user extensions
- A site's overhead paging system

Adding multiple paging extensions to an extension list provides the ability to broadcast a message to the overhead paging system of multiple sites simultaneously.

13.8.7 Multi-Site Paging

The distributed nature of business often requires that business tools available to employees in the corporate headquarters also be available to remote office workers. One such business tool is a paging system. Many businesses need to have a quick way to alert employees that a customer needs assistance or that a call is waiting.

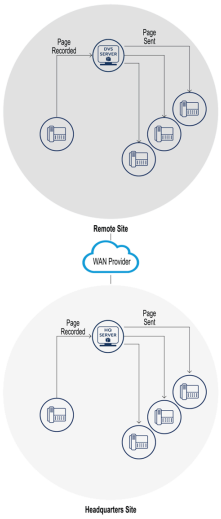
The Multi-site Paging Group feature allows employees to be paged in each remote office in an efficient manner. Multi-site Paging Groups is a Mitel enhancement that improves paging efficiency by allowing the audio for the page to be recorded and sent from a local Voicemail Server. This reduces any impact on WAN bandwidth for pages made within the Headquarters and the remote offices including any dependency on the Headquarter server.

- The Multi-site Paging Group feature allows users to pick up a phone and dial a single system extension to page a group of telephones. With Multi-site Paging Groups, the administrator can now configure local paging extensions for each site.
- The Multi-site Paging Group functionality can be implemented on the Headquarters Server and Distributed Voice Mail Servers. This feature is configured in a similar manner to the Paging Group feature implemented in previous releases.

Note:
Group paging is not available on voicemail-enabled switches.

The following figure shows a two-site implementation where each site has a Paging Group. With Multi-site Paging Groups, both pages are recorded and sent by their local server with no impact on WAN bandwidth.

Figure 10: Multi-site Paging Groups



Note:
There is no additional licensing requirement to implement Multi-site Paging Groups. This feature is not implemented on voicemail-enabled switches.

13.8.8 Priority Paging

Many organizations rely on paging for critical communications with their employees. However, paging messages that are sent to an IP phone from a paging server typically appear as normal or non-urgent calls when the phone is in use. In these instances, the individual using the phone has no indication of the priority of the page. Because of this, there is no guarantee that the individual will suspend the current call to listen to the message being delivered.

Note:

When priority paging is enabled, recipients of a paging message hear the audio of the page whether or not they are on a call. If the intended recipient is on an active call, that call is automatically placed on hold before the page is played. When the page completes, the call automatically resumes.

Normally, a user can press Hold/Transfer/Conference to end a page call. When priority paging is enabled for a paging group, the system does not allow a user to end a page call in this way and the operation is ignored.

Priority paging allows the server to act as a media relay from the source to the recipient. The call controller or the switch plays a limited role.

Note:

The priority paging feature provides new functionality to the page recipient. There are no changes in the core paging implementation.

13.8.8.1 Important Considerations

- When a previously held call is restored, the audio path of the original call is retained. However, in a special case—when the page is over a speaker phone and the user decides to “cradle” the handset, for example—the audio path is not restored to the previous audio path. The audio path would be speaker phone. This exception is for Handset only—the headphone should work as expected. The problem with Handset is that, today’s IP Phones are not notified when the user puts the handset in the cradle (and is on speaker).
- Page-over-page is not supported. For example, if you issue a priority page to an extension while the extension is already being paged, the page is presented as an incoming call. This is because priorities for page groups are not set. In other words, if priorities were assigned to page groups, a page-over-page would result in a lower priority page being put on hold and the higher priority page being answered automatically.
- Other paging group limitations apply. SIP/Analog/OAE pages will still be delivered, but the calls cannot be answered automatically.

13.9 Configuring Pickup Groups

Pickup Groups is a traditional PBX and key system feature used in group environments that allows a user to answer any ringing extension within a specified group. The feature works best in places where a set of people work together on a daily basis, such as design firms. If a group member is away from her desk and across the room when her phone rings, she can quickly answer the call from another person's phone.

Similarly, if she is out of the office and her phone rings, anyone can answer the call from another phone in the pickup group and take a note for her.

Note:

This feature is not supported on SGT1 or SGE1 switches for either the SG or the ST-generation switches.

Users are added to a pickup group using an extension list. Users are added to the extension list and then the extension list is associated with a pickup group. For information about creating extension lists, see Extension Lists on page 546.

- The user whose extension will be picked up must belong to a user group with the COS telephony features **Allow call pickup** and **Show Caller ID name and number for other extensions** enabled.
- Users need not be members of the pickup group to pick up a call.
- A pickup group can have a maximum of 24 members.
- A single switch can host a maximum of 16 pickup groups.

Note:

A single switch can host a combined total of up to 24 hunt groups, bridged call appearances, and pickup groups.

- The number of members assigned to all pickup groups on a single switch cannot exceed 80.
- A single user can be a member of up to 5 pickup groups.

13.9.1 Answering a Pickup Group Call

A call to a member of a pickup group can be answered from any phone within the same pickup group. The call can be answered from an IP phone, an analog phone, or the Connect client.

- IP phone – A button on the IP phone must be configured for pickup groups. To answer a call, the user presses the pickup group button, or key, and then enters the pickup group extension.
- Analog phone – To answer a call, the user presses *13 on the keypad, then enters the pickup group extension.

- Connect client – A button in Connect client must be configured for pickup groups or with a specific pickup group extension. To answer a call, the user does one of the following (depending on the configuration of the button.
  - Presses the pickup group button, and then enters the pickup group extension
  - Presses the button that is configured with the pickup group extension

13.9.2 Viewing Pickup Groups

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Pickup Groups**. The **Pickup Groups** page is displayed.

Note:
For descriptions of the columns on the Pickup Groups page, see Pickup Groups Page: List Pane.

Table 97: Pickup Groups Page: List Pane

Column Name	Description
Name	Name of the pickup group.
Extension	Extension number for the pickup group.
Switch	The name of the server that hosts the pickup group.
Members	Number of members in the pickup group.

13.9.3 Adding or Editing a Pickup Group

Before a pickup group can be implemented, an extension list must be created to specify the extensions to include in the pickup group. For the purpose of a pickup group, members of the extension list must belong to a user group that allows call pickup. For information about creating extension lists, see Extension Lists on page 546.

Note:

You can use the Bulk Edit feature to change the switch for multiple pickup groups at the same time. See Bulk Editing Pickup Groups on page 415 for more information.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Pickup Groups**. The **Pickup Groups** page is displayed.
3. Do one of the following:
   - To edit an existing pickup group, click the name of the pickup group in the **List** pane.
   - To create a copy of an existing pickup group, click **Copy**.
   - To create a new pickup group, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing pickup group.
4. Review the parameters and specify values as appropriate. For descriptions of the pickup group parameters, see Pickup Group Parameters on page 414.
5. Click **Save**.

13.9.4 Pickup Group Parameters

Table 98: Pickup Groups Page: General Tab

Column Name	Description
Name	Specifies the name of the pickup group.
Extension	Specifies the extension number for the pickup group. This extension is invalid and cannot be dialed, and thus acts more like a code than an actual dialable extension.
Show References	Click to display a list of everywhere this extension is used.

Column Name	Description
Switch	In the drop-down list, select the switch to host the pickup group paging. Click **View switch** to view details about the selected switch.
Extension list	In the drop-down list, select the extension list to use for the pickup group. Click **View extension list** to view details about the selected extension list. For information about configuring extension lists, see Extension Lists on page 546.

13.9.5 Bulk Editing Pickup Groups

You can use the Bulk Edit feature to change the switch for multiple pickup groups at the same time.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Pickup Groups**. The **Pickup Groups** page is displayed.
3. In the **List** pane, select the check box for each pickup group you want to include in the bulk edit.
4. Click **Bulk Edit**. The **Bulk Edit** tab in the **Details** pane displays the Switch parameter for editing.
5. Select the **Include in change** check box.
6. In the **Switch** list, select the switch to host all selected pickup groups.
7. Click **Save**.
8. Click the **Results** tab to check the status of the bulk edit operation.

13.10 Configuring Route Points

Route points allow third-party applications complete access to call control signaling (using TAPI) and the actual voice media stream (using TAPI and WAV APIs). Configuring a route point enables calls to be terminated and controlled by a server on the network. For example, administrators who are setting up a MiVoice Connect Contact Center system use this page to configure the route points they will later use as routing

destinations for IRNs and IVR server ports in MiVoice Connect Contact Center Director. Refer to the *MiVoice Connect Contact Center Administration Guide* for more information. Also, refer to the *MiVoice Connect Contact Center Installation Guide* for detailed steps regarding configuring route points specifically for use with the contact center.

13.10.1 Viewing Route Points

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Route Points**. The **Route Points** page is displayed.

Note:
For descriptions of the columns on the Route Points page, see Route Points Page: List Pane.

Table 99: Route Points Page: List Pane

Column Name	Description
Name	Name of the pickup group.
Extension	Extension number for the pickup group.
On-Hours	The current On-Hours schedule used for the route point.
Holiday	The current Holiday schedule used for the route point.
Custom	The current Custom schedule used for the route point.

13.10.2 Adding or Editing Route Points

Note:

You can use the Bulk Edit feature to change the server for multiple route points at the same time. See Bulk Editing Route Points on page 426 for more information.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Route Points**. The **Route Points** page is displayed.
3. Do one of the following:
   - To edit an existing route point, click the name of the route point in the **List** pane.
   - To create a copy of an existing route point, click **Copy**.
   - To create a new route point, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing route point.
4. Review the parameters on all of the tabs in the **Details** pane, and specify values as appropriate.

Note:
For more information about all of the route point parameters on the various tabs of the details pane, see Route Point Parameters on page 417.

5. Click **Save**.

13.10.3 Route Point Parameters

A route point has many details. You configure route point parameters on the following tabs, which you can access on the details pane for a particular route point:

- General Tab on page 417
- Routing Tab on page 421
- Voice Mail Tab on page 421
- DNIS Tab on page 425

13.10.3.1 General Tab

Table 100: Route Points Page: General Tab

Column Name	Description
Name	Specifies the name of the route point.
Extension	Specifies the extension number for the route point.
Show References	Click to display a list of everywhere this extension is used.

Column Name	Description
DID Settings	Click **change settings** to display the following DID settings: • Enable DID • DID Range • DID number
Enable DID	Select this check box to authorize a route point to use a DID number.
DID Range	If a route point is authorized for a DID, in the drop-down list select a DID range for the user.
View System Directory for DID usage	Click this link to view the System Directory page, with directory details for this route point.
DID number	Specifies the DID number for the route point.
Include in System Dial By Name directory	Select this check box if you want the route point to be included in the auto-attendant's dial-by-name directory.
Make extension private	Select this check box to remove this number from the system directory and call routing destination lists. For more information about private numbers, see Configuring Private Extensions on page 547.
Fax redirect	Select this check box to enable fax redirection. When the route point answers a call and a fax tone is detected, the fax is redirected away from the route point to the Headquarters fax extension.
Call stack depth	Specifies the maximum number of simultaneous calls that can be "stacked" on the route point. When this number is met, additional inbound calls are routed to the call forward, busy destination specified on the Routing tab.

Column Name	Description
User group	In the drop-down list, select the user group to associate with the route point. Click **View user group** to view details about the selected user group. The route point inherits Class of Service (COS) permissions from the selected user group. For information about selecting the COS for a user group, see Specifying a Class of Service on page 461.
Server	In the drop-down list, select the server to provide route point services for third-party applications. **Note**: We recommend that you select a server other than the Headquarters server and that you do not configure the selected server with mailboxes.
Language	In the drop-down list, select the language to use for the route point.
Enable mailbox	Select this check box to enable voice mail for the route point. **Note**: If a system administrator changes the extension number of a route point that has an associated mailbox, the system retains the voice mail messages.

Column Name	Description
Mailbox server	In the drop-down list, select the server to host the route point's voice mailbox. If later, the mailbox server is changed to another server, all voice mail messages are automatically moved to the new mailbox server.
Voicemail password	Specifies the password for the route point voice mailbox. The default password is *1234*. Voice mail passwords can only contain numbers.
Recorded name	Use the following buttons to record, import, and play back the route point name: • Click **Record** to record the route point name. You can use a plug-in microphone and speakers or a telephone to record or play the name. • Click **Play** to listen to the recording. • Click **Import** to import a recording of the route point name from an existing file. **Note**: Imported prompts must be CCITT µ-Law, 8 KHz, 8-bit, mono WAV files. By using the system recorder and a plug-in microphone, the recording meets these requirements by default. • Click **Preferences** to select whether to use your PC or your phone to play back your recording; you can also select a phone extension or external number to use to record the route point name. This recording of the route point name is used as a part of the default mailbox greeting, as well as for the Dial By Name directory.

13.10.3.2 Routing Tab

Information about call routing features for routing points is provided on the **Routing** tab in the **Details** pane of the **Routing Points** page. Routing is configured separately for different schedules using the schedule subtabs. The **Routing** tab includes the following subtabs:

- **On-Hours**
- **Off-Hours**
- **Holiday**
- **Custom**

For information about configuring schedules, see Overview on page 621.

The following table describes the parameters on the **Routing** tab of the **Workgroups** page.

Table 101: Route Points Page: List Pane

Column Name	Description
Name	Name of the pickup group.
Extension	Extension number for the pickup group.
On-Hours	The current On-Hours schedule used for the route point.
Holiday	The current Holiday schedule used for the route point.
Custom	The current Custom schedule used for the route point.

13.10.3.3 Voice Mail Tab

Voice mail information for new and existing routing points is provided on the **Voice Mail** tab on the **Routing Points** page. This tab contains the **Mailbox** and **Escalation Profiles** subtabs.

13.10.3.3.1 Mailbox Subtab

The following table describes the parameters on the **Voice Mail** tab and **Mailbox** subtab of the **Route Points Details** pane.

Table 102: Route Points Page: Voice Mail Tab, Mailbox Subtab

Parameter	Description
Accept broadcast messages	Select this check box to allow the user to receive broadcast messages. This is enabled by default.
Email address	Indicates the user's email address, which was configured on the **General** tab of the **Users** page.
Delivery type	Specifies whether and how voice mail messages are sent through email. Select one of the following options: • **Disabled:** Voice mail messages are not sent. • **Email text only:** The system sends an email message that notifies the user of the time, duration, and caller ID for the message that was recorded. • **Attach WAV file:** The system attaches the voice mail message to an email message as a WAV file .
Mark message as heard	Select this check box to have the system mark emailed messages as heard.
Send email warning when mailbox is full	Select this check box to have the system send users a notice informing them that their mailbox is almost full.
Automatic message forwarding	
Destination	Specifies the destination for forwarded voice mail messages. Select one of the following options: • **None:** Voice mail messages are not forwarded. • **Mailbox:** Specify the target mailbox for forwarded messages. • **AMIS Mailbox:** Specify the target AMIS mailbox for forwarded messages.

Parameter	Description
Delete message after forwarding	Select this check box to automatically delete each message after it is forwarded. This option is disabled by default, meaning messages are not deleted after forwarding.

13.10.3.3.2 Escalation Profiles Subtab

The following table describes the parameters on the **Voice Mail** tab and **Escalation Profiles** subtab of the **Route Points Details** pane.

Table 103: Route Points Page: Voice Mail Tab, Escalation Profiles Subtab

Parameter	Description
Escalation notification options	Select one of the following options: • **Escalate for each message** - to begin escalation notification each time a new voice mail message arrives in the voice mailbox. If several messages arrive within a short period of time, users who are notified will receive multiple notifications. • **Escalate for first unheard message** - to begin escalation notification only when the first unheard voice mail message arrives in the voice mailbox. Subsequent unheard messages do not trigger another wave of notifications as long as the first message remains unheard.
Profile subtabs	
Profile name	Specifies the name of the escalation profile.

Parameter	Description
Repeat count	Specifies the number of times the system loops through the 10 steps of this profile before it stops trying to contact the various notification members. Select 0 to execute the escalation profile steps once without repeating. Select one to execute the steps of the profile twice — the initial execution and one repetition. **Note**: This parameter does not apply if you select one of the Notification by email options.
Step subtabs	There is a subtab for each step in a profile; there are a maximum of 10 steps for each escalation profile.
Timeout	Specifies the amount of time, in minutes, that elapses before the next step in the profile is executed. This is the amount of time a message recipient has to respond to the original voice mail before escalation occurs.
Urgent only	Select this check box to send notification only when the escalation is determined to be urgent.
Notification by email	

Parameter	Description
Deliver message as email	Select one of the following three email delivery options: • **Disabled** - to not send email notification. • **Email text only** - to send a text email to the designated user's email inbox. The email message contains basic information about the voice mail message, such as the time, duration, and Caller ID of the message that was recorded. • **Attach WAV file** - to send an email containing a copy of the recorded voice mail message to the designated user's email inbox. The recipient can play the message on his or her PC.
Email address	Specifies the email address to send notification to.
Notification by phone	
Voice mail notification method	Select one of the following phone notification methods: • **Pager** • **Phone** • **None**
Notification number	Specifies the phone or pager number to send notification to.
Pager ID	Specifies the pager pin number required to access the recipient.
Pager data	Specifies the code the recipient requires to indicate that a page is waiting.

13.10.3.4 DNIS Tab

The following table describes the parameters on the **DNIS** tab on the **Route Points** page.

Table 104: Route Points Page: DNISTab

Parameter	Description
Add	To associate the route point with a DNIS, click **Add** and provide details for the DNIS mapping in the displayed fields.
Trunk group name	From the drop-down list, select the trunk group for the DNIS mapping.
Digits	Enter the DNIS number.
Description	Provide a description for the DNIS number. This description is seen by call recipients and in call detail reports (CDRs). The description length can be up to 26 characters.
Music on Hold	From the drop-down list, select a file-based MOH resource.
Remove	If you want to remove a DNIS system that is configured for this route point, click **Remove**.

13.10.4 Bulk Editing Route Points

You can use the Bulk Edit feature to change the server for multiple route points at the same time.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Route Points**. The **Route Points** page is displayed.
3. In the **List** pane, select the check box for each route point you want to include in the bulk edit.
4. Click **Bulk Edit**. The **Bulk Edit** tab in the **Details** pane displays the Server parameter for editing.
5. Select the **Include in change** check box.
6. In the **Server** list, select the server to provide route point services for third-party applications for all selected route points.
7. Click **Save**.

8. Click the **Results** tab to check the status of the bulk edit operation.

13.11 Configuring Call Control Options

This section explains how to configure the Call Control Options.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Options**. The **Call Control Options** page opens.
3. Review the parameters in all areas of the page, and specify values as appropriate. For more information about all of the call control options parameters Call Control Options Parameters on page 427.
4. Click **Save**.

13.11.1 Call Control Options Parameters

You configure call control options in the following areas of the Call Control Options page:

- General Area
- SIP Area
- Voice Encoding and Quality of Service Area
- Call Control Quality of Service Area
- Video Quality of Service Area
- Trunk-to-Trunk Transfer and Tandem Trunks Area

13.11.1.1 General Area

Table 105: Call Control Options Page: General Area

Column Name	Description
Use Distributed Routing Service for call routing	Select this check box to enable Distributed Routing Service. See Distributed Routing Service on page 437 for more information. **Note**: Once a change to this setting is saved, all voice switches will be rebooted and select services on application servers and Collaboration service appliances will be restarted.
Enable monitor/record warning tone	Select this check box to play a tone whenever a two-way Make Me Conference call starts being monitored or recorded. You also can select this check box to play a tone for any recorded call. To allow silent monitoring and recording, clear this check box. See Silent Monitoring and Recording on page 437 for more information. **Note**: When a user transitions between Silent Coach and silent monitor, the warning tones start/stop based on the silent coach or silent monitor warning tone setting.

Column Name	Description
Enable Silent Coach warning one	Select this check box to play a tone whenever Silent Coach is initiated. This setting applies to all Silent Coach sessions on the system. When a user transitions between Silent Coach and silent monitor, the warning tones start/stop based on the silent coach or silent monitor warning tone setting.
Enable My Hold LED indication	Select this check box to increase the LED indicator blink speed for calls placed on hold by a particular phone. When enabled, this feature modifies the blink rate of calls that were placed on hold. The LED indicator for calls placed on hold by a particular phone will blink twice as fast on that phone as for calls that have been placed on hold by other phones. This allows users to easily differentiate the call they placed on hold from calls that other users have placed on hold.
Enable My Hold reminder rings	Select this check box to play a hold reminder tone only on the phone that placed the call on hold. When this feature is not enabled, all phones play the reminder tone for calls placed on hold.
Enable BCA caller ID	Select this check box to send the BCA name and extension as the caller ID information for internal calls from a BCA. When this feature is not enabled, the name and number of the user that placed the call is sent as the caller ID information. **Note**: If the BCA or user extension is a private extension, no caller ID information is sent.

Column Name	Description
Generate an event when a trunk is in-use for	Select this check box to generate an event log when a trunk has been in use for a specified time period. The **minutes** field specifies the period of time in minutes.
Park timeout after	Select this check box to enable timeout for parked calls. The **seconds** field specifies the period of time, in seconds, that a call can remain parked before the call returns to the party that parked the call.
Hang up Make Me conference after silence for	Select this check box to enable timeout for a Make Me Conference. The minutes field specifies the period of time, in minutes, that a Make Me Conference call can be silent before the system ends the call. **Note**: This feature only applies when all parties on the call are on Analog Loop Start trunks.
Overhead paging timeout	Select this check box to enable timeout for paging calls. The **seconds** field specifies the period of time, in seconds, that a paging call remains active before the call is automatically disconnected. This prevents paging calls from getting stuck in an active state due to an incomplete hang up.
Delay before sending DTMF to fax server	Specifies the period of time, in milliseconds, to delay before sending DTMF information to the fax server. See the fax server documentation to obtain the fax server delay parameters.

Column Name	Description
DTMF/RFC-2833 payload type	Specifies the DTMF payload type. The default is 102. It can be configured to a value (96-127) that allows for more precise matching to the requirements of a specific SIP provider. After it is configured, this value is propagated to the entire MiVoice Connect system (switches, servers, and softphones) during SIP negotiation. Conference bridges and all 3rd party SIP devices require manual configuration of the Payload Type by the system administrator based on that device. After manual configuration is complete, the device must be restarted. The ShorePhone IP 8000 conference phone always uses the DTMF payload type as 101 even if the Connect Director setting is different. For inbound calls to the IP 8000 phone, the phone honors the requested payload type from the inbound endpoint. **Note**: No restart is required for Switches and Servers. Non-Mitel devices require manual configuration of this value according to the OEM instructions for those devices.

13.11.1.2 SIP Area

Table 106: Call Control Options Page: SIP Area

Column Name	Description
Realm	Specifies the name of the protected area (realm) to which the SIP authentication parameters are applied. For digest authentication, each domain of this type defines a set of user names and passwords that the system uses for granting access.
Enable session timer	Select this check box to enable the session timer. The session timer controls the interval at which SIP devices transmit or receive a RE-INVITE or UPDATE method to refresh the current session.

Column Name	Description
Session interval	Specifies the interval, in seconds, at which keepalive heartbeats are broadcast. The heartbeat is sent out at the specified period and if no response is received, the session is dropped. See RFC 4028 for more information about this parameter. **Note**: The default of 1800 seconds usually is best for most Mitel installations.
Refresher	Specifies whether the session timer is applied to the caller or called party. Select one of the following options: • **None** - to specify no preference • **Caller (UAC)** - to specify the caller • **Caller (UAS)** - to specify the called party See RFC 4028 for more information about this parameter. **Note**: The method is either RE-INVITE or UPDATE. The method is dynamically selected, based on the methods advertised by the supported header.

13.11.2 Voice Encoding and Quality of Service Area

Table 107: Call Control Options Page: Voice Encoding and Quality of Service Area

Column Name	Description
Maximum inter-site jitter buffer	Specifies the maximum jitter buffer. A larger jitter buffer might result in more delay between calling parties, which might degrade the quality of service.
DiffServ/ToS byte	Specifies the DiffServ/ToS for voicemail, workgroup, account code collection (ACC), and contact center calls.Value must be a decimal number. This parameter applies to all Mitel servers in a MiVoice Connect system. To enable a new DiffServ/ToS setting, you must reboot all Mitel servers.
Media encryption	Specifies the encryption method used by Mitel to protect payload packets. For more information, see Configuring Media Encryption on page 456.
Admission control algorithm assumes RTP header compression is being used	Select this check box to enable the admission control algorithm to assume RTP header compression is being used.
Remote IP phone codec list	Specifies the codec list to use for remote IP phones. For more information about codecs and codec lists, see Codec Negotiation and Bandwidth Management on page 438.

Column Name	Description
Always Use Port 5004 for RTP	Select this check box to always use port 5004 for RTP. **Note**: • This option is not available on systems that use SIP extensions or SIP trunks. • RTP dynamically selects a UDP port per media stream from the range of configured ports. Configure your firewall to allow RTP traffic as needed. All IP Phones and switches must be rebooted for settings to take effect. Failure to reboot may result in one way media.

13.11.2.1 Call Control Quality of Service Area

Table 108: Call Control Options Page: Call Control Quality of Service Area

Column Name	Description
DiffServ/ToS byte	Specifies the DiffServ/ToS for call control traffic from/to switches, servers, and phones. Value must be a decimal number and should not be greater than the Voice Encoding and Quality of Service DiffServ/TOS Byte value. The default value is 96. This parameter applies to all servers in a MiVoice Connect system. **Note**: • This parameter does not impact call control signaling traffic from Connect client residing on the data network or from third party TSP installations. This traffic is usually configured to reset all data traffic to DSCP of zero. • For 400-Series phones, the DSCP value is automatically updated when the value of this parameter is changed in Connect Director. For 6900-Series phones, after changing the value in Connect Director, the phone must be rebooted for the value to be updated.

13.11.2.2 Video Quality of Service Area

Table 109: Call Control Options Page: Video Quality of Service Area

Column Name	Description
DiffServ/ToS byte	Specifies the DiffServ/ToS field in the IP Packet Header of the Video Call payload packet. Value must be a decimal number. Changing this setting does not affect active video sessions; the updated value is applied to all new video sessions. Connect client does not need to be restarted to enable a change to this parameter.

13.11.2.3 Trunk-to-Trunk Transfer and Tandem Trunks Area

Trunk-to-trunk transfer and tandem trunks parameters apply only when the Class of Service allows trunk-to-trunk transfers. For more information about enabling trunk-to-trunk transfers, see Configuring a COS for Telephony Features Permissions on page 461.

Users with trunk-to-trunk transfer permission might accidentally initiate a trunk-to-trunk transfer without realizing it. This can lead to “hung” trunks, resulting in the inability to make outbound calls or receive inbound calls.

You can use trunk-to-trunk transfer and tandem trunks parameters to eliminate unwanted trunk-to-trunk transfers while ensuring that valid trunk-to-trunk transfers are not dropped.

Table 110: Call Control Options Page: Trunk-to-Trunk Transfer and Tandem Trunks Area

Column Name	Description
Hang up after silence of	Select this check box to enable timeout for a silent trunk-to-trunk transfer. The **minutes** field specifies the period of time, in minutes, that both parties of a trunk-to-trunk transfer can be silent before the system ends the call.

Column Name	Description
Hang up after	Select this check box to enable timeout for a trunk-to-trunk transfer. The **minutes** field specifies the period of time, in minutes, that a trunk-to-trunk transfer can be active before the system ends the call. This parameter should be set only if truly needed and be set for a long period.

13.11.3 Silent Monitoring and Recording

Silent monitoring and recording allows operators and supervisors to hide the fact that they are monitoring or recording calls by not playing a warning tone when the call starts being monitored or recorded. This can be desirable in certain situations, such as when a supervisor needs to monitor the telephone manners of an employee.

When monitoring or recording is silent or hidden, Connect client offers no visual or audible indication that the call is being monitored or recorded.

Note:

Mitel does not warrant or represent that your use of call monitoring or recording features of the Software will be in compliance with local, state, federal or international laws that you may be subject to. Mitel is not responsible for ensuring your compliance with all applicable laws.

Before disabling the warning tone, it is recommended that you consult with the legal counsel regarding your intended use.

13.11.4 Distributed Routing Service

Distributed Routing Service (DRS) allows a large system to scale beyond 100 switches to up to a total of 500 switches (including softswitches). DRS is optional on systems up to 100 switches, but must be enabled on systems with 101 or more switches.

When DRS is disabled, switches in a system build an internal routing database from the peer-to-peer communication with other switches. Each switch contains routing information for all endpoints in the system, including information regarding trunk selection for outbound calls. When calls are placed from any extension, each switch is able to route the call to the correct switch based on its internal routing database.

When DRS is enabled, switches only exchange routing information with other switches at the same site, rather than exchanging routing information with every other switch in a multi-site system. Although each switch only maintains routing information within its site, each server also includes an instance of the DRS which maintains system-wide routing information. When calls are initiated, switches contact the DRS in order to find the switch or switches needed to complete the call.

In a system with more than one server, the switches may contact an alternate instance of the routing service if the primary instance is not reachable. servers have a hierarchical relationship and switches first try to contact the nearest instance of the DRS in the hierarchy. If that instance of DRS is not reachable, the instance of DRS at the parent server in the hierarchy will be contacted. If neither instance of DRS is reachable, the switch makes a best effort to route the call based on the internal routing tables built from communicating with peer switches at the same site.

13.12 Codec Negotiation and Bandwidth Management

Mitel supports a variety of codecs. Codec negotiation during voice call setup is facilitated by data structures, including codec lists and profiles.

Bandwidth management and codec negotiation tools available through Connect Director include:

- Codecs that are configurable through Connect Director
- Codec lists that are configurable through Connect Director
- Video codec support
- A Connect Director parameter that permits intersite video sessions
- A SIP codec negotiation method that complies with RFC 3264

13.12.1 Codec Negotiation

Mitel supports simultaneous audio, video, and data codec negotiations to facilitate multimedia sessions between SIP endpoints (as defined by RFC 3264). Codecs specified in the Supported Codecs list are offered during session parameter negotiations.

The Mitel negotiation process that supports RFC 3264 is as follows:

1. The calling device sends the list of codecs it supports to the switch servicing the call.

2. The switch that controls the calling device compiles a codec list. The codec list contains all codecs contained in the following:

   - The calling device's codec list
   - One of the site's codec lists – intersite, intrasite, or fax – depending on the call type

   Codecs on the combined list are sorted as specified by the selected site codec list.
3. (Intersite calls only) The switch that controls the destination device modifies the codec list by removing all codecs that are not listed on the destination site's codec list.
4. The switch controlling the destination device sends the codec list to the destination device.
5. The destination device replies by sending a list of one or more codecs to the originating device. This list typically includes the highest priority codec from the received codec list that it can support.
6. The two devices begin sending RTP streams using the highest priority codec listed in the destination device's reply.

13.12.2 Configuring Supported Codecs

The Supported Codecs list is a comprehensive list of all codecs available to system devices. These codecs are used when negotiating call parameters.

When Mitel is initially installed, the Supported Codecs list comprises the set of codecs provided by Mitel and available on IP phones. Although most commonly used codecs are included, administrators can add more codecs. For example, additional codecs can be added to support SIP devices that may use codecs not initially provided by Mitel.

The Supported Codecs list also indicates the bandwidth required by each codec. The bandwidth numbers are used by the MiVoice Connect system to allocate bandwidth as voice calls are initiated and terminated.

The contents of the Supported Codecs list, including the bandwidth settings, are passed to all switches in the system, where they are used for selecting codecs for individual call sessions.

13.12.2.1 Viewing Supported Codecs

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Supported Codecs**. The **Supported Codecs** page is displayed.

Note:
For descriptions of the columns on the Supported Codecs page, see Supported Codecs Page: List Pane and General Tab.

Table 111: Supported Codecs Page: List Pane and General Tab

Column Name	Description
Name	The fully qualified codec ID string of the codec. Mitel uses this string to specify codecs while negotiating with other calling devices. **Note**: The codec ID string consists of the name and sampling rate of the codec. Although the codec name usually reflects the name by which the codec is commonly known, PCMA specifies a G.711 codec (A-law) and PCMU specifies a G.711 codec (μ-law).
Bandwidth	The bandwidth required by the codec. Mitel uses this figure when allocating bandwidth resources.
Default	Indicates whether or not the codec is a default codec. See Default Codec Lists on page 442for more information about default codecs.

13.12.2.2 Adding or Editing Supported Codecs

Note:

The default codecs supplied with the MiVoice Connect system cannot be edited or deleted.

1. Launch Connect Director.

2. Select **Administration** > **Features** > **Call Control** > **Supported Codecs**. The **Supported Codecs** page is displayed.
3. Do one of the following:

   - To edit an existing codec, click the name of the codec in the **List** pane.
   - To create a copy of an existing codec, click **Copy**.
   - To create a new codec, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing codec.
4. In the **Name** field, enter the fully qualified codec ID string.

Note:
This parameter must be entered exactly as expected by devices that negotiate call parameters.

5. In the **Bandwidth** field, enter the bandwidth required by the codec.

Note:
Use care when entering the bandwidth for a codec. Entering an incorrect value in this field compromises Mitel's ability to manage bandwidth resources.

6. Click **Save**.

13.12.2.3 Deleting Supported Codecs

Note:

The default codecs supplied with the MiVoice Connect system cannot be edited or deleted.

1. Launch Connect Director.
2. Select **Administration** > **Features** > **Call Control** > **Supported Codecs**. The **Supported Codecs** page is displayed.
3. In the **List** pane, select the check box next to each codec you want to delete.
4. Click **Delete**.
5. Click **OK** to confirm.

13.12.3 Configuring Codec Lists

Each Codec list includes a subset of the codecs supported by the MiVoice Connect system.

Codec lists are referenced by sites within a MiVoice Connect system to designate the codecs used for intersite and intrasite voice calls. The Codec Lists page displays all Codec Lists configured in the system. Mitel provides a group of default codec lists. You can also define additional codec lists through Connect Director.

13.12.3.1 Default Codec Lists

Mitel provides default codec lists; these default codec lists cannot be deleted or modified.

The default codec lists provided with the MiVoice Connect system are listed in the table below. The codecs within each list are in priority order.

Table 112: Default Codec Lists

Codec List Name	Codecs Included in List
Fax Codecs — High Bandwidth	T.38 L16/8000 PCMU/8000 PCMA/8000
Fax Codecs — High Bandwidth Passthrough	L16/8000 PCMU/8000 PCMA/8000
Fax Codecs — Low Bandwidth	T.38 PCMU/8000 L16/8000 PCMA/8000

Codec List Name	Codecs Included in List
Fax Codecs — Low Bandwidth Passthrough	PCMU/8000 L16/8000 PCMA/8000
High Bandwidth Codecs	G722/8000 BV32/16000 L16/8000 PCMU/8000 DVI4/8000 iLBC/8000 BV16/8000 G729/8000 PCMA/8000
Low Bandwidth Codecs	BV32/16000 DVI4/8000 iLBC/8000 BV16/8000 G729/8000 PCMU/8000 PCMA/8000

Codec List Name	Codecs Included in List
Medium Bandwidth Codecs	G722/8000 BV32/16000 PCMU/8000 DVI4/8000 iLBC/8000 BV16/8000 G729/8000 PCMA/8000
Very High Bandwidth Codecs	L16/16000 G722/8000 BV32/16000 L16/8000 PCMU/8000 DVI4/8000 iLBC/8000 BV16/8000 G729/8000 PCMA/8000
Very Low Bandwidth Codecs	iLBC/8000 G729/8000 PCMU/8000 PCMA/8000

Note:

The 400-Series and 6900-Series (6910, 6920, 6930, and 6940) IP phones do not support the following codecs:

- BV16/8000
- BV32/16000
- DVI4/8000

13.12.3.2 Viewing Codec Lists

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Codec Lists**. The **Codec Lists** page is displayed.

Note:
For descriptions of the columns on the Codec Lists page, see Codec Lists Page: List Pane

The Codec Lists the following table.

Table 113: Codec Lists Page: List Pane

Column Name	Description
Description	Description of the codec list.
Default	Indicates whether or not the codec list is a default codec list. See Default Codec Lists on page 442 for more information about default codec lists.

13.12.3.3 Adding or Editing a Codec List

Note:

The default codec lists supplied with the MiVoice Connect system cannot be edited or deleted.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Codec Lists**. The **Codec Lists** page is displayed.
3. Do one of the following:
   - To edit an existing codec list, click the name of the codec list in the **List** pane.
   - To create a copy of an existing codec list, click **Copy**.
   - To create a new codec list, click **New**. The **General** tab in the **Details** pane displays parameters for the new or existing codec list.
4. To edit the codec list description, type a new description in the **Description** field.
5. To add a codec to the codec list, select the codec in the **Available** list and click the right arrow button to move the codec to the **Selected** list.
6. To remove a codec from the codec list, select the codec in the **Selected** list and click the left arrow button to move the codec to the **Available** list.
7. To change the location of a codec in the codec list, select the codec to move in the Selected list and then do one of the following:
   - Click the up arrow button to move the codec up in the list.
   - Click the down arrow button to move the codec down in the list.
8. Click **Save**.

13.12.3.4 Deleting a Codec List

Note:

The default codec lists supplied with the MiVoice Connect system cannot be edited or deleted.

1. Launch Connect Director.
2. Select **Administration** > **Features** > **Call Control** > **Codec Lists**. The **Codec Lists** page is displayed.

3. In the **List** pane, select the check box next to each codec list you want to delete.
4. Click **Delete**.
5. Click **OK** to confirm.

13.13 Enabling Intersite Video

Intersite video refers to video communication between more than one Mitel site. The trunk protocol that supports video communication is SIP. Intersite video is enabled through Telephony COS settings. For information on the Telephony COS settings, see Configuring a COS for Telephony Features Permissions on page 461.

Mitel does not allocate bandwidth for video calls. Consequently, heavy traffic on the network can have an impact on video conferences and even audio communication.

To enable intersite video:

1. Launch Connect Director.
2. Click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**. The **Telephony Features Permissions** page is displayed.
3. Do one of the following:

   - To edit an existing set of telephony features, click the name of one of the preconfigured COS profiles (Fully Featured, Minimally Featured, or Partially Featured).
   - To create a new class of service for telephony features, click **New**.

   Note:
   In the **Details** pane, the **Telephony Features Permissions** page for the new or existing class of service displays.

4. Do one of the following:

   - To allow users with the selected COS to participate in video calls, select the **Allow intersite video calls** check box.
   - To prevent users with the selected COS from participating in video calls, clear the **Allow intersite video calls** check box.

13.14 Configuring Automatic Ringdown Circuits

An automatic ringdown circuit is comprised of predefined devices at the circuit endpoints.

Automatic ringdowns are activated on IP Phones by pushing a programmed IP Phone Call Appearance button or lifting a handset on a dedicated ringdown device. These actions cause the recipient device to continuously ring until the call is answered or the calling party ends the call. Automatic ringdown is only supported on phones; Connect client does not support automatic ringdown.

Note:

To force a device to ring until it is answered, the call stack depth for Bridge Call Appearances supporting ringdown should be set to 1 and availability state transfers should be disabled by selecting **No Answer**.

Mitel supports the following ringdown methods:

- **Dedicated Circuit Ringdown :** Ringdown is immediately initiated when a programmed Call Appearance button is pushed or a specified device goes off hook. The ringdown call is answered on the recipient device by pressing the corresponding Call Appearance button or taking the device off hook.
- **Delayed Ringdown Circuit:** Ringdown is initiated when the initiating phone is taken off-hook and a specified amount of time passes with no action by the user. This option is only available for IP phones that provide a dial tone.

13.14.1 Configuring Dedicated Circuit Ringdown

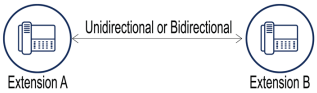
IP Phones with call appearance buttons and the Button Box support dedicated circuit ringdown. A call appearance button is programmed for Ringdown by configuring it as a Bridged Call Appearance and selecting a Ringdown option. When using IP Phones as both calling and receiving devices, an IP Phone button on both device must be configured for Ringdown. Mitel also supports external devices as ringdown recipients.

A ringdown call is initiated by pressing the ringdown button on a calling device. The ringdown button on the recipient device blinks; the recipient device can be configured to ring or remain silent on an inbound ringdown call. The ringdown call is answered on the recipient phone either by lifting the handset or pressing the blinking ringdown button. If the phone is configured to remain silent when a ringdown call is incoming, the blinking button must be pressed to answer the call.

13.14.1.1 Configuring One-to-One Ringdown

Basic one-to-one ringdown, as depicted in the following figure, is enabled by configuring a Call Appearance button on each phone as a Bridged Call Appearance (BCA). During an incoming ringdown call, the BCA button on the recipient device blinks.

Figure 11: One-to-One Ringdown Operation



Mitel supports unidirectional or bidirectional one-to-one ringdown.

- When phones are configured for unidirectional ringdown, one phone is defined as the recipient device; pressing the ringdown button on that device will not initiate a call to the phone on the other end of the circuit.
- When phones are configured for bidirectional ringdown, pressing the ringdown button on either device initiates a call to the device on the other end of the circuit.

13.14.1.1.1 Configuring a Unidirectional One-to-One Ringdown Circuit

Unidirectional ringdown circuits require two Bridged Call Appearances – one for the calling device and one for the recipient device.

1. Create two Bridged Call Appearances.

Note:

For details on how to create a BCA, see Adding or Editing a Bridged Call Appearance on page 361.

2. For the user that will initiate ringdown calls, do the following:

   a. Program an IP phone button on the calling device for one of the BCA extensions.
   b. When configuring the IP phone button, select **Dial extension** under **No connected call action**.

Note:

For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

3. For the user that will receive ringdown calls, do the following:

   a. Program an IP phone button on the receiving device for the remaining BCA extension.
   b. When configuring the IP phone button, select **Dial tone** under **No connected call action**.

> **Note**:
>
> For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

13.14.1.1.2 Configuring a Bidirectional One-to-One Ringdown Circuit

Bidirectional ringdown circuits require two Bridged Call Appearances – one for the calling device and one for each recipient device.

1. Create two Bridged Call Appearances.

   For details on how to create a BCA, see Adding or Editing a Bridged Call Appearance on page 361.
2. For the first user that will initiate and receive ringdown calls, do the following:

   a. Program an IP phone button on the calling device for the first BCA extension.
   b. When configuring the IP phone button, select **Dial tone** under **No connected call action** and then type the extension number of the second BCA in the **Dial extension** field.

> **Note**:
>
> For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

3. For the second user that will initiate and receive ringdown calls, do the following:

   a. Program an IP phone button on the calling device for the second BCA extension.
   b. When configuring the IP phone button, select **Dial tone** under **No connected call action** and then type the extension number of the first BCA in the **Dial extension** field.

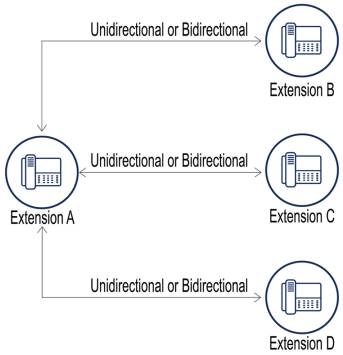
Note:

For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

13.14.1.2 Configuring One-to-Many Ringdown

Mitel supports one-to-many ringdown circuits. When the Ringdown BCA button is pressed on the calling device, Extension A in the following figure, the corresponding button on all recipient devices programmed to receive the ringdown call flashes green. When the call is answered on one of the recipient devices, the Ringdown button on the other recipient devices turns red. If the answering device places the call on hold, the call is parked to the BCA and is again available for all recipient devices. If a conference call involving a ringdown number is placed on hold, the call is not parked on the BCA.

Figure 12: One-to-Many Ringdown Operation



Mitel supports biderectional ringdown for the one-to-many configuration. When a ringdown call is placed from a recipient device (Extension B in the above figure), the ringdown BCA buttons on the other recipient devices (Extensions C and D) become solid red when Extension A answers the call, indicating that the line is busy. Pressing these red buttons has no effect. If Extension A does not answer the ringdown call, the phone rings until the caller on Extension B hangs up or the call routing for Extension A handles the call.

13.14.1.2.1 Configuring a One-to-Many Ringdown Circuit

The process for creating a one-to-many ringdown circuit is similar to creating a unidirectional one-to-one ringdown circuit. However, an IP phone button must be configured for each recipient device.

1. Create two Bridged Call Appearances.

> **Note**:
>
> For details on how to create a BCA, see Adding or Editing a Bridged Call Appearance on page 361.

2. For the user that will initiate ringdown calls, do the following:

   a. Program an IP phone button on the calling device for one of the BCA extensions.
   b. When configuring the IP phone button, select **Dial extension** under **No connected call action**.

> **Note**:
>
> For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

3. For each user that will receive ringdown calls, do the following:

   a. Program an IP phone button on the receiving device for the remaining BCA extension.
   b. When configuring the IP phone button, select **Dial tone** under **No connected call action**.

Note:

For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

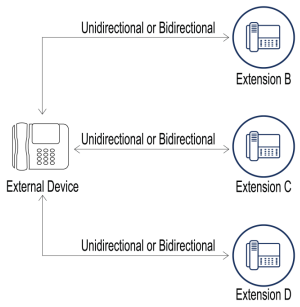
13.14.1.3 Configuring Ringdown to an External Device

Ringdown to an external device is supported by programming the ringdown button to access a trunk group that has a unique trunk access code and contains only one trunk. When the user presses the ringdown button, that trunk is accessed.

To place a call over a ringdown circuit to an external device, the user enters the trunk access code in addition to the phone number of the device. For instance, when an analog trunk group is configured to service the ringdown call, the default trunk access code of 9 must be dialed to place a ringdown call.

This trunk is not required to be reserved solely as the ringdown circuit. Any user can dial this trunk access code to select this trunk. If the trunk is busy, pressing the ringdown button generates a busy signal. “Enable availability state” only applies for an incoming call. It is not applicable for an outbound call.To enable ringdown buttons on the Mitel devices (Extensions B, C and D in the following figure), the BCA extension must be configured on the Trunk Groups page.

Figure 13: Ringdown to an External Device



13.14.1.3.1 Configuring a Ringdown Circuit with an External Endpoint

The process for creating a ringdown circuit to an external endpoint differs from the procedure for circuits with internal endpoint as follows:

- The external number must be accessed through a specific trunk that is configured as the only trunk within a trunk group.
- The number of the recipient device includes the Trunk Access Code of the specified trunk group.

1. Create a Bridged Call Appearance.

> **Note**:
>
> For details on how to create a BCA, see Adding or Editing a Bridged Call Appearance on page 361.

2. For the user that will initiate ringdown calls, do the following:

   a. Program an IP phone button on the calling device for the BCA extension.
   b. When configuring the IP phone button, select **Dial external** under **No connected call action** and then type the desired telephone number in the field.

> **Note**:
>
> For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.

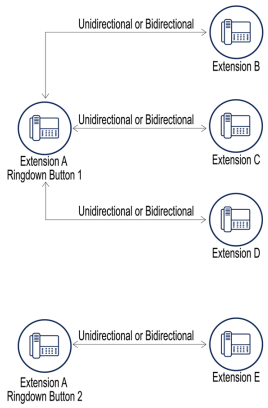
13.14.1.4 Configuring Multiple Ring Down Buttons

IP Phones with sufficient call appearance buttons support multiple ringdown circuits. In the following figure, Extension A is configured to support two ringdown circuits:

- One ringdown circuit with Extensions B, C, and D at the other end.
- One ringdown circuit with Extension E at the other end.

This configuration requires four Bridge Call Appearance extensions: two BCA extensions for Extension A; one BCA extension shared by Extensions B, C, and D; and one BCA extension for Extension E.

Figure 14: Multiple Ringdown Buttons



13.14.2 Configuring Phone Delayed Ringdown

Mitel permits IP phones that provide a dial tone to perform ringdowns by taking the handset off hook. If a number is not dialed within a specified period after taking the phone off hook, a ringdown call is directed to the predefined recipient device.

Analog phones to which a user extension is assigned can receive incoming calls even when configured for delayed ringdown calls. When an anonymous user is assigned to the port, the device cannot receive incoming calls if it is configured to make delayed ringdown calls.

13.14.2.1 Configuring a Delayed Ringdown Circuit

A unidirectional delayed ringdown circuit requires one Bridged Call Appearance that is assigned to the recipient end of the circuit.

1. Create a Bridged Call Appearance.

Note:

For details on how to create a BCA, see Adding or Editing a Bridged Call Appearance on page 361.

2. For the user that will initiate ringdown calls, do the following:

   a. Launch Connect Director.
   b. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
   c. In the **Details** pane for the selected user, select the **Telephony** tab.
   d. Select the **Enable delayed ringdown** check box.
   e. In the **Ringdown number** field, type the BCA extension or the external number to use as the ringdown endpoint.
   f. In the **Ringdown delay** field, type the number of seconds that you want the system to wait for the receiver to respond before dialing the ringdown number.

Note:
The delay period is the time between when the handset is lifted and when the ringdown call is initiated.

3. For each user that will receive ringdown calls, do the following:

   a. Program an IP phone button on the receiving device for the remaining BCA extension.
   b. When configuring the IP phone button, select **Dial tone** under **No connected call action**.

Note:

- For complete details on how to program an IP phone button for a BCA extension, see Configuring an IP Phone Button for a BCA Extension on page 368.
- This step is not required if the endpoint of the ringdown circuit is an external number.

13.15 Configuring Media Encryption

Mitel encrypts RTP (payload) packets within the Mitel network. Call control packets are encrypted on IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones. Call control packets are not encrypted on the earlier IP phones.

To configure media encryption:

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Call Control** > **Options**. The **Call Control Options** page is displayed.
3. Under **Voice encoding and quality of service**, in the **Media encryption** drop-down list, select **SRTP - 128 bit AES**.
4. Click **Save**.

13.15.1 System Support

Encryption is enabled or disabled through Connect Director on a system basis only and cannot be enabled for individual devices or selected calls. End users have no control over which calls are encrypted. Changing the system encryption setting does not alter calls that are in progress; unencrypted calls in progress when encryption is enabled remain unencrypted until the calls are terminated.

System administrators enable encryption and select an encryption algorithm through Connect Director. The following encryption options are available:

- None
- SRTP - 128 bit AES

SRTP with AES and authentication has a significant impact on the system load when a large number of media channels are encrypted.

SRTP-AES encryption is available on MiVoice Connect and ST9 and later systems. A license is not required.

13.15.2 Supported Platforms

Switches and Codecs

Encryption is supported by the following voice switches:

- All voicemail-enabled switches
- All 1-U Half Width switches
- All 1-U Full Width switches

Switches do not support SRTP with linear (LRNB/8000) or wide-band (LRWB/16000) codecs. When SRTP is enabled, codec negotiation excludes these codecs.

Switches support a maximum of 36 encrypted media streams. This limitation potentially impacts switches that provide SGT1 or SGE1 channels with high three-way conference call traffic.

Each channel in a three-way conference requires two media stream encryption resources, limiting switches to 18 encrypted channels for three-way conferences. In this scenario, all remaining trunks provided by the switch are blocked while 18 channels are engaged in three-way conference calls. Switches can service any combination of two-way (one encrypted media stream) and three-way (two encrypted media streams) calls that do not exceed 36 media streams. Analog ports on the SG220T1A are included in this limitation.

13.15.2.1 Phones and Applications

Encryption is supported for all IP phones that run on a Mitel network. SoftPhone, which is available through Connect client, does not support encryption.

When Media Encryption is enabled in Connect Director, whether or not media encryption is in effect for a particular call depends on the type of phones involved in the call, as follows:

- All calls that involve only 400-Series IP phones and 6900-Series (6910, 6920, 6930, and 6940) phones are encrypted.
- All calls that involve only older IP phones (MGCP phones) are encrypted.
- All calls that involve both 400-Series IP phones and 6900-Series (6910, 6920, 6930, and 6940) phones and earlier phones are not encrypted. However, if all callers using one type of phone drop out of a mixed-phone conference call, leaving only callers with the same type of phone in the call, the call is encrypted from then on.

Connect client and IP phones (except for IP110 and IP115 phones) display a padlock icon for each call with active SRTP encryption. The padlock icon is also displayed in the Call History list to indicate encrypted calls. The padlock icon indicates the call is secure on the Mitel network; Mitel cannot guarantee call security outside of the network, for example, for calls that terminate across an analog or digital trunk.

Mitel service appliances support SRTP-AES encryption. For some other Mitel products, the following distinctions might be important to keep in mind:

- If the Headquarters server is hosting voicemail and Auto-Attendant, it does not encrypt the media stream by using SRTP-AES encryption.
- If the voicemail-capable switches (such as the Voice Switch 90V) are hosting voicemail and Auto-Attendant, the switch encrypts the media stream.
- The IP 8000 Conference Phone does not support SRTP-AES encryption.

Phones that do not support SRTP cannot perform barge in, whisper, or silent monitor functions on calls that are using SRTP encryption. When added to a call using SRTP, new parties using devices that do not support SRTP exchange unencrypted media

streams. SRTP does not address user registration, call setup, or signaling-related security.

Configuring Users 14

This chapter contains the following sections:

This chapter describes how to create a user account and configure all parameters that relate to the user.

14.1 Overview

This chapter provides information about user configuration for new Mitel installations and established MiVoice Connect systems.

14.1.1 Configuring Users in a New Mitel Installation

For a new installation, you must first configure all of the following system components in the following order:

1. Define the classes of service (COS).
2. Create the user groups.
3. Create individual user accounts.

For a new system, the following information must be available when you create new user accounts:

- A list or outline of the COSs that are appropriate for the Mitel deployment and available for assignment to user groups
- A list or outline of user groups to which individual users are assigned
- A list of new users to add to the system

Note:

A new MiVoice Connect system has sets of default COSs and user groups.

14.1.2 Configuring Users in an Established MiVoice Connect System

For established Mitel networks, you can bypass the prerequisite tasks and go directly to adding a new user or viewing existing user accounts. For more information, see Configuring a User Account on page 488.

14.2 Specifying a Class of Service

A Class of Service (COS) specifies a set of features and privileges. A user's assigned COS determines the features that user can access. Mitel defines three types of service classes: telephony features, call permissions, and voice mail permissions.

14.2.1 Configuring a COS for Telephony Features Permissions

Telephony features permissions are assigned to user groups and define how users can use their telephone features, such as call stack depth, paging, and call forwarding to an external number.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**. The **Telephony Features Permissions** page opens.
3. Do one of the following:

   - To edit an existing COS for telephony features, click the name of one of the preconfigured COS profiles (Fully Featured, Minimally Featured, or Partially Featured) in the **List** pane.
   - To create a copy of an existing COS for telephony features, click **Copy**.
   - To create a new COS for telephony features, click **New**.

Note:
The **Details** pane displays the telephony features permissions parameters for the selected the new or existing COS.

4. Specify the telephony features permissions parameters, as described in the following table.

Table 114: Telephony Features Permissions Page: General Tab

Parameter	Description
Name	A descriptive name for the class of service.
Max. call stack depth	The maximum number of simultaneous calls that can be “stacked” on a user’ extension. When this number is reached, additional inbound calls are routed to the call forward busy destination. Valid entries are 1–16.
Max. buddies per user	The number of individuals that a user with this service class can designate as contacts in Connect client. Users can monitor their contacts’ presence status. Valid entries are 1–500.
Max. private contacts	The maximum number of personal contacts in Connect client that a user with this class of service can have. Valid entries are 10– 10,000. **Note**: To enable users to upload personal contacts, you must select the **Allow upload of personal contacts to server** check box on this page.

Parameter	Description
Max. parties in Make Me conference	The maximum number of parties that can be included in any Make Me conference call made from your site. Select the number of parties from the drop-down list. The value range is 3 through 8. The maximum for ST voice switches is 8; other switch types support a maximum of 6 participants. **Note**: The maximum number of participants also depends on the switch configuration. See IP Phone, SIP, and Make Me Conference Support on page 156for more information.
Allow call pickup	Enables call pickup. Call pickup allows users to pick up any ringing extension (including the night bell) or pick up any parked call. You must also enable the **Show caller ID name and number for other extensions** option to allow users to pick up calls.

Parameter	Description
Allow trunk-to-trunk transfer	Enables trunk-to-trunk call transfers. Examples of trunk-to-trunk transfers include the following call scenarios: • An internal party is talking with an external party. The internal party transfers the external party either blindly or consultatively to an external party by using the telephone or Connect client. • During a three-party conference call that has one internal party and two external parties, the internal party drops out of the call by using the phone (its handset or buttons) or Connect client. **Note**: Trunk-to-trunk transfer does not refer to the transfer of a call from an external party to an external number by a user's availability state. (This is addressed by the **Allow external call forwarding and Find Me destinations** permission). When enabled, trunk-to-trunk transfer is automatic and bypasses toll-related call permissions. If a potential exists for toll fraud by employees who could abuse this feature, selectively limit permission to a few user groups (such as executive and sales user groups). If this parameter is enabled, you can manage the trunk-to-trunk feature in the Call Control Options page.
Allow overhead and group paging	Allows users to dial any site paging extension and make an announcement by using the overhead paging system or group paging.
Allow make hunt group busy	Allows users to perform the following actions: • Busy-out a hunt group. • Return the hunt group to service by keying ***18** on the telephone keypad. If a hunt group is busied out during a holiday or an off-hours schedule, the schedule takes precedence.

Parameter	Description
Allow extension reassignment	Allows users to reassign their extension to another telephone.
Allow PSTN failover	Allows site-to-site calls that fail over proprietary routes to be automatically rerouted over a PSTN number. You must enter the PSTN number to use in case of failure in the **PSTN failover** field on the General tab of the Users detail pane.
Show caller ID name and number for other extensions	Allows users to see incoming caller ID. The impact of this setting is system-wide; for example, it determines whether for any other user extension caller ID appears in Connect client, on phone displays, and elsewhere.
Enumerate individually held calls for unpark	Allows users to view individual calls parked on another user's call stack. A user requires this permission to specify the call to be unparked from another user's stack.
Allow customization of IP phone buttons and client monitor windows	Allows users to configure the programmable buttons on their IP phone or button box. Clear the check box to prevent users from being able to configure custom buttons. For example, this action prevents users from configuring their phones to monitor the extension of another user. (Instead, Extension Monitor and other programmed-button features would need to be set up by a system administrator.)
Show extensions with different prefixes in directory	Displays extensions that have different prefixes. Because of the On-Net Dialing feature, a remote site can have a different prefix from the Headquarters site. Selecting this check box causes all extensions (including remote extensions) to appear in the directory.
Allow collaboration features	Enables document sharing. For more information, see Configuring Private Extensions on page 547.

Parameter	Description
Allow recording of own calls	Allows a user to record a call. This function is also affected by the **Enable monitor/record warning tone** parameter on the Call Control Options page. For more information, see Configuring Call Control Options on page 427.
Allow intersite video calls	Enables users to participate in video calls with users at other Mitel sites. Intersite video traverses SIP trunks.
Allow call notes	Enables the Call Notes feature in Connect client. This feature enables users to make text notes during calls. Notes appear in the call history. **Note**: If you disable the Call Notes feature in Connect Director, existing notes remain available for users to view, but these notes cannot be edited.
Show call history	Select this check box to enable call activity tracking. Call detail records are recorded for all calls and call history is available from the phone redial and will show in the Connect client call history. Clear this check box to enable Call History Privacy. Users can place and receive calls without the calls being tracked and recorded in the call detail records. In addition, the calls will not be available from the phone redial and will not show in the Connect client call history. For more information, see Configuring Call History Privacy on page 548.
Allow upload of personal contacts to server	Enables users to upload contacts in Connect client.

Parameter	Description
Directed intercom: Allow initiation	Enables the Directed Intercom feature. For more information about configuring this feature, see Configuring Call Intervention Methods on page 575.
Directed intercom: Accept	Specifies whether users can receive intercom calls or pages. Select one of the following options: • None means that users cannot receive intercom calls or pages. • All means that users with this permission can receive intercom calls or pages from anyone with this class of service. • Only From means that users with this class of service may receive intercom calls or pages from only the person or extension specified in the associated field. For more information about configuring this feature, see Configuring Call Intervention Methods on page 575.
Whisper Paging: Allow Initiation	Enables a user to place a whisper page call. For more information about configuring this feature, see Configuring Call Intervention Methods on page 575.
Whisper Paging: Accept	Specifies whether users can receive whisper page calls. Select one of the following options: • None means the user with this COS cannot receive whisper page calls. • All means the user with this COS can receive whisper page calls from all users. • Only From means the user with this COS may receive whisper page calls only from the specified user.

Parameter	Description
Barge-in: Allow initiation	Enables users to barge in on other users' calls. **Note**: Barge-in permits one party to join an existing call as a fully conferenced participant. When barge-in is initiated, a brief intrusion tone is played to the other participants and (if present) the monitor/record warning tone is discontinued. For more information, see Configuring Availability State Delegation on page 568.
Barge-in: Accept	Specifies whether users' calls can be barged-in upon. Select one of the following options: • None means that users with this class of service may not receive barge-ins from anyone. • All means that users with this class of service may receive barge-ins from anyone else in this class of service. • Only From means that users with this class of service may receive barge-ins only from the person or extension specified in the field associated with this option.
Record other's calls: Allow initiation	Enables users within this class of service to record the calls of other system users. For example, a supervisor could record the call of an agent. For more information, see Configuring Call Intervention Methods on page 575. The Selectable Mailboxes feature allows recorded calls to be automatically placed into mailboxes other than the mailbox of the user who recorded the call. For more information, see Overview on page 284. When you record another user's call, the system plays a warning tone. To disable the tone, uncheck **Enable monitor/record warning tone** parameter on the Call Control Options page. For more information, see Configuring Call Control Options on page 427.

Parameter	Description
Record other's calls: Accept	Specifies whether users within this class of service may have their calls recorded by other users. Select one of the following options: • None means that users within this COS may not have their calls recorded by anyone. • All means that users within this COS may have their calls recorded by anyone else in this COS. • Only From means that users within this COS may have their calls recorded only by the person or extension specified.
Silent monitor/Silent coach other's calls: Allow initiation	Allows a supervisor to monitor a phone call of a user and to speak to the user without the other party hearing. For more information, see Configuring Call Intervention Methods on page 575.
Silent monitor/Silent coach other's calls: Accept	Specifies whether users within this class of service may have their calls silently monitored or silently coached by other users. Select one of the following options: • **None** means that users within this COS may not have their calls silently monitored or be silently coached during a call by any other system user. • **All** means that users within this COS may have their calls silently monitored or be silently coached during a call by any other user in this class of service. • **Only From** means that users within this COS may have their calls silently monitored or be silently coached during a call only by the person or extension specified.
Allow current availability state changes	Allows users to change their current availability state from IP phones and Connect client.
Allow current availability state detail changes	Allows users to change all availability state settings, such as call-forwarding destinations, from Connect client.

Parameter	Description
Allow external call forwarding and find me destinations	Allows users to forward incoming calls to an external number.
Allow external assignment	Select this check box to allow users to assign their extension to a PSTN phone for use with the External Assignment feature. If you select this check box, the user can use a cell phone or home phone as an extension in the Mitel network. **Note**: This option is only available when Allow external call forwarding and fine me destinations is enabled.

Parameter	Description
Allow additional phones to ring simultaneously and to move calls	Select this check box to allow users to configure one or two additional phones to ring at the same time as their main IP phone. The user can specify the phone number of additional phones in Connect client, or you can configure these numbers through Connect Director (**Administration** > **Users** > **Users** > **Routing** > **Ring Me**). After a simultaneous ringing call is established, the user can move the call between devices by using an IP phone. The user can also suspend the call forwarding function by using Connect client. **Note**: • You can configure an optional ring delay to let the user's main telephone ring a configurable number of times before the additional phones start ringing. • This option is only available when Allow external call forwarding and find me destinations is enabled.

Parameter	Description
Scope	Configures the following call permission levels for the COS: • **Local only:** Allows forwarding or extension reassignment only to local or additional local area codes, as defined on the Sites page. • **National long distance:** Allows forwarding or extension reassignment to long-distance numbers within the country, as defined on the Sites page. • **National mobile:** Allows forwarding or extension reassignment to mobile numbers. Because some countries use caller-pays mobile calling, by not selecting this option your organization can avoid incurring the associated costs of calls being sent to a mobile phone. • **International long distance:** Allows forwarding or extension reassignment to international numbers, as defined on the Sites page. • **All calls:** Allows forwarding or extension reassignment to any number, including Carrier Select, Operator Assisted, and 900 numbers. This capability is enabled by default. **Note**: These options are only available when Allow external call forwarding and find me destinations is enabled.
Restrictions	Applied to calls in addition to the Scope. Follow these rules for specifying restrictions:

Parameter	Description
Restrictions (continued)	• The comma-separated restriction expressions have a limit of 50 characters, total (including commas and semicolons). • Numbers must be entered in canonical format, including the international designation “+” and country code. For example, to restrict forwarding to the 408 area code in the U.S., use +1408. • Non-routable calls (311, 411, etc.) for a country must be designated by the country code plus the “/” character. For example, to restrict forwarding to 311 in the U.S., use 1/311. • Each field can contain multiple entries as long as they are separated by commas or semicolons. • Multiple entries must be separated by commas or semicolons and can consist only of the numerals 0–9, “x””“, “/”, or “+”. • Access codes (such as 9) must not be included. • The wildcard of “x” can be used. **Note**: • When a call is both restricted and permitted, it is permitted. For example, restricting +1 408 and permitting +1 408 331 restricts all calls to the 408 area code except those to 408 331-xxxx. • This option is only available when Allow external call forwarding and fine me destinations is enabled.

Parameter	Description
Permissions	Applied in addition to the Scope. Follow these guidelines for specifying permissions: • The comma-separated permission expressions have a limit of 50 characters, total (including commas and semicolons). • Numbers must be entered in canonical format including the international designation “+” and country code. For example, to permit forwarding to the 408331 area code and prefix in the U.S., use +1408331. • Non-routable calls (311, 411, and so on) for a country must be designated by the country code plus the “/” character. For example, to permit forwarding to 311 in the U.S., use 1/311.
Permissions (continued)	• Each field can contain multiple entries as long as they are separated by commas or semicolons. • Multiple entries must be separated by commas or semicolons and can consist only of the numerals 0–9, “x”, “/”, or “+”. • Access codes, such as 9, must not be included. • The wildcard of “x” can be used. **Note**: • When a call is both restricted and permitted, it is permitted. For example, restricting +1 408 and permitting +1 408 331 restricts all calls to the 408 area code except those to 408 331-xxxx. • This option is only available when Allow external call forwarding and fine me destinations is enabled.

14.2.2 Call Permissions

This section describes the types of call permissions the Mitel administrator can set. Call permissions are classes of service that specify the type of call users are allowed to dial. Call permissions are assigned to user groups. The parameters on the **Call Permissions** page are described in the following table.

Table 115: Call Permissions Page: General Tab

Parameter	Description
Name	Shows the descriptive name of the COS being added or edited.
Scope	Defines the following general permission levels for the COS: • **Internal only:** Allows calls only to internal extensions and to the configured emergency number. • **Local only:** Allows calls only to local or additional local area codes, as defined on the Site edit page. • **National long distance:** Allows calls to long-distance numbers within the country, as defined on the Site edit page. • **National mobile:** Allows calls to mobile numbers within the country, as defined on the Site edit page. • **International long distance:** Allows calls to international numbers, as defined on the Site edit page. • **All calls (Default):** Allows calls to any number, including 900, Operator Assisted, and Carrier Select numbers. It supports use of Vertical Service Codes.

Parameter	Description
Restrictions	Applied in addition to the Scope setting. The rules for specifying restrictions are as follows: • For this COS, the maximum number of characters in the comma-separated restriction expressions is 255. • Numbers must be entered in canonical format including the international designation “+” and country code. For example, to restrict calls to the 408 area code in the U.S., type +1408. • Non-routable calls (311, 411, and so on) for a country must be designated by the country code plus the “/” character. For example, to restrict 311 in the U.S., type 1/311. • Each field can contain multiple entries as long as they are separated by commas or semicolons. • Multiple entries must be separated by commas or semicolons and can consist only of the numerals 0–9, “x”, “/”, or “+.” • Access codes, such as 9, must not be included. • The wildcard of “x” can be used. **Note**: If a call is both restricted and permitted, it is permitted. This behavior can be used to create a filter. For example, restricting +1 408 and permitting +1 408 331 restricts all calls to the 408 area code except those to 408 331-xxxx.

Parameter	Description
Permissions	Applied in addition to the Scope setting. The rules for entering restrictions are as follows: • For this COS, the maximum number of characters in the comma-separated permission expressions is 255. • In general, numbers must be entered in canonical format including the international designation “+” and country code. For example, to permit calls to the 408331 area code and prefix in the U.S., use +1408331. • Non-routable calls (311, 411, and so on) for a country must be designated by the country code plus the “/” character. For example, to permit 311 in the U.S., use 1/311. • Each field can contain multiple entries as long as they are separated by commas or semicolons. • Multiple entries must be separated by commas or semicolons and can consist only of the numerals 0–9, “x”, “/”, or “+”. • Access codes, such as 9, must not be included. • The wildcard of “x” can be used. **Note**: If a call is both restricted and permitted, it is permitted. This behavior can be used to create a filter. For example, restricting +1 408 and permitting +1 408 331 restricts all calls to the 408 area code except those to 408 331-xxxx.

14.2.3 Voice Mail Permissions

This section describes the classes of service that you configure from the **Voice Mail Permissions** page. Voice mail permissions are assigned to user groups and provide specific capabilities in the Mitel voice mail system. The following table describes the parameters on the **Voice Mail Permissions** page.

Table 116: Voice Mail Permissions Page: General Tab

Parameter	Description
Name	Describes the name of the COS record that you are creating or editing.
Incoming message length (0 - 3600)	Specifies the maximum length of an incoming voice mail message. The default is 300 seconds.
Incoming max. messages (0 - 500)	Specifies the maximum number of messages that can be queued in a mailbox, including new and saved messages. The default is 50 seconds.
Outgoing message length (0 - 3600)	Specifies the maximum message length that a user can record before sending a message to another extension. This parameter controls both the composed message and the greeting. The default is 300 seconds. **Note**: Do not confuse this message with the user's personal voice mail greeting.

Parameter	Description
Enable voice mail callback	Enables users with this COS to call back a caller after listening to a voice mail from the caller on a telephone. **Note**: The behavior of the Call Back feature depends on the phone model: • For the 6900, 480, and 485 models, the **Call Back** softkey is displayed in the visual prompt of voice mails. To call back the caller, the user must press the **Call Back** softkey. • For the MGC Shoretel phones, the **Call Back** option is available in the audio prompt of the voicemail menu as visual voicemail is not supported in these phones. To call back the caller, the user must select the **Call Back** option from the audio prompt of voicemail menu.
Lifespan of voice mail password (30 - 365)	Enables users to set the lifespan of their voice mail password. The default is 90 days. To increase system security, Mitel recommends that you enable this feature. The password change applies to the following Dialed Number types: • User extensions • Workgroup extensions • Route point extensions • External user extension

Parameter	Description
Days in advance of password expiration before warning (1 - 30)	Specifies the number of days before a password expires that users are notified about the upcoming password expiration. The default is 7 days. **Note**: If you do not enable this warning, password expiration warning messages are not sent to the COS members.
Allow access to broadcast distribution list	Allows users to have access to the company-wide distribution list. A user with this permission can broadcast voice mail messages to all users.
Allow access to system distribution lists	Allows users to access system distribution lists.
Allow message notification	Enables message notification. The default is that this setting is enabled.
Allow message notification to external number	Enables message notification to an external number. This parameter cannot be enabled unless Allow message notification is also enabled. The default is that this setting is enabled.
Allow downloading voice messages as WAV files	Allow users to download voice messages as WAV files.
Voice mail prompt mode	Select one of the following prompt styles: • Mitel (the default) • Octel
Auto-Delete	

Parameter	Description
Delete saved / unheard messages after (7 - 2000) days	Specifies the number of days after which the system deletes saved and unheard voice messages. Valid values are 7-2000. The default is 0, which means that saved and unheard messages are not deleted.
Delete heard messages after (7 - 2000) days	Specifies the number of days after which the system deletes heard voice messages. Valid values are 7-2000. The default is 0, which means that heard messages are not deleted.
Enable auto-delete notification	Sends automatic notifications to users, by email and/or voice mail, before the system deletes their voice mail messages. The system sends warning messages two weeks prior to the deadline and then one week prior to the deadline. Notification messages can be emailed if the user's email address is specified in the user profile. **Note**: This option is available only if you enable **Delete saved/unheard messages after (7-2000) days or Delete heard messages after (7-2000) days**.

14.3 Configuring User Groups

This section describes how to create or modify a user group. The information in this section applies to a new Mitel installation or an existing system. Configuring user groups is the second major phase in the creation of user accounts in a new system.

14.3.1 Viewing User Groups

The User Groups page includes a list of default Mitel user groups.

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page opens.

Note:
For descriptions of the columns on the User Groups page, see User Groups Page: List Pane.

Table 117: User Groups Page: List Pane

Parameter	Description
Name	Name of the user group.
COS - Telephony	Telephony features permissions COS associated with the user group.
COS - Call Permissions	Call permissions COS associated with the user group.
COS - Voice Mail	Voice mail COS associated with the user group.
Voice Mail Interface	The voice mail interface associated with the user group. • **None:** Users use a standard Mitel voice mailbox. • **External Voice Mail, SMDI:** Connects to an external voice mail system using the SMDI protocol. • **Mitel Voice Mail, SMDI:** Connects to a legacy Mitel system using the SMDI protocol. • **External Voice Mail, SIP:** Connects to an external voice mail system by using the Session Initiation Protocol (SIP). • **External Voice Mail, QSIG:** Connects to an external voice mail system using the QSIG protocol.

Parameter	Description
Account codes	Indicates the account code collection mode for the user group: • None: Account codes are not enabled. • Optional: Account codes are optional. • Required: Account codes are required.
DID as CESID	Indicates whether or not the user's telephone number is sent to the service provider when a user in this user group dials an emergency services number. If this option is not enabled and **Send caller ID as caller's emergency service identification** is also not enabled, the outbound caller ID becomes the site's CESID.

14.3.2 Adding or Editing a User Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page opens.
3. Do one of the following:
   - To edit an existing user group, click the name of the user group in the **List** pane.
   - To create a copy of an existing user group, click **Copy**.
   - To create a new user group, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing user group.

4. Review the parameters on all of the tabs in the details pane, and specify values as appropriate.

Note:
For more information about all of the user group parameters on the various tabs of the details pane, see User Parameters on page 490.

5. Click **Save**.

14.3.3 User Group Parameters

A user group has many details. You configure user group parameters on the following tabs, which you can access on the details pane for a particular user group:

- General Tab on page 484
- Profile Tab on page 487

14.3.3.1 General Tab

General information about new and existing user groups is provided on the **General** tab in the **Details** pane of the **User Groups** page.

The following table describes the parameters on the **General** tab of the **User Groups** page.

Table 118: User Groups Parameters: General Tab

Parameter	Description
Name	Specifies the name of the user group.
COS - Telephony	In the drop-down list, select the telephony features permissions COS to associate with the user group.
COS - Call Permissions	In the drop-down list, select the call permissions COS to associate with the user group.
COS - Voice Mail	In the drop-down list, select the voice mail COS to associate with the user group.

Parameter	Description
Send caller ID as caller's emergency identification (CESID)	Select this check box to use the caller ID configured on the User's page as the telephone number sent to the service provider when a user dials an emergency services number. If this option is not selected, the outbound caller ID will be either the user's DID or the site's CESID. This setting is enabled by default. **Note**: If RAY BAUM is enabled, then this option is not applicable for US sites. For more information about setting up emergency dialing, see Configuring a System for Emergency Calls on page 983.
Send DID as caller's emergency identification (CESID)	Select this check box to send this telephone number to the service provider when a user dials an emergency services number. If this option is not selected and **Send Caller ID as Caller's Emergency Service Identification** is also not selected, the outbound caller ID becomes the site's CESID. **Note**: If RAY BAUM is enabled, then this option is not applicable for US sites. For more information about setting up emergency dialing, see Configuring a System for Emergency Calls on page 983.

Parameter	Description
Account code collection mode	In the drop-down list, select one of the following account code collection modes for the user group: • **None:** Account collection is not active for this group. • **Optional:** Users are prompted to enter an account code. If no account code is entered, the call is completed without account code records. • Required: Users must enter an account code for all calls outside the bounds of the call permissions set for the user. For more information about account codes, see the Configuring Multi-Site Account Codes on page 356.
Show Mitel Connect client users a list of account codes when dialing	Select this check box to allow Connect client users to select an account code from the complete list of account codes when prompted for an account code. Clear this check box to restrict access to account codes for members of this user group.
Voice mail interface mode	In the drop-down list, select one of the following voice mail interfaces to associate with the user group: • **None:** Users use a standard Mitel voice mailbox. • **External Voice Mail, SMDI:** Connects to an external voice mail system using the SMDI protocol. • **Mitel Voice Mail, SMDI:** Connects to a legacy Mitel system using the SMDI protocol. • **External Voice Mail, SIP:** Connects to an external voice mail system by using the Session Initiation Protocol (SIP). • **External Voice Mail, QSIG:** Connects to an external voice mail system using the QSIG protocol.
Music on hold	In the drop-down list, select the music on hold resource to associate with the user group.

Parameter	Description
Outgoing trunk groups (Access Code)	Specifies the trunk groups this user group can access for outgoing calls. You can assign multiple trunk groups for this user group by clicking the name of each trunk group in the **Available** list and clicking the arrow button to move the trunk groups to the **Selected** list.

14.3.3.2 Profile Tab

Profile information for new and existing user groups is provided on the subtabs of the **Profile** tab in the **Details** pane of the **User Groups** page.

The following table describes the parameters on the **General** tab of the **User Groups** page.

Table 119: User Groups Parameters: Profile Tab with Subtabs

Subtab and Parameter	Description
Toolbars > Toolbar	Specifies the Connect client toolbars to appear for all members of this user group. A user group can have up to three global toolbars.
Phone Applications	Specifies On Idle and Available applications for the selected user group. A user group can have one On Idle application and up to ten Available applications.
Ringtones > Ring Pair	Specifies available internal and external ringtones that are accessible for the selected user group. A user group can have up to ten available pairs of ringtones.
Wallpapers > Wallpaper	Specifies available wallpapers. A user group can have up to four available wallpapers.

14.4 Configuring a User Account

This section describes how to view configured users in the system and how to create or modify a user account for either a new deployment or an existing MiVoice Connect system.

14.4.1 Viewing Users

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.

Note:
For descriptions of the columns on the Users page, see Users Page: List Pane.

Table 120: Users Page: List Pane

Column Name	Description
First Name	The first name of the user, fax machine, conference room, or virtual user.
Last Name	The last name of the user.
Extension	The user's extension.
Mobile Extension	The user's mobile extension, if one is configured.
Client User Name	The username that the user types to log into the Mitel system.
Site	The site associated with the user.
User Group	The user group associated with the user.

Column Name	Description
Access License	The type of access license the user has. This determines the user's capabilities in Connect client.
Primary Switch	The switch associated with the user.
VM Server	The server that hosts the user's voicemail box.
Server Type	The voice mail server type. If the voice mail server is a QSIG or SIP server, the name of the server is displayed; otherwise **Regular** is displayed.
Primary Port	The port associated with the user or the MAC address of an IP phone.
Status	The user's telephone port status, which can be one of the following values: • **Home** indicates that the user is at his or her home telephone port. • **Assigned** indicates that the user has assigned his or her extension to a different phone. • **Unassigned** indicates that there is no phone assigned to the user.
Soft Phone	Indicates whether or not the user is enabled for soft phone.
License Type	The type of license the user has. The license type determines the user groups and mailbox servers available to assign to the user.

14.4.2 Adding or Editing a User

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.

3. Do one of the following:

   - To edit an existing user, click the name of the user in the **List** pane.
   - To create a copy of an existing user, click **Copy**.
   - To create a new user, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the new or existing user.

4. Review the parameters on all of the tabs in the **Details** pane, and specify values as appropriate.

> **Note**:
> For more information about all of the user parameters on the various tabs of the details pane, see User Parameters on page 490.

14.4.3 User Parameters

A user account has many details. You configure user parameters on the following tabs, which you can access on the details pane for a particular user:

14.4.3.1 General Tab

General information about new and existing users is provided on the **General** tab on the **Users** page. Several of these parameters are automatically filled in from other fields in Connect Director.

The following table describes the parameters on the **General** tab of the **Users** page.

Table 121: Users Page: General Tab

Parameter	Description
Active Directory user	Select this check box to enable Active Directory for this user. **Note**: This option is only available when Active Directory integration is enabled for the Mitel system. For information about enabling AD integration, see Enabling AD Integration on a MiVoice Connect System on page 524.
Account(domain\username)	Enter the domain or the username of the user.
Show from AD	Click to display parameters for the user's Active Directory account. **Note**: This option is only available when Active Directory is enabled for the user.
Sync from AD	Click to synchronize user account records with contents from the Active Directory database. **Note**: This option is only available when Active Directory is enabled for the user.

Parameter	Description
First name	Specifies the first name of a user, fax machine, conference room, or virtual user.
Last name	Specifies the last name of the user.
Extension	Specifies the user's extension. **Note**: When configuring a new user, this field populates automatically with a number based upon a local cookie that was stored the last time a new user was configured.
Show References	Click to display a list of everywhere this extension is used.
Email address	Specifies the user's unique email address. This email address can be used in only one user profile. **Note**: The **Email address** field must be: • In standard email address format. • Not be a duplicate of an email address of any other user already in the system.
Edit System Directory record	Click this link to open the System Directory page, which allows you to edit the system directory details for this user.

Parameter	Description
Client username	Specifies the username that the user types to log into the Mitel system. Although the system generates a default username, which consists of the first letter of the first name and the full last name of the user, the system administrator can change the user ID to any string that follows these rules: • **Maximum length:** 100 characters **Note**: If Active Directory is enabled for the user, the maximum length of the Client username is 20 characters • Allowed characters: a - z, A - Z, 0 - 9, _, -, ., @, $ (underscore, dash, period, “at” symbol, dollar symbol) **Note**: When an administrator types values for the user’s first name and last name (even before clicking **Save**), the system generates a default client username (often called the client user ID or just the user ID), which consists of the first letter of the first name and the complete last name.
Include in System Dial by Name directory	Select this check box if you want the user’s name to be included in the auto-attendant’s dial-by-name directory.

Parameter	Description
Make extension private	Select this check box to remove this number from the system directory and call routing destination lists. For more information about private numbers, see Configuring Private Extensions on page 547.
Enable DID	Select this check box to authorize a user to use a DID number.
DID range	If a user is authorized for a DID, in the drop-down list select a DID range for the user. Before you can specify a DID range, DID services must be configured for the desired trunk group, which is enabled by default if a DID trunk group is configured.
View System Directory for DID usage	Click this link to view the System Directory page, with directory details for this user.
DID number	Specifies the DID number for the user.

Parameter	Description
PSTN failover	Specifies the PSTN number to be dialed to complete a failed site-to-site call. Enables you to select the following PSTN failover options: • None • External Number • DID The user must have a Class of Service with **Allow PSTN Failover** enabled. For more information, see Specifying a Class of Service on page 461. If there is no available bandwidth or if a WAN is down for a site-to-site call and if the call destination has no PSTN failover, the call is directed to voice mail.
Caller ID (overwrite DID)	Specifies the caller ID number for outbound calls. A caller ID number entered here takes precedence over the user's DID and the site's CESID number (both for normal outbound and 911 calls). If no number is entered, the user's DID or the site's CESID is used for outbound caller ID. This feature is available only for outbound calls on a SGT1 PRI trunk.

Parameter	Description
License type	Select one of the following license types from the drop-down list: • Extension and Mailbox • Extension-Only • Mailbox-Only **Note**: • The license type determines the user groups and mailbox servers available to assign to the user. This is based on the voice mail interface mode assigned to each individual user group and mailbox server. See License Types and Mailbox Interface Modes on page 503 for more information. • Mitel capacity is licensed by user license type, so ensure that your system has the required licenses for all users.

Parameter	Description
Access license	Specifies one of the following access levels for Connect client: • Phone only: Provides desktop call control, visual voice mail, call history, instant messaging, and directory services, as well as options to control availability states and message notification. This level does not require a special license. • Connect Client (default): Provides access to Instant Messaging, Presence, Contact Viewer, and SoftPhone. A video license is also provided to users who have rights to Connect client, providing access to VGA video. • Workgroup Agent: Provides access to workgroup features, including login, logout, wrap-up, queue monitor, and shared workgroup mailbox, plus the ability to transfer calls by dragging and dropping call cells into the buddy list. Does not include access to video. • Workgroup Supervisor: Provides access to the agent monitor, in addition to all features available to workgroup agents. • Operator: Provides access to XGA video and detailed information about destination extensions, including access to an extension monitor, in addition to all the features available to the workgroup supervisor.

Parameter	Description
User group	Select the user group to associate with the user from the drop-down list. The default user group is Executives. **Note**: Depending on the license type assigned to the user, some user groups may not be available for selection. See License Types and Mailbox Interface Modes on page 503 for more information.
Go to this user group	Click this link to go to the User Groups page, where you can view or edit the settings for the selected user group.
Site	Select the site for the user from the drop-down list. This setting filters the list of switch ports that you must select from as well as provides a different default DID number, if available.
Go to this site	Click this link to go to the Sites page, where you can view or edit the settings for this site.
Language	In the drop-down list, select the language that this user will hear for voice mail prompts.

Parameter	Description
Primary phone port	Select the primary phone port for the user from the following types: • **IP phone:** If you select **IP phone**, the drop-down list displays **Any IP Phone** as the default. For information about the Any IP Phone feature, see Overview on page 460. • **Port & CESID:** Select this option to assign an available analog port to the user from the drop-down list. If you assign an analog port and do not specify a port, Connect Director selects the next available port. Enter the CESID for the analog port. **Note**: To comply with RAY BAUM, you must provide the CESID for the analog port. • **SoftSwitch:** Select this option to create a user without a port (a virtual user). **Note**: Assigning users to an analog port or SoftSwitch for their home port can cause the loss of phone service if the user selects the **Go Home** option in Connect client. For this reason, Mitel recommends that Extension Assignment users be assigned **Any IP Phone** as their home port.

Parameter	Description
Current port	Indicates the user's current switch port. This shows the switch port to which the user has assigned his or her extension. You cannot edit this field directly, but you can change the current port setting to the home port by clicking **Go Primary Phone**. **Note**: If the user's extension is assigned to a soft switch, "Headquarters" is shown in this field.
Go Primary Phone	Clicking **Go Primary Phone** causes the system to force the user back to the home telephone. This option is useful when a temporary user is no longer using that phone.

Parameter	Description
Jack #	Specifies the patch-panel jack number associated with the user's switch port. **Note**: When you enter the jack number information in Connect Director and click **Save**, it is not saved. To address this issue, consider the following conditions: • In the **Primary phone port** field, if you select **IP phone**, then you must select the MAC address from the drop-down list. You can save the jack number only after you select the MAC address from the drop-down list. • In the **Primary phone port** field, if you select **SoftSwitch**, then you cannot save the jack number information.
Mailbox server	In the drop-down list, select the server to host the user's mailbox. **Note**: Depending on the license type assigned to the user, some mailbox servers may not be available for selection. See License Types and Mailbox Interface Modes on page 503 for more information.

Parameter	Description
Client password	Specifies the password that a user enters when logging in to Connect client. Value range: a - z, A - Z, 0 - 9, ! @ # $ % ^ & * ( ) _ + - = ~ ` [ ] \ ; ' , . / { } | : " < > ?. Default: changeme (Users are prompted to change this password when they log in for the first time.) **Note**: Mitel recommends that you do not change the default password because it is needed by users who are configuring their Connect client for the first time.
Must change on next login	Forces the user to enter a new password upon first-time login to Connect client. After the user enters a new password, the system clears this box. **Note**: If a user forgets his or her password, the system administrator can reset this option (select the check box) and enter a generic password, which allows the user to re-enter a new password.

Parameter	Description
SIP phone password	Specifies the user's SIP password. This enables the extension to support SIP; a SIP phone password is generated automatically when SIP is enabled for a user. If the SIP password is deleted, the extension will not support SIP. Value range: **a - z, A - Z, 0 - 9, !#$%&'()* +,-.:;=@[\]^_/`{|}~** Invalid characters: **? " <>** For more information, see Setting an Extension Password on page 718

14.4.3.1.1 License Types and Mailbox Interface Modes

The license type assigned to a user determines the user groups and mailbox servers available to assign to that user. This is based on the voice mail interface mode assigned to each individual user group and mailbox server.

- For Extension and Mailbox licenses:
  - Only user groups that use a voice mail interface mode of None are available in the drop-down list.
  - Only servers that use a voice mail interface mode of None, SMDI External voice mail, or SMDI Mitel voicemail are available in the Mailbox server drop-down list.
- For Extension-Only licenses:
  - The Voice Mail tab on the Users page is disabled.
  - User groups that use SMDI Mitel voice mail are not available.
  - When a user group that uses a voice mail interface mode of None is selected, the Mailbox server parameter is disabled.
  - When a user group that uses a different type of voice mail interface mode is selected, only servers that use the same type of voice mail interface mode are available in the Mailbox server drop-down list.

- For Mailbox-Only licenses:
  - Users with this license type cannot be assigned to ports.
  - Extension Assignment is not available to Mailbox-Only users, regardless of the COS settings.
  - User groups that use SMDI External, SIP Mitel, or QSIG External voice mail are not available.
  - When a user group that uses a voice mail interface mode of None is selected, only severs that use a voice mail interface mode of None, SMDI External voice mail, or SMDI Mitel voicemail are available in the Mailbox server drop-down list.
  - When a user group that uses a voice mail interface mode of SMDI Mitel voicemail is selected, only severs that use a voice mail interface mode of SMDI Mitel voicemail are available in the Mailbox server drop-down list.

14.4.3.2 Telephony Tab

Information about telephony features for users is provided on the **Telephony** tab. The following table describes the parameters on the **Telephony** tab of the **Users** page.

Table 122: Users Page: Telephony Tab

Parameter	Description
Call stack depth	Specifies the maximum number of calls, including active and held calls, that an extension can handle simultaneously. Valid values are 1-16. When this number is exceeded, calls are either given a busy tone or forwarded, depending on the availability state that is currently in effect. **Note**: The value specified in the **Max. call stack depth** parameter of the user's COS is the upper limit.

Parameter	Description
Ring type	In the drop-down list, select the ring type. Most IP phone models allow the user to load customized ring tones onto a phone, so each user can have a unique ring tone. For more information, see the Customizing Ringtones on page 313. **Note**: Ring type is a personal option for the user, not a phone configuration. When a user moves from phone to phone, their ring type follows.
Wallpaper	In the drop-down list, select the default wallpaper or background for the phone.
Automatic off-hook preference	Specifies one of the following devices that automatically gets activated for incoming and outgoing calls: • **Speaker** • **Headset** • **Wireless headset** • **Bluetooth headset** For configuration instructions, see Specifying Automatic Off-Hook for Wireless Headsets on page 326.
Enable handsfree mode	Select this check box to enable handsfree mode; this disables the dial tone so that the user can use a headset or speakerphone to answer and make calls from the desktop client. The default for this option is disabled.

Parameter	Description
Enable call waiting tone	Select this check box to enable the call-waiting tone, the user hears this tone for incoming calls while on a call. The default for this option is enabled. **Note**: The system plays different call waiting tones for calls waiting on the primary extension and calls waiting on a monitored BCA extension.
Trunk access code	In the drop-down list, select a trunk group access code. When you select this parameter, the user does not need to configure the trunk access code on his or her phone.
Mailbox for recorded calls	Specifies the mailbox to be used for recorded calls. The maximum recording length is determined by the voice mail class of service for the destination mailbox.
DECT headset quality	You can choose whether to optimize Mitel DECT headsets for voice quality or for a larger number of configured DECT headsets. Specify one of the following options: • **Wideband:** Deploy fewer Mitel DECT headsets in an area, but with better voice quality. • **Narrowband:** Deploy more headsets in an area, but with lower voice quality

Parameter	Description
DECT headset power mode	You can choosE whether to optimize DECT headsets for deployment density or operating range. Specify one of the following options: • **Normal:** Deploy DECT headsets in a higher density but a smaller operating range. • **High:** Deploy DECT headsets in a larger operating range but with poorer reception in areas with a high number of deployed DECT headsets. All DECT devices in an area must be configured to use the same headset power mode setting.
Fax support	Select one of the following options from the drop-down list to ensure that faxes are clearly and reliably transmitted: • **User - No Redirect:** Extension is connected to a user; do not redirect inbound Fax calls. • **User - Redirect:** Extension is connected to a user; redirect inbound Fax calls to site Fax redirect extension. • **Fax Server: Extension** is connected to a Fax server; do not redirect inbound fax calls but pulse DTMF digits. • **Fax Machine:** Extension is connected to a fax machine; do not redirect inbound fax calls. • **Non-T38 Data Terminal** • **Non-T38 Fax Server** **Note**: This option freezes the jitter buffer and disables the echo canceler at the beginning of the call and applies to environments that use SIP PSTN gateways.
Enable video calls	Select this check box to allow users to make video calls. Video calls are a licensed feature. In the drop-down list, select one of the following options: • **Standard -** for standard-resolution video • **High -** for high-resolution video

Parameter	Description
Enable telephony presence	Select this check box to enable the user to access the telephony presence information of other users. Telephony presence indicates a user's availability for accepting voice calls.
Enable shared call appearances	Select this check box to allow a user to participate in shared call appearance functions. For more information, see Configuring Bridged Call Appearance Conferencing on page 370.
Enable use of soft phone	Select this check box to allow the user to have access to the soft phone option in Connect client.
Enable phone API (PAPI)	Select this check box to enable the phone API, which allows third-party applications to run on certain IP phone models. Check with Mitel Technical Support for models that support this feature. **Note**: Selecting this check box enables the IP phone associated with this user to go into PAPI browser mode, thus allowing the phone to run those third-party applications.
Enable remote phone authentication	Select this check box if the user needs secure remote phone access. For more details about configuring remote phones, see Configuring VPN Phones on page 341.

Parameter	Description
Enable enhanced mobility with extension	Select this check box to add a user's mobile device as an additional phone on the user extension. A SIP extension is automatically created for the mobile client phone on the system and is displayed in the text field. (The SIP Phone License increments after the user phone is registered.) If the user's two additional phones are already allocated, you can replace one with the number of the new mobile extension. **Note**: To enable simultaneous ringing for the mobile extension, the user's assigned class of service must enable this feature.
Show References	Click to display a list of everywhere this extension is used.
Mobile phone number	Enter the user's mobile phone number. **Note**: This parameter is only available when the **Enable enhanced mobility with extension** check box is selected.
Enable delayed ringdown	Select this check box to enable delayed ringdown for the extension.

Parameter	Description
Ringdown number	Specifies the extension or outside number of the receiving device. If you specify an outside number, include the trunk access code. **Note**: This option is only available when the Enable delayed ringdown check box is selected.
Ringdown delay	Specifies the period of time, in seconds, that the phone waits after the user picks up the handset before initiating the ringdown call. Enter 0 in this field to cause the phone to immediately dial the ringdown device whenever the handset is picked up. **Note**: This option is only available when the Enable delayed ringdown check box is selected.
RAY BAUM E911 configuration options for endpoints	
Enable E911 vendor app usage	This option is used for endpoints (for third-party softphones only) that need to use vendor apps to update location information. **Note**: This option is applicable as part of RAY BAUM and should be enabled only for US customers.

Parameter	Description
Enable HELD for E911	This option is for future use. It will allow administrators to enable HELD (HTTPS-Enabled Location Discovery) directly from 400-Series and 6900-Series phones, so that these phones can provide the location information for emergency calls through the RedSky/Intrado location server. This HELD capability is being developed and will be included in the phone firmware at a later date. **Note**: This option is applicable only for US customers as part of RAY BAUM and is disabled by default.
Enable HELD location information report status	This option is for future use. It will allow administrators to enable HELD (HTTPS-Enabled Location Discovery) directly from 400-Series and 6900-Series phones, so that these phones can send the location information report status during an emergency call through the RedSky/ Intrado location server. This HELD capability is being developed and will be included in the phone firmware at a later date. **Note**: This option is applicable only for US customers as part of RAY BAUM and is disabled by default.

Parameter	Description
Enable teleworker location	Select this option to enable the teleworker location information during an emergency call **Note**: • This option is enabled by default for existing US-sites users. • This option is disabled by default for non-US customers. • This option is applicable only for 400-Series and 6900-Series phones.
Enable teleworker location update prompt	Select this option to receive a prompt regarding the location update from a teleworker phone for an emergency call. **Note**: • This option is enabled by default for existing US-sites users. • This option is disabled by default for non-US customers. • This option is applicable only for 400-Series and 6900-Series phones.

Parameter	Description
Enable teleworker location update notify	Select this option to receive notifications regarding the location update from a teleworker phone for an emergency call. **Note**: • This option is enabled by default for existing US-sites users. • This option is disabled by default for non-US customers. • This option is applicable for 400-Series and 6900-Series phones.

HELD is not currently supported by phones integrated with MiVoice Connect. Therefore, do not enable HELD-related options on these phones. You will not be alerted by any error messages if you enable these flags and therefore, you must configure these appropriately. The teleworker-related flags are meant only for teleworker (TW) phones. If you log in to the teleworker mode, these flags will be communicated as configured by administrator. For on-premises phones, these flags will always be treated as disabled. In this context, MiVoice Connect will consider the phone to be in teleworker mode only if a MAC-based entry in the IP address map with **Teleworker User** option is enabled.

Note:
You must provision the IP address map as explained above before provisioning these flags. If you do not do this, these flags will not be communicated until there is any change in the **Users** page or after a switch restart or server restart.

For example, if a new user is added before the IP address map is updated, then these flags will not be communicated to the phone immediately. Therefore, the administrator must follow these instructions:

Note:
These flags are meant only for Physical SIP phones (that is, IP 400-Series and 6900-Series phones).

For easy migration from earlier versions of US sites and to ensure that non-US sites are not affected, during the upgrade, teleworker-related flags are set to **true** for all users belonging to US sites in the configuration in earlier releases (releases earlier than 19.2 SP2). For all other sites, teleworker-related flags must be set to **false** before the upgrade so that this feature will not have any impact on non-US site customer and will not require any action from them. For US customers, after you complete the upgrade, you must update the IP address map and trigger a switch or server restart to communicate the actual flags to the phones.

Whenever there is a change in the Basic Service Set Identifier (BSSID), the phone will identify it and give a pop-up indication to the user about this. It is the responsibility of the teleworker user to update the new location information in the third-party vendor database with the help of the system administrator. If this is not done, the 911 emergency call might give incorrect location information to the PSAP.

The Mitel SIP phones (IP 400-Series and 6900-Series) running the latest firmware version send notifications to the user when a SIP phone is moved from one location to another. In this situation, the SIP phone will send a notification to MiVoice Connect, and MiVoice Connect adds that information to the messages log in the file named `EmergencyLocationUpdateInfo`. This information can be used for audit purposes later to determine whether the location was not updated by the end-user even after the phones requested for this.

This will be present in the standard log location of the controlling servers. These files will not be deleted automatically based on log file archive configuration; administrators can delete these log files manually only if they are no longer required for further auditing.

Logging the event might be required for legal auditing or other purposes. This is because the phone log is temporary and the vendor is not in Mitel's control. It is a single point of audit for MiVoice Connect solution that helps resolve any complaints.

The location change notification from teleworker phones can be enabled or disabled by the administrator by using the following options in the Connect Director configuration:

- **Enable HELD**
- **Enable HELD location information report status**
- **Enable teleworker location**
- **Enable teleworker location update prompt**
- **Enable teleworker location update notify**

See Users Page: Telephony Tab for more information.

By default, these options are enabled on the phone side and MiVoice Connect side for US customers and disabled on MiVoice Connect side for non-US users.

For more information, see Users Page: Telephony Tab.

14.4.3.3 Voice Mail Tab

Information about new and existing users' voice mail settings is provided on the **Voice Mail** tab on the Users page.

The following table describes the parameters on the **Voice Mail** tab and **Mailbox** subtab of the **Users Details** pane.

Table 123: Users Page: Voice Mail Tab

Parameter	Description
Voice mail password	Specifies the password that users enter when logging into their voice mailbox from the telephone. Characters in this field appear as asterisks. The default password is 1234. Users are prompted to change it the first time they log in to the system. We recommend that the default password be kept as the default because users configuring their telephone for the first time use 1234. For more information about setting passwords, see Voice Mail Password Recommendations on page 517
Must change on next login	Forces the user to enter a new password upon first-time login to a voice mailbox. After the user enters a new password, the system clears this box. **Note**: If a user forgets his or her password, the system administrator can reset this option (select the check box) and enter a generic password, which allows the user to re-enter a new password.
Accept broadcast messages	Select this check box to allow the user to receive broadcast messages. This is enabled by default.
Play envelope information when listening to messages	Select this check box to play a message stating the sender and the time the message was received at the beginning of each voice mail message.

Parameter	Description
Email delivery options	
Email address	Indicates the user's email address, which was configured on the **General** tab of the **Users** page.
Delivery type	Specifies whether and how voice mail messages are sent through email. Select one of the following options: • **Disabled:** Voice mail messages are not sent. • **Email text only:** The system sends an email message that notifies the user of the time, duration, and caller ID for the message that was recorded. • **Attach WAV file:** The system attaches the voice mail message to an email message as a WAV file. • **Email voicemail as link:** The system sends an email notification that includes a link to play, download or delete the voicemail message. If the user plays the voicemail message, the message is marked as heard in the voicemail system. If the user downloads the voicemail message, the message is downloaded to the computer. The voicemail state does not change. If the user deletes the voicemail message, the message is deleted from the voicemail system and moved to the deleted folder. **Note**: The email link points directly to the user's active voice mail server. If this voice mail box is moved to a different server, then the email link becomes invalid. However, the message is not lost; it can be accessed from Connect Client or the phone.

Parameter	Description
Mark message as heard	Select this check box to have the system mark emailed messages as heard. **Note**: This option is not available is the **Delivery** type is set to **Disabled**.
Send email warning when mailbox is full	Select this check box to have the system send users a notice informing them that their mailbox is almost full.
Automatic message forwarding	
Destination	Specifies the destination for forwarded voice mail messages. Select one of the following options: • **None:** Voice mail messages are not forwarded. • **Mailbox:** Specify the target mailbox for forwarded messages. • **AMIS Mailbox:** Specify the target AMIS mailbox for forwarded messages.
Delete message after forwarding	Select this check box to automatically delete each message after it is forwarded. This option is disabled by default, meaning messages are not deleted after forwarding.

14.4.3.3.1 Voice Mail Password Recommendations

Mitel recommends you follow these guidelines for creating secure voice mail passwords:

- When creating a new user, assign the user a complex initial password.
- Educate end users to change the default PIN to one that is more complex. (Avoid passwords with simple digit patterns such as 1111, 4321, and so on).
- Check CDRs regularly to detect any abnormal calling activities, such as calls coming and going to a country with which you are not doing business.
- If your business does not require international dialing, prevent international call-back from voicemail by restricting the relevant user group to local and long-distance calls

only. You can also restrict voicemail call-back to any external number using the Class of Service Voice Mail Permissions.
- Increase the voicemail password length to at least 6 digits system-wide. A longer PIN is more secure and creates more number combinations.
- Enable email alerts for system event ID 1113 for repeated voicemail login access failures.

14.4.3.4 Routing Tab

Information about new and existing users' call routing settings is provided on the **Routing** tab of the **Users** page. This tab contains the following subtabs, and information about these parameters is provided in the subsequent sections:

- **Phones**
- **Ring Me**
- **Availability States**
- **Power Routing Rules**

14.4.3.4.1 Phones Subtab

Phones Subtab

For details about the fields on the Phones subtab, see Implementing Simultaneous Ringing on page 347.

14.4.3.4.2 Ring Me Subtab

For details about the fields on the Ring Me subtab, see Routing Calls to Other Phones on page 555.

14.4.3.4.3 Availability States Subtab

From this tab, you can set the current availability state for the user. For details about availability states, see Configuring Availability States on page 559.

14.4.3.4.4 Power Routing Rules Subtab

Any power routing rules that the user has created in Connect client are listed here. For details on configuring power routing rules, see Configuring Power Routing Rules on page 569.

14.4.3.5 Membership Tab

New and existing users' call routing settings are provided on the **Routing** tab of the **Users** page. This tab contains the **Distribution List** and **Workgroups** subtabs.

14.4.3.5.1 Distribution List Subtab

A distribution list lets a user send a voice mail message to multiple users at one time. Each distribution list has a descriptive name and an extension associated with it.

When a user is associated with a distribution list, the user receives messages sent to that list. Users can be associated with more than one distribution list. Users can be associated with distribution lists from either this **Distribution List** subtab or from the **System Distribution List** page.

For details about adding distribution lists and populating them with multiple users, see Configuring System Distribution Lists on page 583.

To add or delete a single user from a distribution list:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the user you want to add or remove from a distribution list.
4. In the **Details** pane, click the **Membership** tab and the **Distribution List** subtab.
5. Do one of the following:
   - To include the user in a specific distribution list, select the distribution list in the **Available** list and click the right arrow button to move it to the **Selected** list.
   - To remove the user from a distribution list select the distribution list in the **Selected** list and click the left arrow button to move it to the **Available** list.
6. Click **Save**.

14.4.3.5.2 Workgroups Subtab

The **Workgroups** subtab on the **Membership** tab of **Users** page allows you to edit a user's workgroup membership. Users can belong to multiple workgroups; however, a user's login status is the same for all workgroups of which the user is a member.

The **Workgroups** page shows the workgroup lists that are currently available. You can change a user's membership in workgroups as follows:

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. In the **Details** pane, click the **Membership** tab and the **Workgroups** subtab.
4. Do one of the following:

   - To include the user in a workgroup, select one or more workgroups in the **Available** list and click the right arrow button to move the workgroups to the **Selected** list.
   - To remove the user from a workgroup, select one or more workgroups in the **Selected** list and click the left arrow button to move the workgroups to the **Available** list.
5. To activate the user's membership in the selected workgroups select the **Logged in** option in the **Agent state field**.
6. Click **Save**.

For more information about the Workgroups feature, see Configuring Workgroups on page 631.

14.4.3.5.3 Delegation Tab

You can delegate availability state management for an individual user to one or more other users, such as an administrative assistant. For details about this capability, see Configuring Availability State Delegation on page 568.

14.4.3.6 DNIS Tab

The following table describes the parameters on the **DNIS** tab of the **Users Details** pane.

Table 124: Users Page: DNIS Tab

Parameter	Description
Add	To associate the user with a DNIS, click **Add** and provide details for the DNIS mapping in the displayed fields.
Trunk group name	From the drop-down list, select the trunk group for the DNIS mapping.
Digits	Enter the DNIS number.

Parameter	Description
Description	Provide a description for the DNIS number. This description is seen by call recipients and in call detail reports (CDRs). The description length can be up to 26 characters.
Music on Hold	From the drop-down list, select a file-based MOH resource.
Remove	If you want to remove a DNIS system that is configured for this user, click **Remove**.

14.4.3.7 Applications Tab

The **Applications** tab displays whether various Connect Sync services are enabled for the user. The following table describes the parameters on the **Applications** tab of the **Users Details** pane.

Table 125: Users Page: Applications Tab

Parameter	Description
Conference Bridge Appliance	In the drop-down list, select the Service Appliance to assign to the user for conferencing.
Instant Messaging Server/ Appliance	In the drop-down list, select the Service Appliance to assign to the user for instant messaging.

14.5 Adding or Editing Users in the System Directory

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **System Directory**. The **System Directory** page opens.
3. Do one of the following:

   - To edit an existing system directory record for a user, click the name of the user in the list pane.
   - To add a new system directory record for a user, click **New**.

Note:
The **General** tab displays the details for the system directory record in the **Details** pane.

4. Edit some or all of the fields on the **General** tab as necessary.

14.6 Using Active Directory with a MiVoice Connect System

Directory services store organization information and settings in a central, organized, accessible database. Active Directory (AD) is the Microsoft application that implements AD on Windows-based systems. AD is widely deployed among large enterprises.

The Mitel AD implementation supports the synchronization of user records between the Mitel database and other applications that use AD on Windows-based networks.

Mitel AD includes the following features:

- Authentication of AD Users, as described in AD User Authentication on page 524.
- Synchronizing AD and Connect Director user records, as described in Synchronizing Mitel User Records with AD User Records on page 526.
- Bulk provisioning of user accounts, as described in Bulk Provisioning of AD User Accounts on page 528.

14.6.1 Configuring AD Integration on a MiVoice Connect System

Active Directory Integration is an optional Mitel feature that is disabled by default. Systems that do not have AD integration enabled do not recognize links to the Active Directory for properties attached to system users and do not provide AD authentication, synchronization, or provisioning services.

When AD integration is enabled, only users who have administrative permissions can log into Connect Director. This requirement means that at least one administrator role must be defined. It also means that users who need access to Connect Director must receive an administrative role.

Note:

At least one user account must have administrative rights before Active Directory is enabled. AD does not allow a user to log in through the default admin account.

14.6.1.1 Creating a New AD User with Administrative Rights

At least one AD user account must be created and assigned administrative rights before AD is enabled. AD does not allow a user to log in through the default admin account.

1. Log in to the Active Directory account through which you access Connect Director.
2. Launch Connect Director, and log in with the following default credentials:
   - username – **admin**
   - password – **changeme**
3. If the system presents an option to register, click **Later**.
4. If the AD user you want to give administrative permissions to does not already exist in the MiVoice Connect system, add a new user to the MiVoice Connect system that uses the Client Username that matches the Active Directory login name of the new administrator. For detailed instructions on adding a user, see Adding or Editing a User on page 489.
5. Launch Connect Director.
6. In the navigation pane click **System** > **Administrative Permissions** > **Administrators**.

   The **Administrators** page is displayed.
7. Click **New**.

Note:

The General tab in the details pane displays parameters for the new administrator.

8. In the **User extension** field, enter the extension for the Active Directory user you want to make an administrator.
9. In the **Role** list, select **System Administrator**.
10. Click **Save**.

The new system administrator is added in the list pane.

14.6.1.2 Enabling AD Integration on a MiVoice Connect System

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Additional Parameters**. The **Additional Parameters** page opens.
3. Under **Active directory (AD) integration**, select the **Enable AD integration** check box.
4. In the **AD path** field, enter a valid AD path.
5. Click **Save**.

14.6.1.3 Enabling AD Integration for a User

1. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
2. Click the name of the user you want to enable AD integration for in the list pane.
3. On the **General** tab, select the **Active Directory user** check box.
4. In the **Account** field, enter the domain and client username as follows:

   ```
   domain\username
   ```
5. Click **Save**.

Whenever Connect Director is subsequently launched using this username and domain, the user is logged into Connect Director automatically.

14.6.2 AD User Authentication

Mitel supports AD authentication for users who log into Connect client and Connect Director. This allows users access to these programs without providing the Mitel username or password.

AD users who log into Connect Director and Connect client are authenticated through single sign on (SSO) with their current network credentials. Users are not required to re-enter credentials to access these applications.

14.6.2.1 AD Authentication for Connect Director

When AD Integration is enabled, user access to Connect Director includes the following restrictions:

- Only users with a domain account can log into Connect Director.
- Only users with administrative permissions can log into Connect Director.
- Users do not need to log into their domain account to access Connect Director.
- Users do not need their Mitel account configured for Active Directory (AD Users) to access Connect Director.

14.6.2.1.1 AD User Logged into the Domain

If a Mitel user with AD configured is logged in to the domain and tries to access Connect Director without entering network credentials, the user is directed to the Diagnostics & Monitoring Dashboard page.

When a user with AD access logs out, the browser displays a Connect Director login page.

14.6.2.1.2 Non-AD User Logged into the Domain

If a user without AD configured is logged in to the domain and tries to access Connect Director, the user is directed to a Connect Director login page. The user logs into Connect Director from this screen by entering a Mitel username and password.

14.6.2.1.3 Users Not Logged into the Domain

If a user attempts to access Connect Director without first logging into the domain network, the user is initially routed to a domain login page. After entering network credentials, the user is routed to the appropriate page. AD users are routed to the Diagnostics and Monitoring Dashboard, and non-AD users are directed to a Connect Director login page.

14.6.2.2 AD Authentication for Connect Client

When AD Integration is enabled, access to Connect client is available to all system users, including users who have no domain account or are not configured as Mitel AD users.

14.6.2.2.1 Initial Configuration

When installing Connect client, users authenticated through AD are not queried for their credentials; they are immediately prompted for the server name after which wizard panels guide them through the setup process.

Users that are not authenticated through AD are required to enter their username, password, and server name. After verifying the user’s credentials, Connect client guides the user through the setup process.

14.6.2.2.2 Logging into Connect Client

Attempts to log into Connect client after the initial setup are handled on the basis of the user's AD configuration. Active Directory users are authenticated by SSO through the verification of their AD credentials.

Users not configured for Active Directory are authenticated through the verification of their Mitel username and password, if previously loaded through their Connect client account. Connect client behavior after an authentication failure is not changed by this feature.

The username of the user is visible on the **Preferences** > **Account** > **Login** tab of the Connect client.This field can be altered from the **Preferences** > **Account** > **AD Credentials** tab. For more information, see the *Mitel Connect Client User Guide*.

14.6.3 Synchronizing Microsoft Office 365 in Connect Director

If you are using Microsoft Office 365 or Exchange 2013, enter the following AD credentials to enable Microsoft Exchange synchronization for Mitel conferences.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Additional Parameters**. The **Additional Parameters** page opens.
3. Under **Exchange Server**, enter the following details:

    a. Type **outlook.office365.com** in the **Exchange Server field**.
    b. Enter **NONE** in the **Username** field.
    c. Leave the **Password** field blank.

14.6.4 Synchronizing Mitel User Records with AD User Records

Connect Director provides an interface for adding, updating, and deleting AD users from the Mitel database. Synchronization is performed on individual users and does not affect the AD directory.

You can designate whether the AD user principal name or the email address should be used to sync the records. By default, Connect Director syncs from the AD user's user principal name. To sync from the AD user's email address, set the value of the `HKLM \Software\Wow6432Node\Shoreline Teleworks\UseADSMTPFieldForEMail` registry key to 1 or any non-zero value.

14.6.4.1 Viewing Mapped Active Directory and Mitel Fields

Mitel user records contain eleven data fields that map directly to Active Directory records. The following is a list of these data fields, categorized by the Connect Director page that sets their Mitel value.

- **Users Page**
  - **First name:** Active Directory field capacity is 64 characters; Mitel capacity is 50.
  - **Last name:** Active Directory field capacity is 64 characters; Mitel capacity is 50.
  - **Email address**
  - **Client username:** Active Directory length is limited to 20 characters.
- **System Directory**
  - **Home phone**
  - **Work phone**
  - **Mobile phone**
  - **Fax**
  - **Pager**
- **Mitel Database** (This data field does not appear in Connect Director).
  - **AD GUID:** Used internally by the MiVoice Connect system when performing subsequent user updates from the AD database.

To view mapped fields for a user:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the AD user to view mapped fields for in the list pane.

Note:
The **General** tab in the **Details** pane displays the parameters for the selected user.

4. In the AD section, click **Show from AD**. The **AD Data** dialog box displays all mapped fields for the selected user.
5. Review the mapped fields, and then click **OK** to close the dialog box.

14.6.4.2 Updating AD User Records

Active Directory users can synchronize user account records with contents from the Active Directory database by pressing the **Sync from AD** button located to the right of the user's Active Directory userid. Pressing the **Show From AD** button displays parameter settings for the user's Active Directory account.

The **Show From AD** and **Sync From AD** buttons are inactive for users accessing this page that are not configured as AD users.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the AD user to update in the list pane.

Note:
The **General** tab in the **Details** pane displays the parameters for the selected user.

4. In the AD section, click **Sync from AD**.
5. Click **Save**.

14.6.4.3 Removing AD Users

When an administrator attempts to delete a user with an AD account, Mitel displays a warning and requires confirmation before it removes the record from the Mitel database.

14.6.5 Bulk Provisioning of AD User Accounts

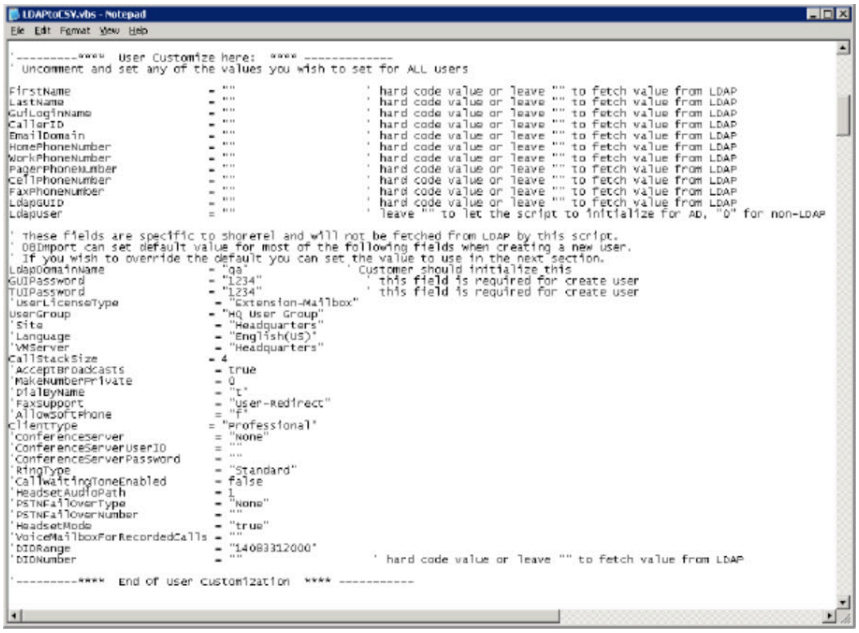
Mitel supports the bulk provisioning of user accounts from AD records through the following process:

1. Export AD records to a CSV file.
2. Modify the CSV file to conform to the format needed by the database import utility (User Import Tool). For detailed information about the database import utility, see Modifying the CSV File on page 530.
3. Import records from the CSV file to the Mitel user database using the database import utility (User Import Tool). For detailed information about the database import utility, see Importing the CSV File on page 539.

14.6.5.1 Exporting AD Records

Mitel provides a sample VBScript file (ldaptocsv.vbs) that can be used as a template for exporting records from an AD database to a CSV file. Before using the VBScript file to export AD records, the file must be customized to work with your specific system requirements. The following figure shows the parameter section of the VBScript file.

Figure 15: Sample ldaptocsv.vbs File, Parameter Sections



The parameter section in the figure above has two subsections:

- The top section pulls values for each user record from the AD database into the CSV file. As indicated in the comments section, a single value can be assigned to an individual field for all users by entering the value inside of the quotation marks.
- The bottom section is a data template containing non-AD fields that are saved to the CSV file. The values entered in these fields are assigned to all user records retrieved from the AD database.

The following command line entry executes the export from AD to the CSV file:

```
cscript ldaptocsv.vbs outputCSVfile LDAPpath
[modifiedInLastN#OfDays]
```

- `outputCSVfile` specifies the name of the output file
- `LDAPpath` specifies the path to the AD database
- `[modifiedInLastN#OfDays]` is an optional delimiter in the form of a number of days

This delimiter allows you to import only the active directory entries that have been modified within the past number of days specified. This can reduce the amount of information that the system has to export.

The resulting CSV file can be modified using a spreadsheet program to customize user settings for import into the Mitel database.

14.6.5.2 Modifying the CSV File

Once the AD record are exported to a CSV file, the CSV file must be modified to conform to the format needed by the database import utility (User Import Tool). For detailed information about the required format of the CSV file, see Setting Up the CSV File for Import on page 532.

The following fields are required in the CSV file in order to support AD record imports:

- **LDAP-User flag:** A flag that indicates the user settings came from an AD database.
- **LDAP-GUID:** A data field that creates an association between an AD record and the corresponding Mitel record.
- **NTLoginName:** Specifies the user's domain and username.

14.7 User Management Utilities

To facilitate user management, the MiVoice Connect system includes the following utilities and capabilities, which are described in the subsequent sections:

- User Import Tool
- Bulk Edit
- Notify Users
- Extension Lists

14.7.1 User Import Tool

The database import utility (User Import Tool) allows a system administrator to add users to a Mitel system in bulk. The database import utility can also be used to delete users from the system or to make modifications to all users in a system. The utility increases the ease and speed with which a system administrator can modify information for large groups of users.

The administrator prepares a CSV file containing user data, and then modifies the user data in a "free form" approach (instead of modifying each user's information within Connect Director).

The administrator can prepare the CSV file using one of the following methods:

- Export user information from Connect Director to a CSV file.
- Use an application, such as Microsoft Excel, to prepare a spreadsheet containing user information and then save the file as a CSV file.
- Export Active Directory records from an AD database to a CSV file. For information about exporting AD records, see Bulk Provisioning of AD User Accounts on page 528.

After the user information has been modified within the spreadsheet, the CSV file can be imported into the MiVoice Connect system.

- The database import utility supports modify, delete, and add operations. This allows a system administrator to add users, delete users, or modify the account of an existing user.
- Using the database import utility does not require scheduled downtime. However, when importing large files that contain many rows of information, performance may be affected as the database is frequently queried. Depending on the size of the imported file and the type of information that is being added or modified, it may be recommended to perform the import during off hours.
- The primary phone port for a user is set using the HomePhoneMACAddress database import field. The primary phone port is determined according to the following rules, in this exact order:

  1. If the HomePhoneMACAddress field is specified, the primary phone port is assigned to the defined IP phone.
  2. If the HomePhoneMACAddress field is left blank and UserLicenseType is set to Extension-Mailbox, the primary phone port is set to Any IP Phone on the Headquarters server.
  3. If the HomePhoneMACAddress field is left blank and the Site is set to a remote site with a SoftSwitch (DVS) available, the primary phone port is set to SoftSwitch on the remote site.
  4. If none of the above apply, the primary phone port is set to SoftSwitch on the Headquarters server.

14.7.1.1 Exporting the CSV File

The system administrator can export user information from Connect Director to a CSV file. This CSV file contains all the compatible headings and is in the format required by the database import utility.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click **Export**.
4. Follow the prompts to save the CSV file.

14.7.1.2 Setting Up the CSV File for Import

The following table describes the fields accepted by the database import utility. All field headers are case-sensitive, and the following fields must be included in the CSV file:

- Extension
- FirstName
- LastName
- GuiLoginName
- GUIPassword
- TUIPassword

The field headers can appear in any order within the first row of the CSV file.

Note:
CSV files created by exporting user information from Connect Director contain all headings compatible with the database import utility.

- For fields that require string input, the string must already exist in the MiVoice Connect system. For example, if a new user is to be created at a site named New York, “New York” must already exist as a site name in the MiVoice Connect system. Strings are case-sensitive.
- For fields that require code input, the field must be entered exactly as it appears in Connect Director. Data validation translates the displayable value to the appropriate code. Descriptions are case-sensitive.
- Boolean fields can be true/false or 1/0.
- When updating an existing user, fields left blank will not change existing values.

Table 126: Fields Required by the Database Import Utility

CSV Field Header	DataBase Field Name	Accepted Input
Extension	UserDN	Number
FirstName	TabAddresses.FirstName	String
LastName	TabAddresses.LastName	String
GuiLoginName	GuiLoginName	String

CSV Field Header	DataBase Field Name	Accepted Input
GUIPassword	GUIPassword	String
TUIPassword	TUIPassword	String
UserLicenseType	LicenseTypeID	Code; must exactly match one of the following: • `Extension-Mailbox` • `Extension-Only` • `Mailbox-Only`
CallerID	CIDNumber	Number; must be a full canonical number (such as +1 (408) 331-3300)
UserGroup	UserGroupID	String; must exactly match the name of an existing User Group configured on the system.
Site	Site	String; must exactly match the name of an existing Site configured on the system
Language	DN.LanguageID	Code; must exactly match the name of one of the enabled languages on the system (e.g. “English(US)”).

CSV Field Header	DataBase Field Name	Accepted Input
VMServer	VMServerID	String; must exactly match the name of an existing VM, SIP, or QSIG server configured on the system (depending on the Voicemail interface mode configured for the user group that the user is assigned to).
CallStackSize	CurrentCallStackDepth	Number
AcceptBroadcasts	Mailboxes.NoReceiveBroadcasts	Boolean
MakeNumberPrivate	DN.Hidden	Boolean
DialByName	DN.ExcludeFromDialByName	Boolean
FaxSupport	FaxSupport	Code; must exactly match one of the following: • `User-No Redirect` • `User-Redirect` • `FAX Server` • `Fax Machine` • `Non-T38 Data Terminal` • `Non-T38 Fax Server`
AllowSoftPhone	AllowSoftPhone	Boolean

CSV Field Header	DataBase Field Name	Accepted Input
ClientType	ClientType	Code; must exactly match one of the following: • `Phone Only` • `Connect Client` • `Workgroup Agent` • `Workgroup Supervisor` • `Operator`
EmailDomain	TabAddresses.EmailAddress	String
ConferenceServer	BridgeID	String; must exactly match the name of an existing service appliance configured on the system.
RingType	RingToneID	Code; must exactly match the name of an existing ring tone available on the system. Examples: • `Standard` • `Ring 2` • `Ring 3` • `Ring 4`
CallWaitingToneEnabled	CallWaitingToneEnabled	Boolean
HeadsetAudioPath	UseHeadsetAudioPath	Number
HeadsetMode	HeadsetMode	Boolean

CSV Field Header	DataBase Field Name	Accepted Input
PSTNFailOverType	PSTNFailOverTypeID	Code; must exactly match one of the following: • `None` • `External` • `DID`
PSTNFailOverNumber	PSTNFailOverNumber	Number; must be a full canonical number (such as +1 (408) 331-3300)
DIDRange	DIDDigitMap.DIDRangeID	Number; must be a full canonical number base of range (such as +1 (408) 331-3300)
DIDNumber	DIDDigitMap.Digits	Number; the number of digits for the DIDNumber must match the number of digits expected from the central office (CO) **Note**: The number of digits expected from the CO is configured on the Inbound tab on the Trunk Groups page for the trunk group with the DID Range that matches the user's DID Range. For more information, see Inbound Tab on page 225.

CSV Field Header	DataBase Field Name	Accepted Input
VoiceMailboxForRecordedCalls	VoiceMailboxForRecordedCalls	Number; must be an existing valid extension (or can be left blank)
MustChangeTUIPassword	MustChangeTUIPassword	Boolean
MustChangeGUIPassword	MustChangeGUIPassword	Boolean
EnableCC	ContactCenterIntegration	Boolean
MustRecordName	MustRecordName	Boolean
HomePhoneMACAddress		String; must be digits only, do not use spaces or dashes
HomePhoneNumber		Number; must be a full canonical number base of range (such as +1 (408) 331-3300)
WorkPhoneNumber	TabAddresses.WorkPhone	Number; must be a full canonical number base of range (such as +1 (408) 331-3300)
PagerPhoneNumber	TabAddresses.PagerPhone	Number; must be a full canonical number base of range (such as +1 (408) 331-3300)
CellPhoneNumber	TabAddresses.CellPhone	Number; must be a full canonical number base of range (such as +1 (408) 331-3300)

CSV Field Header	DataBase Field Name	Accepted Input
FaxPhoneNumber	TabAddresses.FAXPhone	Number; must be a full canonical number base of range (such as +1 (408) 331-3300)
LdapUser	LDAPUser	Code; must exactly match one of the following: • `Non-LDAP user` • `Active Directory`
LdapGuid	LDAPGuid	String
NTLoginName	NTLoginName	String; must exactly match the domain and username of the AD user in the following format: `domain\username`
AllowPapi	AllowPAPI	Boolean
AllowVideoCalls	AllowVideoCalls	Code; must be blank or exactly match one of the following: • `None` • `Standard` • `High Resolution`
AllowTelephonyPresence	AllowTelephonyPresence	Boolean
IMServer	IMServerID	String; must exactly match the name of an existing IM server configured on the system. “<NULL>” clears the field.

CSV Field Header	DataBase Field Name	Accepted Input
SIPPassword	SIPPassword_formatted *and* SIPPassword_confirmation_formatted	String

You can create or modify the spreadsheet to perform the following actions:

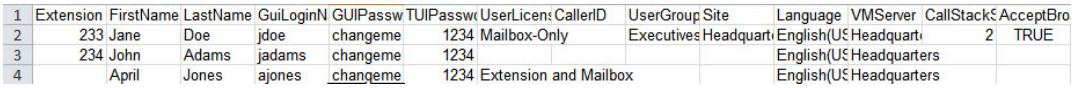
- Add Users
  - Ensure that you have included values for each new user in the following required fields: FirstName, LastName, GUIPassword, TUIPassword, and GUILoginName.
  - The Extension field is optional; if the extension field is left blank, an extension is assigned to the user automatically.
  - With the exception of the Extension field, any fields left blank for a new user will be left blank in Connect Director.
- Modify Users
  - Enter data for any fields that you want to change. Fields left blank will remain unchanged in Connect Director.

Note:
When a user is updated, the user is assigned to “Any IP Phone” on the Headquarters server

- Delete Users
  - Enter the extension for the user you want to delete and leave all other fields blank.

Example: The following figure illustrates some of the spreadsheet values before importing them into Connect Director.

Figure 16: Spreadsheet Values before Connect Director Import



	Extension	FirstName	LastName	GuiLoginN	GUIPassw	TUIPassw	UserLicen	CallerID	UserGroup	Site	Language	VMServer	CallStack	AcceptBro
2	233	Jane	Doe	jdoe	changeme	1234	Mailbox-Only		Executives	Headquart	English(US	Headquart	2	TRUE
3	234	John	Adams	jadams	changeme	1234					English(US	Headquarters		
4		April	Jones	ajones	changeme	1234	Extension and Mailbox				English(US	Headquarters		

14.7.1.3 Importing the CSV File

The following procedure describes the process of importing data from a CSV file into the MiVoice Connect user database using the database import utility. This procedure assumes that you have already done one of the following:

- Exported a spreadsheet from Connect Director.
- Created a spread sheet and successfully exported it to a CSV file that conforms to the format required by the database import utility For information about creating the CSV file, see Setting Up the CSV File for Import on page 532.
- Exported Active Directory records from an AD database to a CSV file and modified the CSV file to conform to the format required by the database import utility. For information about exporting AD records, see Bulk Provisioning of AD User Accounts on page 528.

1. Verify that the CSV file to be imported is located on the Headquarters server in the following location:

   `C:\ProgramFiles\ShorelineCommunications\ShoreWareServer`
2. Open the command prompt window in the directory shown above and run the following command:

   ```
   Dbimport -u <username> -p <password> -log DbLog.log -err
   DbErr.err <filename.csv>
   ```

   - username and password must be valid log in credentials used to log in to Connect Director
   - `-err DBErr.er` is the flag to create a file named DBErr.er in the current directory; error messages are stored in this file
   - `-log DBLog.log` is the flag to create a log file named DBLog.log in the current directory
   - `filename` is the name of the CSV file that will be imported

14.7.2 Bulk Edit

You can use the Bulk Edit feature to make changes to multiple users at the same time. This allows you to identify a set of users and globally change certain parameters. You can also use the Bulk Edit feature to copy the Programmable Buttons (IP Phones and Button Box) settings from one user to one or more other users. Run the bulk edit feature during off hours as it may drop calls in the system.

To use the Bulk Edit feature, do the following:

1. Launch Connect Director with administrator privileges.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. In the **List** pane, select the check box for each user you want to include in the bulk edit.
4. Click **Bulk Edit**. The **Bulk Edit** tab in the **Details** pane displays the parameters available for editing.

5. Review the parameters and specify values as appropriate.

> **Note**:
> For more information about all of the available parameters on the **Bulk Edit** tab, see Users Page: Bulk Edit Tab.

6. Click **Save**.

To copy Programmable Buttons settings to other users:

1. Launch Connect Director with administrator privileges.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. In the **List** pane, click to highlight the name of the user you want to copy **IP Phone Button** or **Button Box** settings from.
4. In the **List** pane, select the check box for each user you want to copy the settings to.
5. Click **Bulk Edit**. The **Bulk Edit** tab in the **Details** pane displays the parameters available for editing.
6. Select one or more of the following check boxes to copy the corresponding Programmable Buttons settings:
   - **IP Phones**
   - **Button Box 1**
   - **Button Box 2**
   - **Button Box 3**
   - **Button Box 4**
7. Click **Save**.

Table 127: Users Page: Bulk Edit Tab

Parameter	Description
User group	Select this check box to edit the user group for all selected users. In the drop-down list, select the desired user group to associate with the users.

Parameter	Description
Call stack depth	Select this check box to edit the call stack depth for all selected users. Specify the maximum number of calls, including active and held calls, that an extension can handle simultaneously. Valid values are 1-16. When this number is exceeded, calls are either given a busy tone or forwarded, depending on the availability state that is currently in effect. **Note**: The value specified in the **Max. call stack depth** parameter of the user's COS is the upper limit.
Personal assistant	Select this check box to edit the personal assistant for all selected users. The personal assistant is the user that calling parties are routed to when they dial "0" in a user's mailbox. Specify the extension of the personal assistant.
Email domain	Select this check box to edit the email domain (@company.com) for all selected users. Specify the desired email domain.

Parameter	Description
License type	Select this check box to edit the license type for all selected users. Select one of the following license types from the drop-down list: • Extension and Mailbox • Extension-Only • Mailbox-Only **Note**: Mitel capacity is licensed by user license type, so ensure that your system has the required licenses for all users.
Access license	Select this check box to edit the access license type for all selected users. In the drop-down list, select one of the following access levels for Connect client: • Connect Client (default): Provides access to Instant Messaging, Presence, Contact Viewer, and SoftPhone. A video license is also provided to users who have rights to Connect client, providing access to VGA video. • Operator: Provides access to XGA video and detailed information about destination extensions, including access to an extension monitor, in addition to all the features available to the workgroup supervisor. • Phone only: Provides visual voice mail (for supported phone models), call history, and directory services, as well as options to control availability states and message notification. This level does not require a special license.

Parameter	Description
Access license (continued)	• Workgroup Agent: Provides access to workgroup features, including login, logout, wrap-up, queue monitor, and shared workgroup mailbox, plus the ability to transfer calls by dragging and dropping call cells into the buddy list. Does not include access to video. • Workgroup Supervisor: Provides access to the agent monitor, in addition to all features available to workgroup agents.
Instant Messaging Server/ Appliance	Select this check box to edit the instant messaging service appliance for all selected users. In the drop-down list, select the Service Appliance to assign to the user for instant messaging.
Mailbox server	Select this check box to edit the mailbox server for all selected users. In the drop-down list, select the server to host the user's mailboxes.
Conference Bridge Appliance	Select this check box to edit the conference bridge appliance for all selected users. In the drop-down list, select the Service Appliance to assign to the selected users for conferencing.
Enable video calls	Select this check box edit the video calls parameter for all selected users. Select the second check box to allow users to make video calls. Video calls are a licensed feature. From the drop-down list, select one of the following options: • **Standard** - for standard-resolution video • **High** - for high-resolution video
Enable use of soft phone	Select this check box edit the soft phone parameter for all selected users. Select the second check box to allow users to have access to the soft phone option in Connect client.

Parameter	Description
Trunk access code	Select this check box to edit the trunk access code for all selected users. In the drop-down list, select a trunk access code. When you select this parameter, the user does not need to configure the trunk access code on his or her phone.
IP Phones	Select this check box to copy all IP Phone button settings from the specified user to all other selected users.
Button Box 1	Select this check box to copy all Button Box 1 settings from the specified user to all other selected users.
Button Box 2	Select this check box to copy all Button Box 2 settings from the specified user to all other selected users.
Button Box 3	Select this check box to copy all Button Box 3 settings from the specified user to all other selected users.
Button Box 4	Select this check box to copy all Button Box 4 settings from the specified user to all other selected users.

14.7.3 Notify Users

You can notify users that their Connect client or Connect client for Mobile – has been installed or upgraded. Once the user receives notification that their client application has been installed, the user can begin configuring personal options and use the application.

14.7.3.1 Invoking Automatic Notification

1. Launch Connect Director with administrative privilege.
2. In the navigation pane, click **Administration** > **Features** > **Client** > **Notify Users**. The **Notify Users** page opens.

3. Do one of the following:

   - To notify all users using the client who have not already been notified, select **All new users** under **Send welcome email to users not yet notified**.
   - To notify all users using the client who have not already been notified and are on a particular server, select **All users on this server** under **Send welcome email to users not yet notified**.
   - To notify a specific user, enter the name of the user to notify in the **User extension** field under **Send welcome email to this one user**.

4. Click **Send Email**.

14.7.4 Extension Lists

You can create extension lists for group paging and departmental auto-attendant.

1. Launch Connect Director with administrator privilege.
2. In the navigation pane, click **Administration** > **Features** > **Client** > **Extension Lists**. The **Extension Lists** page opens.
3. Do one of the following:

   - To edit an existing extension list, click the name of the extension list in the **List** pane.
   - To create a copy of an existing extension list, click **Copy**.
   - To create a new extension list, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays the parameters for the new or existing extension list.

4. In the **Name** field, enter a name for the extension list.
5. Do one of the following:

   - To add an extension to the extension list, select the extension in the **Available** list and click the right arrow button to move the extension to the **Selected** list.
   - To remove an extension from the extension list, select the extension in the **Selected** list and click the left arrow button to move the extension to the **Available** list.

6. Click **Save**.

Configuring User Features 15

This chapter contains the following sections:

This chapter is about setting up users in the MiVoice Connect system.

15.1 Configuring Private Extensions

A user's extension can be made private; private extensions are not listed in the System Directory or in Connect client Quick Dialer and thus have Caller ID information suppressed.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. In the **List** pane, select the user whose extension you want to make private.

Note:
The **General** tab in the **Details** pane displays parameters for the user.

4. Select the **Make extension private** check box.
5. Click **Save**.

15.1.1 Conditions for Private Extensions

The conditions for Private Extensions are as follows:

- The user's extension does not appear in the Connect client QuickDialer for dial-by-name operations, in the Directory Viewer, or in the History/Redial on the phone or in the client.

- Internal calls placed from a private extension show the caller's name but not their number to the dialed party. This applies to analog phones, IP phones, and associated instances of Connect client. The ring style is a double-ring, indicating an internal call.
- External calls placed from a private extension do not deliver a Direct-Inward-Dial (DID) number as Caller ID when PRI trunks are used for the outbound call. The proper CESID (Caller's Emergency Service ID) is only delivered for 911 calls.
- Calls placed from a private extension to an off-system extension on PRI trunks with NI-2 signaling deliver the caller's name but not their number.
- Routing slips and the client and History viewer show the name of the user with a private extension but their extension number is not shown.
- Users with a private extension are listed with name and number in the **Extension Monitor extension selection** dialog box.
- A private extension can be dialed directly from a telephone or the client if the extension is known.
- Contacts imported from Microsoft Outlook or Exchange that reference a user's private extension are not blocked and are fully visible in the client Quick Dialer.
- CDR database records show both number and name for users with a private extension. However, the Caller-ID Flags field indicates that only the name is valid.
- CDR legacy log files show the number of calls that are inbound or outbound for private extensions.
- Connect Director shows number information for users with private extensions as with other users. For example, the user's extension is displayed on the **Users** page.

15.2 Configuring Call History Privacy

The Mitel system tracks all call activity and places call detail records in a database on the server. The system uses these records to generate CDR reports. However, there are some situations that require calls not be tracked and that no records of calls be kept. For example, a high level executive may require that all calls from their phones are private and not tracked in the Mitel phone system.

Note:
The Call History Privacy feature only impacts call tracking within the Mitel phone system. Calls to external numbers may generate call records on the recipient's phone system and trunk calls may generate records with the carriers connecting the calls.

Call History Privacy provides users with an entirely private environment for their phones. When Call History Privacy is enabled, calls are not tracked or recorded in the call detail records. In addition, the calls are not available on the phone redial or shown in the Connect client call history.

Note:
Call History Privacy is not supported on SIP or Analog phones.

To use Call History Privacy, the user must be a member of a user group that has the Class of Service (COS) configured with the telephony feature Show call history disabled.

To configure COS permissions for Call History Privacy:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Do one of the following:
   - To create a new user group, click **New**.
   - To use an existing user group, click the name of that user group.
4. In the **COS - Telephony field**, click the **View Class of Service link**. The **Telephony Features Permissions** page for the associated COS is displayed.
5. Clear the **Show call history** check box.
6. Click **Save** to store your changes.

15.3 Configuring Extension Assignment

Extension Assignment is a feature of the MiVoice Connect system that allows a user to quickly and easily re-assign his or her extension to any telephone on or off the system. The user's communications profile is reassigned to that telephone, and calls placed to the user's extension are routed to that telephone. Calls placed from that telephone reflect proper caller ID information.

On-Network extension assignment can be used by the following types of users:

- Multi-site users, such as executives or managers, who might use the system across multiple locations. Extension Assignment allows these users to pick up a telephone at any location on the enterprise network, log into voice mail, and assign their extension to that telephone.
- Office hotel users, such as contractors or telecommuters, who may occasionally be out of the office or who might share a cubicle, and thus a phone, with another employee. Extension Assignment allows these users to have their own extension and mailbox, yet not have a dedicated switch port. They can simply assign their extension to a telephone on the network when they are in the office while allowing another user to usurp that phone when they are done with it.

- Remote or mobile users, such as employees in sales or support, who might travel frequently and would like to have all calls directed to their cell phone or home office PSTN phone. Extension Assignment allows these users to have their own extension and mailbox, yet not have a dedicated switch port, thus optimizing system resources.
- Legacy PBX Users, such as users with Off-System Extensions working with Connect client.

Extension Assignment also allows the system administrator to configure all telephones as anonymous telephones and all users as virtual users, eliminating administrative costs associated with frequent moves. When a move occurs, users simply assign their extension to the telephone at the new location.

For information about configuring on-network extension assignment, see Configuring On-Network Extension Assignment on page 554.

Using off-network extension assignment, a user can manage a call via the client. So while the conversation occurs over a cell phone or home phone, the call appears via the client and can be controlled using many of the features available via the client. Note that this requires the user to be located near a PC that is running the client and has access to a broadband connection. For information about configuring off-network extension assignment, see Configuring Off-Network Extension Assignments on page 553.

Other benefits of off-network extension assignment include:

- Use the existing PSTN line for voice while managing the call via the client over an ordinary broadband Internet connection.
- Emulate analog extension hook switch actions via star-star (**) for FLASH and pound-pound (##) for on-hook/off-hook.
- Access the user's directory numbers at the office.
- The user appears to be calling from the office.
- Keep communication costs minimized with flexible IP and trunking requirements.
- Retain call management features of the MiVoice Connect system over a broadband connection while maintaining audio quality over PSTN.

15.3.1 Special Considerations for Extension Assignment

- When an Extension Assignment call finishes but the carrier has not reported back to the MiVoice Connect system that the far side has disconnected, the call remains active for approximately five seconds before it is finally disconnected. To initiate a new call during the five-second window, the user can press ##.
- To use the Extension Assignment feature, the user must be a member of a user group that has the Class of Service (COS) configured with the telephony feature Allow extension reassignment enabled. For information on the Telephony COS settings, see Configuring a COS for Telephony Features Permissions on page 461.
- Mitel supports up to 1,000 virtual users.

- When a user's extension has been assigned to an off-net location, incoming calls ring the off-system extension. If the call is not answered, normal call routing allows the caller to leave a message in the user's Mitel mailbox.
- When assigned to an off-net location, Extension Assignment is fully controllable through Connect client excluding answering a call, which must be done manually. In addition, Extension Assignment has limited TUI functionality.
- Extension Assignment calls that are terminated through Connect client are not followed by the standard dial tone. Extension Assignment uses a unique set of internal and external dial tones. This difference in tones can be important in installations where network devices have been configured to listen for normal class progress tones before taking action on a call, such as hanging up.
- Calls placed or answered through Extension Assignment, when assigned to an off-net location, continue to exist in the Connect client call stack. Normal call control functions, such as hold, unhold, conference, transfer, and park, continue to work. In contrast, Park to the Extension Assignment extension is not supported when it is assigned to an off-network location.
- Extension Assignment, when assigned to an off-net location, behaves like an automated Find Me feature except that the caller does not press 1 to find the called party. The PSTN phone number is immediately called. The call recipient can answer the call by lifting the handset, or activating a cell phone, and pressing the DTMF digit **1** in response to the repeating prompt.
- For off-net Extension Assignment, prompts can be used to confirm answering. The answer style can be configured to be one of the following:
  - **Wait for DTMF** (default) - The call is not forwarded until the user presses 1.
  - **Wait for Answer** - The MiVoice Connect system forwards the call as soon it detects the far-end answer.

Note:

For some trunk types, a central office might not support answer-detection at the far end. In this case, the user would have to press **1**. The caller can hear the DTMF tone in this case.

15.3.1.1 Terminology

The terms used to describe Extension Assignment are as follows:

- Anonymous telephone: A telephone not currently assigned a user. You can make a call from an anonymous telephone, but you cannot call an anonymous telephone.
- Any IP Phone: The feature that lets a user assign his or her extension to any IP phone on the enterprise network.

- Assign: The command that assigns an extension to a telephone.
- Assigned: The status of a user who is currently assigned to a telephone that is not their home phone.
- Current telephone: The telephone to which the user is currently assigned, which is also known as the current switch port.
- Go Primary Phone: The command to assign a user's extension back to his or her primary telephone.
- Home: The status of a user who is assigned to his or her primary telephone.
- Home telephone: The telephone to which the user is normally assigned, which is also know as the primary phone port. This is the telephone to which the user returns when using the Go Primary Phone command.
- Extension Assignment: The feature that lets a user assign his or her extension to any telephone, on-system or off-system extension.
- Unassign: The command that unassigns an extension from a telephone.
- Vacated phone: A home telephone that currently does not have a user assigned. Vacated phones are listed on the Vacated Phones page in Connect Director.
- Virtual user: A user who does not have a physical telephone port and is currently assigned to the SoftSwitch.

15.3.2 Configuring COS Permissions for Extension Assignment

To use the Extension Assignment feature, the user must be a member of a user group that has the Class of Service (COS) configured with the necessary telephony feature permissions.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Do one of the following:
   - To create a new user group, click **New**.
   - To use an existing user group, click the name of that user group.
4. In the **COS - Telephony** field, click the **View Class of Service** link. The Telephony Features Permissions page for the associated COS is displayed.
5. Select the **Allow Extension Reassignment** check box.
6. Select the **Allow External Call Forwarding and Find Me Destinations** check box, and then select the appropriate **Scope** radio button.
7. Click **Save** to store your changes.

15.3.3 Configuring Off-Network Extension Assignments

Extension Assignment is intended for remote users who often work outside the office. Users that travel frequently or work from home can have all calls directed to an off-network device, such as a cell phone or home office PSTN phone. Extension Assignment allows a user to have a Mitel extension and mailbox without requiring a dedicated switch port and physical telephone in the office.

Note:

For an off-network phone to display the ID of a caller who is outside a Mitel site, the system administrator must activate the Enable original caller information feature on applicable trunk groups. Refer to Forwarding Original Caller ID Outside a Mitel Network on page 258 for additional information.

This section provides information about how to assign an external phone number.

1. Launch Connect client on the client machine. The dashboard is displayed.
2. Click the **<username> tab**. The profile information is displayed on the second pane.
3. Click the **Select Number** drop-down list below the external assignment number option. The **Select Number** screen is displayed.

Note:

If the **Select Number** option is not displayed, contact system administrator.

4. Type a name in the **Label** field. For example, Home or Mobile.
5. Enter the associated phone number in the **Number**field. You cannot use a phone number that is assigned to Connect for iOS or Android.
6. To connect to the external number, click the drop-down list and choose any of the following:
   - **Automatically connect**
   - **Press 1 to connect**
7. In the **rings to try field**, increment or decrement to select a number.

Note:

This number determines the number of rings to the external phone number before forwarding the call to your voicemail.

8. Select a number that you have defined as an external number.
9. Click Use **Selected Number** to save the number. The user's extension is assigned to the selected phone.

15.3.4 Configuring On-Network Extension Assignment

On-network extension assignment is intended for users who travel frequently and require access to the MiVoice Connect system from multiple sites on the network. Users can assign their extension to any telephone on the Mitel network using the voice mail menu.

You can assign or unassign an extension to any on-network telephone using the voice mail Telephone User Interface or using the client. Refer to Managing Inbound Calls on page 555 for information about assigning and unassigning extensions using the client.

15.3.4.1 Configuring Extension Assignment Using the Telephone User Interface

Assigning an Extension to a Telephone

1. Log in to voice mail.

Note:

If the phone is already assigned, you will need to press **#** twice; once to log in to voice mail and then again at the prompt.

2. Press **7** to select **Change Mailbox Options**.
3. Press **3** to select **Re-assign Extension**.
4. Press **1** to select **Assign**.
5. Wait for a dial tone, and then hang up.

This option is available only from telephone ports and is not available from trunk ports.

15.3.4.1.1 Unassigning an Extension from a Telephone

1. Log in to voice mail.
2. Press **7** to select **Change Mailbox Options**.
3. Press **3** to select **Re-assign Extension**.
4. Press **2** to select **Unassign**.
5. Wait for a dial tone, and then hang up.

If no other user is assigned to the primary phone port, the extension automatically reverts back to the primary phone. If another user is assigned to the primary phone port, the extension is assigned to the SoftSwitch until the primary phone port becomes available. A user can remove the other user from the primary phone port by assigning the extension from their primary phone using the procedure above.

15.4 Managing Inbound Calls

15.4.1 Routing Calls to Other Phones

The following features are available for routing calls to additional phones:

- The **Ring Additional Phones** feature routes incoming calls to a user's primary phone and up to two additional phones simultaneously. You can choose the availability states that initiate this action.
- The **Find Me** feature routes incoming calls to additional phones, in a specified order, when callers reach a user's voice mail. You can choose the availability states that initiate this action.

The **Find Me** feature routes inbound calls to a specified extension or external number as an alternative to sending calls to voice mail. Two separate Find Me destinations can be configured for each user. Find Me can be enabled for one or all availability states.

Note:

To use the Find Me feature, the user must be a member of a user group that has the Class of Service (COS) configured with the telephony feature **Allow external call forwarding and find me destinations** enabled. For information on the Telephony COS settings, see Configuring a COS for Telephony Features Permissions on page 461.

To initiate **Find Me**, a caller presses **1** while listening to the recipient's voice mail greeting. The caller hears a message that the Find Me destinations are being called and the call is then routed to the first Find Me destination. If the call is not answered, it is then routed to the second Find Me destination. Calls not answered at either Find Me destination are sent to voice mail.

Note:

The standard voice mail greeting does not prompt the caller on the availability of Find Me; the user should record a custom message to prompt callers when Find Me is available.

You can also choose to automatically route calls to Find Me destinations without requiring the user to press **1**. See Configuring Ring Additional Phones on page 557 for more information.

When a call is forwarded to a Find Me destination, the phone at the Find Me destination displays the recipient's voice mail caller ID to the caller. When answering a call, the recipient hears a prompt announcing the call and, if available, the caller's caller ID information. The recipient can then accept the call or route the call to voice mail.

15.4.1.1 Configuring Additional Phones

Before enabling the Ring Additional Phones or Find Me feature, you must configure the additional phones available for routing calls to. You can configure a mobile phone, home phone, and up to five additional phones for use with the Ring Additional Phones and Find Me features.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. In the **List** pane, select the user to configure additional phones for.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing user.

4. Select the **Routing tab**, and then select the **Phones** subtab.
5. Review the parameters and specify values as appropriate. For descriptions of the Phones parameters, see the following table.

Table 128: Users Page: Routing Tab, Phones Subtab

Parameter	Description
Label	Specifies the label used to refer to the additional phone.
Phone number	Specifies the telephone number.
Activation	In the drop-down list, select the action required to accept a call on this phone. • **Accept call by pressing '1'** requires the call recipient to press 1 to accept the call after the caller information is announced. • **Accept call by answering** requires the call recipient to only pick up the phone in order to accept the call. **Note**: This parameter applies for External Assignment only.
Number of rings (1-20)	Specifies the number of times to ring this phone before sending the call to the next step.

15.4.1.2 Configuring Ring Additional Phones

Before enabling the Ring Additional Phones or Find Me feature, you must first configure the additional phones available for routing calls to. For information about configuring additional phones, see Configuring Additional Phones on page 556.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. In the list pane, select the desired user.

Note:
The **General** tab in the **Details** pane displays parameters for the selected user.

4. Select the **Routing** tab, and then select the **Ring Me** subtab.

5. Review the parameters and specify values as appropriate. For descriptions of the Ring Me parameters, see the following table:

Table 129: Users Page: Routing Tab, Ring Me Subtab

Parameter	Description
Incoming calls ring	In the drop-down list, select the phone to initially route all incoming calls to.
Ring Additional Phones	
When my Availability State is	Select the check box next to each of the availability states that you want to initiate Ring Additional Phones.
Ring delay	In the drop-down list, select the desired ring delay option. • **None** - to start ringing the phone audibly on the first ring. • **1, 2, 3, or 4** - to ring the phone silently for the selected number of rings before ringing phone audibly. • **Don't Ring** - to not ring the phone audibly.
Simultaneously ring	In the drop-down list, select the additional phone to ring simultaneously fo r incoming calls.
Also ring	In the drop-down list, select a second additional phone to ring simultan eously for incoming calls.
Find Me	
When callers reach my voice mail and my Availability State is	Select the check box next to each of the availability states that you want to initiate Find Me.
Find me at the following phones	
First phone	In the drop-down list, select the first phone to route Find Me calls to.
Second phone	In the drop-down list, select the second phone to route Find Me calls to (in case the recipient is not reached on the first phone).
Send incoming caller ID	Select this check box to enable caller ID for incoming Find Me calls.

Parameter	Description
Enable record caller's name for Find Me	Select this check box to prompt callers to record their name; the recording is played to the call recipient when confirming an incoming call. **Note**: When this check box is selected and the Record name even if caller ID is present is cleared, callers are only prompted to record their name if their caller ID information is not available.
Record name even if caller ID is pre sent	Select this check box to prompt callers to record their names for playback when confirming an incoming call even when caller ID information is avail able.
Enable Find Me for incoming calls be fore playing greeting	Select this check box to automatically route incoming calls to Find Me destinations whenever a call reaches the recipient's voice mail. When this check box is selected, the caller is not required to press **1** to initiate **Find Me**. **Note**: If this check box is selected, ensure that the user's outgoing voice mail message does not tell callers to press **1** to activate the **Find Me** feature.

15.4.2 Configuring Availability States

Availability states specify how, when, and where calls are forwarded, and whether the user requires message notification when a voice mail is received. You can set the Availability States defaults to apply to each new user and you can edit the availability state options for each existing user individually. Users can also modify their availability state options from their desktop client applications or through a web interface on the server. For details and the web URL, refer to the *MiVoice Connect Planning and Installation Guide*.

Mitel defines the following availability states:

- Available
- In a Meeting
- Out of Office
- Do Not Disturb
- Vacation
- Custom

One availability state is always active for each user. By default, Mitel automatically selects the active availability state based on system schedules maintained by the system administrator and the state of the user. Users can also manually select their active availability state. For information about system schedules, see Overview on page 621.

15.4.2.1 Configuring the Availability States Defaults

The Availability States Defaults are the set of availability state parameters assigned to a new user each time a new user is added to the MiVoice Connect system. Mitel strongly recommends that you review and change these defaults before adding the bulk of your users.

Once a user is saved to the system, there is no relationship between the user's availability states and the default availability states. Changes to the default availability states do not affect the availability states of existing users.

You configure parameters for each availability state on the following tabs on the **Availability States Defaults** page:

- **Available**
- **In a Meeting**
- **Out of Office**
- **Vacation**
- **Custom**
- **Do Not Disturb**

Note:

You can change the Personal Assistant for some or all users using the bulk edit feature. For more information about bulk editing, see Bulk Edit on page 540.

To configure availability states for a user:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Availability States Defaults**. The **Availability State Defaults** page is displayed.
3. Review the parameters on each of the availability state tabs, and specify values as appropriate. For more information about the parameters on the availability state tabs, see the following table.

Table 130: Availability State Defaults

Parameter	Description
Call forward condition	Select one of the following options for forwarding calls for the selected availability state: • **Always** automatically forwards all calls to the user's voice mail. • **No Answer/Busy** forwards the call to the user's voice mail if the line is busy or the call goes unanswered after the specified number of rings. • **Never** disables call forwarding. The recommended default is **No Answer/Busy**. **Note**: Call forward destinations cannot be specified for availability state defaults; all calls are forwarded to the user's voice mail box. See Routing Calls to Other Phones on page 555 for information about specifying different call forward destinations for individual users.

Parameter	Description
Forward after (1-20) rings	Specifies the number of times a call rings a line before it is forwarded to a configured extension. **Note**: • This option is available only when the **Call forward** condition is set to **No Answer/Busy**. • For UK and India, the call is forwarded to a configured extension after N*2 rings if **Forward after (1-20) rings** option is configured with N under the Availability state configuration.
Personal assistant	Specify the extension of the personal assistant. The personal assistant is the u ser that calling parties are routed to when they dial 0 in a user's mailbox.
Enable Find Me	Select this check box to enable the Find Me feature by default. For more informa tion about the Find Me feature, see Configuring Ring Additional Phones.
Enable message notification	Select this check box to enable message notification. The manner in which the user is notified is determined by the user's message notification settings.
Enable calling additional phones	Select this check box to enable the Ring Additional Phones feature by default. F or more information about the Ring Additional Phones feature, see Configuring Ring Additional Phones.
Do not record voice messages, only play greeting	Select this check box to enable the voice mail server to play a greeting and then disconnect the call, without taking a message. When this mode is enabled, the voice mail server issues the following prompt: No messages may be taken for this mail box.

Parameter	Description
Schedule	In the drop-down list, select the schedule to associated with the selected availability state. For example, you might want to associate the **Available** availability state with a schedule that is active from the hours of 9 a.m. to 5 p.m., and associate the **Custom** availability state with a graveyard schedule that is active from the hours of 10 p.m. to 6 a.m. For more information about system schedules, see Overview on page 621. **Note**: This parameter does not apply to In a Meeting, Out of Office, or Do Not Disturb availability states.
View schedule	Click this link to view the selected schedule.

15.4.2.2 Configuring Availability States for Individual Users

You can edit the availability state options for each existing user individually. Users can also modify their availability state options from their desktop client applications or through a web interface on the Mitel server. For details and the web URL, refer to the *MiVoice Connect Planning and Installation Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

You configure parameters for each availability state on the following Availability States subtabs, located on the Routing tab on the **Users** page:

- **Available**
- **In a Meeting**
- **Out of Office**
- **Do Not Disturb**
- **Vacation**
- **Custom**

To configure availability states for a user:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.

3. In the **List** pane, select the desired user.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the selected user.

4. Select the **Routing** tab, and then select the **Availability States subtab**.
5. Review the parameters on each of the availability states subtabs, and specify values as appropriate.

> **Note**:
> For more information about the parameters on the availability state subtabs, see Users Page: Routing Tab, Availability State Subtab.

Table 131: Users Page: Routing Tab, Availability State Subtab

Parameter	Description
Current availability state	To manually select the availability state to apply to the user, select the d esired availability state in the drop-down list.
Availability state synchronized with cal endar status (Supports on MS Outlook and Gmail calendar)	Select this check box to enable a user's Microsoft Outlook Calendar to c ontrol his or her availability state.
Note	Enter the text to display for the custom availability state. **Note**: This parameter is only available for the Custom availability state.

Parameter	Description
Color	Select one of the following color options to display for the custom availability state: • **Green** - Available • **Yellow** - Busy • **Red** - Not Available **Note**: This parameter is only available for the Custom availability state.
Call forward condition	Select one of the following options for forwarding calls for the selected availability state: • **Always** automatically forwards all calls to the specified destination. • **No Answer/Busy** forwards the call to the specified destination if the line is busy or the call goes unanswered after the specified number of rings. • **Never** disables call forwarding.
Forward after (1-20) rings	Specifies the number of times to ring the line before forwarding the call. **Note**: This option is available only when the **Call forward** condition is set to **No Answer/Busy**.

Parameter	Description
Always destination	Specifies the destination for forwarded calls. The destination can be an extension or an external number. If the destination is an external number, the access code must be included. **Note**: This option is available only when the **Call forward condition** is set to **Always**.
Busy destination	Specifies the destination for forwarded calls when the line is busy. **Note**: This option is available only when the **Call forward condition** is set to **No Answer/Busy**.
No answer destination	Specifies the destination for forwarded calls when a call goes unanswered after the specified number of rings. **Note**: This option is available only when the **Call forward condition** is set to **No Answer/Busy**.

Parameter	Description
When caller presses ‘0’, transfer to	Specifies the assistant extension. When a caller connects to a user’s voice mail and presses **0**, the call is forwarded to the specified extension. **Note**: If no extension is defined and a caller presses **0**, the call is transferred to the site operator. If no site operator is defined, the call is transferred to the auto-attendant.
Enable message notification	Select this check box to enable message notification. The manner in whic h the user is notified is determined by the user’s message notification sett ings.
Do not record voice messages, only p lay greeting	Select this check box to enable the voice mail server to play a greeting and then disconnect the call, without taking a message. When this mode is enabled, the voice mail server issues the following prompt: No messag es may be taken for this mail box.
Schedule Mode change	In the drop-down list, select the schedule to associated with the selected availability state. For example, you may want to associate the **Available** availability state with a schedule that is active from the hours of 9am to 5pm, and associate the **Custom** availability state with a graveyard schedule that is active from the hours of 10pm to 6am. For more information about system schedules, see Overview on page 621. **Note**: This parameter does not apply to In a Meeting, Out of Office, or Do Not Disturb availability states.
View schedule	Click this link to view the selected schedule.

Parameter	Description
Voice mail escalation profile	In the drop-down list, select the escalation profile for the selected availability state. For more information about escalation profiles, see Configuring Escalation Notification on page 597.
View users Escalation Profiles	Click this link to view the selected user's escalation profile.

15.4.2.3 Configuring Availability State Delegation

The Availability State Delegation window lets the system administrator specify a list of users who can change the Availability State of another user. A delegated or authorized user with an Operator Access License can modify another user's Availability State through Connect client or Connect client for Web Client. These authorized or delegated users are specified through Connect Director by the system administrator or through Connect client by the user whose active availability state is changed.

15.4.2.3.1 Delegating through Connect Director

Selecting the users who are authorized to change another user's active availability state:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. Select the user for whom you are authorizing other users to change the active availability state.

Note:
The **General** tab in the **Details** pane displays parameters for the selected user.

4. Click the **Membership** tab, and then click the **Delegation** subtab.
5. Do one of the following:

   - To add a user to the list of users authorized to change the availability state for the selected user, select the user to authorize in the **Available** list and click the right arrow button to move the user to the **Selected** list.
   - To remove a user from the list of users authorized to change the availability state for the selected user, select the user in the **Selected** list and click the left arrow button to move the user to the **Available** list.

6. Click **Save**.

15.4.2.3.2 Selecting Delegates through Connect Client

Users can manage the list of individuals who can change their active availability state through the client. The *Mitel Connect Client User Guide* contains more information.

15.4.3 Configuring Power Routing Rules

Power Routing rules specify the call routing method for incoming calls to a user's phone number. Calls are forwarded based on specific criteria, such as the incoming phone number, the number the caller dialed to reach the user, the user's availability state, as well as the time of day or day of week the call is received.

Power Routing is available to users with one of the following Access Licenses:

- Connect Client
- Operator
- Workgroup Agent
- Workgroup Supervisor

Note:

Administrator authorization is not required for users with one of these Access Licenses.

Each user can have a maximum of 10 Power Routing rules. These rules can be enabled or disabled and organized according to priority.

Before a user actually receives the inbound call, the system evaluates the call conditions against the highest priority Power Routing rule that is enabled. If all of the criteria in the rule match the call conditions, the call is routed according to the rule's action. If any of the criteria do not match the call conditions, the system continues the plan execution by evaluating the call against the next highest priority Power Routing rule that is enabled.

This process is repeated for all enabled Power Routing rules. If the call conditions do not match the conditions of any of the enabled Power Routing rules, the call is routed according to the user's active availability state.

15.4.3.1 Creating Power Routing Rules

Power Routing rules specify the call routing method for incoming calls to a user's phone number. Calls are forwarded based on specific criteria, such as the incoming phone

number, the number the caller dialed to reach the user, the user's availability state, as well as the time of day or day of week the call is received.

Power Routing is available to users with one of the following Access Licenses:

- Connect Client
- Operator
- Workgroup Agent
- Workgroup Supervisor

Note:

Administrator authorization is not required for users with one of these Access Licenses.

Each user can have a maximum of 10 Power Routing rules. These rules can be enabled or disabled and organized according to priority.

Before a user actually receives the inbound call, the system evaluates the call conditions against the highest priority Power Routing rule that is enabled. If all of the criteria in the rule match the call conditions, the call is routed according to the rule's action. If any of the criteria do not match the call conditions, the system continues the plan execution by evaluating the call against the next highest priority Power Routing rule that is enabled.

This process is repeated for all enabled Power Routing rules. If the call conditions do not match the conditions of any of the enabled Power Routing rules, the call is routed according to the user's active availability state.

15.4.3.2 Viewing Power Routing Rules

The **Power Routing Rules** subtab, located on the **Routing** tab of the **Users** page in Connect Director, lists the Power Routing rules created by the selected user. The name, condition, action, and status of each rule is displayed. The rules appear in the order that the user created them, not according to the priority specified by the user in the Connect client. Therefore, you cannot determine priority by viewing Power Routing rules in Connect Director.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page is displayed.
3. In the **List** pane, select the user whose Power Routing Rules you want to view.

Note:
The **General** tab in the **Details** pane displays parameters for the selected user.

4. Select the **Routing** tab, and then select the **Power Routing Rules** subtab.

15.5 Monitoring Extensions from an IP Phone

Extension monitoring allows a user to monitor the extension of another user and answer calls on the other user's extension, if necessary. For example, two assistants are working on different floors of the same building and are both responsible for answering calls from the main phone line. With extension monitoring enabled, if one assistant is on a call when another call arrives on the main line, the other assistant can see that the first assistant is busy and, therefore, knows to answer the incoming call.

Extension monitoring is enabled by configuring a programmable phone button on the monitoring party's phone with the Monitor Extension feature. The Monitor Extension button can be configured for multiple functions, depending on the status of the monitoring party's phone.

15.5.1 Configuring Extension Monitoring

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Programmable Buttons**. The **Users Programmable Buttons** page is displayed.
3. In the **List** pane, click the name of the user to configure extension monitoring for.

Note:
The **IP Phone Buttons** tab in the **Details** pane displays parameters for the selected user.

4. Select the one of the following tabs:
   - **IP Phone Buttons** - to configure extension monitoring on a phone or button box.
   - **Client Toolbars** - to configure extension monitoring from a client toolbar.
5. Select the subtab for the device or toolbar the user will use to monitor another extension.
6. In the **Function** column for the button to configure, select **Monitor Extension**. The extension monitoring options are displayed.

7. In the **Long Label** and **Short Label** fields, enter a label to appear next to the button on the phone or button box LED display to remind the user of the button's function.

> **Note**:
> For details, see Configuring Programmable Buttons through Connect Director on page 333.

8. In the **Extension** field, enter the extension you want the user to monitor.
9. In the **Ring delay before alert** list, select one of the following:

   - **None** - to start ringing the phone audibly on the first ring.
   - **1, 2, 3,** or **4** - to ring the phone silently for the selected number of rings before ringing the phone audibly.
   - **Don't Ring** - to not ring the phone audibly.

10. Under **Show caller ID on monitored extensions**, select one of the following:

    - **Never** - to not show caller ID for inbound calls on the monitored extension.
    - **Only when ringing** - to show caller ID for inbound calls on the monitored extension only when the phone is ringing.
    - **Always** - to show caller ID for inbound calls on the monitored extension when the phone is ringing and as long as the call is connected.

11. To assign a secondary function to the phone button, select the desired function under **No connected call action**.

> **Note**:
> This secondary function applies when the button is pressed while the monitoring party's phone is not on an active call.

12. To assign a tertiary function to the phone button, select the desired function under **With connected call action**.

> **Note**:
> This tertiary function applies when the button is pressed while the monitoring party's phone is on an active call.

13. Click **Save**.

15.5.2 Extension Monitoring Details

The following list includes further details about extension monitoring:

- IP480, IP480g, and IP485g phones support only one custom button per monitored extension. If you designate more than one custom button on a particular phone to monitor the same extension, the specifications are ignored and the additional monitor extension buttons are converted to regular call appearance buttons. Connect Director does not reflect this change.
- For SIP 6.0 and earlier versions, on 6900-Series (6920, 6930, and 6940) phones, press the programmable button twice to pick up a Monitored Extension call. With the first button press, the CallerID is displayed; and with the second button press, you can answer the call.
- For SIP 6.1 and later versions, on 6900-Series (6920, 6930, and 6940) phones, press the corresponding programmable button once to pick up a Monitored Extension call.

Note:
Currently, 6900-Series phones allows you to designate more than one custom button on a particular phone to monitor the same extension. However, this results in incorrect functionality on the phone.

- The Monitor Extension button can be configured for multiple functions, depending on the status of the monitoring user's phone.
  - When there is an incoming call on the monitored extension, pressing the Monitor Extension button answers the incoming call.
  - When there is no active call on the monitoring user's phone, pressing the Monitor Extension button initiates the action configured for the No connected call action parameter (see table below for more information).
  - When there is an active call on the monitoring user's phone, pressing the Monitor Extension button initiates the action configured for the With connected call action parameter (see table below for more information).
- The Monitor Extension button shines red when the user whose extension is being monitored is on a call. If that call is put on hold and a second call is accepted on the monitored extension, the LED turns green and flashes twice. Similarly, the LED flashes three times if a third call is accepted. For information about LED flash patterns, see the following table.
- When **Show caller ID name and number for other extensions** is not enabled for the COS telephony permissions, Connect client Contact Viewer (and Agent Viewer) show the number of calls on a user's stack but do not show who the user is talking to. Properties is also disabled.

Table 132: Programmable Buttons LED Flash Patterns

State	Pattern
CALL APPEARANCE STATES	
Idle	Off
Idle and DND	Orange, Steady On
Idle and Message Waiting	Off
Idle, Message Waiting and DND	Orange, Steady On
Off Hook	Green, Steady On
Active Call	Green, Steady On
Active Conference Call	Green, Steady On
Remote Hold	Green, Steady On
Offering Call	Green, 1000/1000 ms
Active Call Whisper Muted	Red, Steady On
EXTENSION MONITOR STATES	
Idle	Off
Idle and DND	Orange, Steady On
Idle and Message Waiting	Off
Idle, Message Waiting and DND	Orange, Steady On
Held or Parked Call [3]	Orange, 250/250 ms
Monitored Ext. on Active Call	Red, Steady On
Monitored Ext. on Conference Call	Red, Steady On
Monitored Ext on Active Call + Offering Call	Green, 200/100/700/1000 ms
Picked up Monitored Ext. Call + Monitor Ext on Active Call	Green, 800/Orange 200 ms
Picked up Monitored Ext. Call and Held + Monitor Ext on	Active Call, Orange, 200/100/200/500 ms
Picked up Monitored Ext. Call + Monitor Ext held Active Call	Orange, 200 msGreen, 800 msOrange, 200 msGre en, 100 ms
BRIDGED CALL APPEARANCE STATES	
Idle	Off
Offering Call	Green, 1000/1000 ms
Active Call Picked Up	Green, Steady On
Line In-Use	Red, Steady On
Held or Parked Call [3]	Orange, 250/250 ms
FEATURE KEY WITH EXTENSION TARGET STATES	
Idle or Offering Call	Off
Connected or Held Call	Red, Steady On
DND	Orange, Steady On
(Dial/Transfer Mailbox Only) MWI	Red, Steady On
(Pickup, Pick/Unpark, Pickup NightBell Only) Offering	Green, 1000/1000 ms

State	Pattern
(Unpark, Pick/Unpark Only) Held/Parked	Orange, 250/250 ms
TOGGLE FUNCTIONS (RECORD, WHISPER MUTE)	
Function Off	Off
Function Available	Orange, Steady On
Record Active	Orange, 500/500 ms
Whisper Mute Active	Orange, 500/500 ms

15.6 Configuring Call Intervention Methods

Call intervention methods allow users to intervene in the calls of other users. In order to use a call intervention method, both the initiating user and the receiving user must be a member of a user group that has the Class of Service (COS) configured with the appropriate permissions.

Note:
A user must also have an access license of Workgroup Supervisor or higher to record the calls of other users.

A COS can be configured to allow initiation for call intervention and to accept call intervention of the following types:

- Directed intercom
- Whisper paging
- Barge-in
- Record calls
- Silent monitor/Silent coach

To configure call intervention methods for a COS:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Class of Service** > **Telephony Features Permissions**. The **Telephony Features Permissions** page is displayed.
3. Click the name of the COS profile to configure call intervention methods for.

Note:
In the **Details** pane, the **Telephony Features Permissions** page for the selected COS is displayed.

4. Specify the call intervention permissions, as described in the following table.

Table 133: Telephony Features Permissions: Call Intervention Methods

Parameter	Description
Directed intercom: Allow initiation	Enables the Directed Intercom feature.
Directed intercom: Accept	Specifies whether users can receive intercom calls or pages. Select one of the following options: • **None** means that users cannot receive intercom calls or pages. • **All** means that users with this permission can receive intercom calls or pages from anyone with this class of service. • **Only From** means that users with this class of service may receive intercom calls or pages from only the person or extension specified in the associated field.
Whisper Paging: Allow Initiation	Enables a user to place a whisper page call. For more information about whisper paging, see Whisper Paging on page 580.

Parameter	Description
Whisper Paging: Accept	Specifies whether users can receive whisper page calls. Select one of the following options: • **None** means the user with this COS cannot receive whisper page calls. • **All** means the user with this COS can receive whisper page calls from all users. • **Only From** means the user with this COS may receive whisper page calls only from the specified user.
Barge-in: Allow initiation	Enables users to barge in on other users' calls. **Note**: Barge-in permits one party to join an existing call as a fully conferenced participant. When barge-in is initiated, a brief intrusion tone is played to the other participants and (if present) the monitor/record warning tone is discontinued.

Parameter	Description
Barge-in: Accept	Specifies whether users' calls can be barged-in upon. Select one of the following options: • **None** means that users with this class of service may not receive barge-ins from anyone. • **All** means that users with this class of service may receive barge-ins from anyone else in this class of service. • **Only From** means that users with this class of service may receive barge-ins only from the person or extension specified in the field associated with this option.
Record other's calls: Allow initiation	Enables users within this class of service to record the calls of other system users. For example, a supervisor could record the call of an agent. The Selectable Mailboxes feature allows recorded calls to be automatically placed into mailboxes other than the mailbox of the user who recorded the call. For more information, see Overview on page 284. When you record another user's call, the system plays a warning tone. To disable the tone, see Configuring Call Control Options on page 427.

Parameter	Description
Record other's calls: Accept	Specifies whether users within this class of service may have their calls recorded by other users. Select one of the following options: • **None** means that users within this COS may not have their calls recorded by anyone. • **All** means that users within this COS may have their calls recorded by anyone else in this COS. • **Only From** means that users within this COS may have their calls recorded only by the person or extension specified.
Silent monitor/Silent coach other's calls: Allow initiation	Allows a supervisor to monitor a phone call of a user an d to speak to the user without the other party hearing.
Silent monitor/Silent coach other's calls: Accept	Specifies whether users within this class of service may have their calls recorded by other users. Select one of the following options: • **None** means that users within this COS may not have their calls silently monitored or be silently coached during a call by any other system user. • **All** means that users within this COS may have their calls silently monitored or be silently coached during a call by any other user in this class of service. • **Only From** means that users within this COS may have their calls silently monitored or be silently coached during a call only by the person or extension specified.

15.6.1 Directed Intercom

A user can initiate an intercom call through a programmable button on an IP phone, through Connect client, or through phone by entering ***15** + extension number. For more information about the Intercom feature, see the *MiVoice Connect Planning and Installation Guide*.

As an alternative to using an in-house paging system, you can broadcast a message to a group of phones using the paging groups feature. For more information about paging groups, see Configuring Paging Groups on page 403.

15.6.2 Whisper Paging

The Whisper Page feature allows a user to break into an active call in order to speak with an internal user. This occurs without the remote caller hearing the interruption and without the operator hearing the remote caller.

A real-world example illustrates the function: You are on a call with a client when another client arrives in the lobby for an appointment with you. The administrative assistant knows that you are on a call and uses the Whisper Page feature to interrupt the call to announce that someone is waiting for you in the lobby. You hear the voice of the administrative assistant and the client at the same time, but neither of them can hear the other.

Implementation details:

- The Whisper Page feature can be invoked from:
  - Connect client
  - Any phone (analog or IP) by pressing the code *19
  - One of the IP Phone soft keys
- While on a Whisper Page call, the internal user can mute the audio channel to the original caller. The user can respond to the operator without the original caller hearing. This can be accomplished from:
  - One of the IP Phone soft keys, rather than the standard mute button
  - Connect client, if you do not have an IP phone
- Both the operator and the internal user hear a tone when the Whisper Page call is connected. The tone is the same as the tone for the Intercom feature.
- To receive a Whisper Page call, the internal user must be on the handset of a multiline IP Phone. If a Whisper Page call is sent to any other phone (SoftPhone), the call will be treated as an intercom call.
- If a Whisper Page call is sent to a phone that is not on an active call, the feature behaves the same as an intercom call.

- The Whisper Page feature does not work if the internal party is on a three-way conference call.
- No call control operations can be performed on a Whisper Page call, except to hang up the call. For example, the Whisper Page call cannot be put on hold, transferred, parked, and so on.

15.6.3 Barge-In

Barge-in allows a user to join an existing call as a fully conferenced participant. When Barge-in is initiated, a brief intrusion tone is played to the other participants and, if present, the monitoring warning tone is disabled.

A supervisor can barge in to a call he or she is currently monitoring. However, it is not possible to revert a barge back to a monitored call. If desired, the supervisor can hang up the call and restart monitoring.

The original controlling party of a call remains the controlling party even after a barge-in. A subsequent agent hook flash disconnects the supervisor, who was the last party added.

15.6.4 Recording Calls

The MiVoice Connect system provides the capability for users to record calls. For more information about call recording, see the *MiVoice Connect Planning and Installation Guide*.

Note:

A user must have an access license of Workgroup Supervisor or higher to record the calls of other users.

A warning tone is normally played to call participants when the call starts being monitored or recorded. However, silent monitoring and recording allows operators and supervisors to hide the fact that they are monitoring or recording calls by not playing a warning tone. For more information about silent monitoring and recording, see Silent Monitoring and Recording on page 437.

15.6.5 Silent Monitor

Monitoring allows a supervisor to monitor a user's calls. The supervisor hears the other call participants, but they do not hear the supervisor. Monitoring is undetectable by the parties being monitored, except for an optional warning tone. Monitoring is typically used

in workgroups to evaluate agent performance. For information about enabling the silent monitor warning tone, see Silent Monitoring and Recording on page 437.

In a monitored call, a supervisor hook flash is ignored. However, a hook flash by the other parties works the same as in a two-party call. In particular, an agent flash puts the call on hold and allows a consultative transfer or conference.

If a conference call is already in progress, it cannot be monitored. If monitoring is already in progress, no one else can monitor the call.

15.6.6 Silent Coach

Silent Coach is a client feature that lets a user (the initiator) intervene in another user's active call and communicate with that user (the recipient). The initiator can speak to the recipient and listen to all other participants on the call. The recipient is the only call participant that can hear the initiator. For more information about silent coach, see Configuring Silent Coach on page 383.

Configuring Voice Mail 16

This chapter contains the following sections:

This chapter provides information about configuring the voice mail system.

16.1 Configuring System Distribution Lists

System distribution lists provide a mechanism for sending the same message to multiple users at one time. In Connect Director, you can add or edit system distribution lists.

16.1.1 Viewing System Distribution Lists

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **System Distribution Lists**. The **System Distribution Lists** page opens.

Note:
For descriptions of the columns on the **System Distribution Lists** page, see the following table.

Table 134: System Distribution Lists Page Columns

Parameter	Definition
Name	The name of the system distribution list.
Extension	The extension assigned to the distribution list.

16.1.2 Adding or Editing a System Distribution List

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **System Distribution Lists**. The **System Distribution Lists** page opens.
3. Do one of the following:

   - To edit an existing distribution list, click the name of the distribution list in the list pane.
   - To create a copy of an existing distribution list, click **Copy**.
   - To create a new distribution list, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the new or existing distribution list.

4. Review the parameters and specify values as appropriate.

> **Note**:
> For descriptions of the distribution list parameters, see the following table.

5. Click **Save**.

Table 135: System Distribution List Parameters

Parameter	Description
Name	Specifies the name of the distribution list.
Extension	Specifies the extension that is used for sending messages to members of the distribution list. Users can enter this number either in the Connect client or when addressing a message from the telephone user interface.
Show References	Click to display a list of everywhere this extension is used.

Parameter	Description
Recorded name	Use the following buttons to record, import, and play back the distribution list name: • Click **Record** to record the distribution list name. • Click **Play** to listen to the recording. • Click **Import** to import a recording of the distribution list name from an existing file. **Note**: Imported recordings must be CCITT µ-Law, 8 KHz, 8-bit, mono WAV files. When using the system recorder, the recording meets these requirements by default. • Click **Preferences** to select whether to use your PC or your phone to play back your recording; you can also select a phone extension or external number to use to record the distribution list name.
Distribution list members: Available or Selected	Displays the list of users that are available to add to the distribution list and the list of users included in the distribution list. You can edit the user names included in the distribution list as follows: • To add users to a distribution list, select the user or users from **Available** list and use the right arrow button to move the users to the **Selected** list. • To remove users from a distribution list, select the user or users from the **Selected** list and use the left arrow button to move the users to the **Available** list. **Tip:** To filter the list of Available users, use the filter button. You can use the page and row controls to navigate through the list.

Parameter	Description
AMIS system	You can add AMIS system users to system distribution lists. In the drop-down list, select the AMIS system where the users reside, and then click **Add**. A dialog box prompts you for the extension number of the user. Enter the number and click **OK**. The AMIS System ID and extension, or Mailbox ID, appears in the distribution list box.

16.1.3 Adding or Removing Users from a System Distribution List

Note:

You can also add or remove a user from a system distribution list on the Users page (on the Membership tab of the details pane). For more information, see Configuring a User Account on page 488.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **System Distribution Lists**. The **System Distribution Lists** page opens.
3. Click the name of the distribution list you want to edit in the **List** pane.

Note:
The **General** tab in the **Details** pane displays parameters for the distribution list.

4. Do one of the following:

   - To add users to the distribution list, select the users in the **Available** list and click the right arrow button to move the users to the **Selected** list.
   - To remove users from the selected distribution list, select the users in the **Selected** list and click the left arrow button to move the users to the **Available** list.

5. Click **Save**.

16.1.4 Configuring the Broadcast Distribution List

The MiVoice Connect system lets a user with the proper class of service send a broadcast message to all mailboxes. Unlike system distribution lists, the broadcast distribution list cannot be edited. However, if you need to remove someone from the broadcast distribution list, you can remove individual mailboxes through the **Accept broadcast messages** field on the Voice Mail tab and Mailbox subtab on the Users page, Workgroups page, or Route Points page.

16.2 Configuring Voice Mail Options

System-wide voice mail options are configured on the Voice Mail Options page.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **Options**. The **Voice Mail Options** page opens.
3. Review the parameters and specify values as appropriate.

Note:
For more information about all of the user parameters on the **Voice Mail Options** page, see the following table.

4. Click **Save**.

Table 136: Voice Mail Options Page

Parameter	Description
General	
Min voice mail password length	Specifies the minimum number of digits required for a voice mail password.
Force all users to change voice mail password at next login	Select this check box to prompt users to change their voice mail password the next time they log on to the voice mail system.

Parameter	Description
Max login attempts before disconnect	Specifies the number of times a user can fail when attempting to log in to voice mail from a phone. When the user fails this number of login attempts, the system notifies the user and terminates the call. Valid values are 2–50.
Min message length accepted	Specifies the minimum length, in milliseconds, that a message must be in order to be accepted. The system default is 2000 milliseconds. Valid values are 1000-5000 milliseconds. The Voice Mail application automatically removes silence from voice messages. If the resultant message after silence removal is less than this minimum message length, the message is assumed to be a hang-up and is deleted from the system.
Enable default forward to voicemail prompt	Select this check box to enable the default forward to voicemail prompt.
From address for email notifications	Specifies the sending email address to use when sending email notifications about new messages.
Enable default forward to voicemail prom pt	Select this check box to enable the default forward to voicemail pro mpt.
Enable default voicemail logon greeting	Select this check box to enable the default voicemail logon greeting.
AMIS	
Enable AMIS	Select this check box to enable all AMIS systems. This option is enabled by default. Individual AMIS systems can be enabled and disabled from the AMIS page. For more information about AMIS systems, see Configuring AMIS Voice Mail Systems on page 589.

Parameter	Description
Allow incoming AMIS access to Broadcast distribution list	Select this check box to allow delivery of incoming AMIS messages to the Broadcast Distribution List.
Allow Incoming AMIS access to system distribution list	Select this check box to allow delivery of incoming AMIS messages access to the System Distribution Lists.

16.3 Configuring AMIS Voice Mail Systems

The MiVoice Connect system sends voice mail messages to and receives voice mail messages from legacy voice mail systems by using Audio Messaging Interchange Specification (AMIS) protocol Version 1 — Spec February 1992. To send voice mail messages to remote AMIS sites, Mitel dials a phone number to access the remote system. Likewise, to receive voice messages from a remote system, the remote system must have the number to dial into the MiVoice Connect system. To reach the MiVoice Connect system, the remote system must be configured to dial a number that reaches an auto-attendant menu.

AMIS call support is enabled by default. Incoming AMIS voice mail is delivered in the same manner as other voice mail; however, users cannot send replies to AMIS voice mail. To send outbound AMIS voice mail, you must create AMIS systems in Connect Director.

Mitel negotiates the setup, handshaking, and teardown of AMIS system calls. Each voice mail requires a call over the AMIS delivery and call-back numbers.

You can configure AMIS systems for two addressing methods. If the system does not use off-system extensions, a System ID number is required to direct the voice mail to the correct site. When a user wants to send a voice mail to a recipient on an AMIS system, he or she first must enter the System ID and then the mailbox number or extension.

Table 137: Examples of Address with a System ID

System ID	Recipient Mailbox Number
8331	1234
8408331	45657

If the system uses off-system extensions, these extensions become off-system mailboxes. In this case, users simply address the voice mail by mailbox number and without entering the System ID.

16.3.1 AMIS Restrictions

The following restrictions are placed on AMIS voice messages:

- Mitel establishes a call to an AMIS system for each voice mail. If a voice mail is addressed to multiple recipients, Mitel delivers as many as nine voice mails in a single call. If a voice mail has more than nine recipients, Mitel makes additional calls until the voice mail is delivered to all recipients. You can optimize AMIS voice mail delivery by using distribution lists at the remote AMIS sites.
- The maximum message length permitted is eight minutes.
- After ten failed attempts to complete a call to an AMIS system, Mitel disables the AMIS system and generates an event log.
- After Mitel establishes an AMIS system call, it tries three times to complete message delivery to each recipient. If Mitel fails to deliver a voice message after three attempts, it stops trying and returns the message to the sender. However, if the sender's voice mailbox is full, the sender will not receive the failed message.
- Outbound voice mail messages for disabled AMIS systems are accepted and queued. To deliver queued messages, enable the AMIS system in question on the AMIS edit page.

16.3.2 Creating AMIS Systems

Perform the following steps before you create AMIS systems to remote sites:

- AMIS is enabled by default, but ensure that AMIS is enabled in your system. For more details, see Enabling AMIS Systems on page 590.
- Review the extension plans for all the systems to which you want to connect. Make sure they use the same extension length and that extension numbers do not overlap.

After setting these global parameters, the next step is creating and configuring the individual AMIS systems.

16.3.2.1 Enabling AMIS Systems

Before using AMIS with the MiVoice Connect system, you must make sure AMIS is enabled for the system.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **Options**. The **Voice Mail Options** page opens.

3. Select the **Enable AMIS** check box.
4. Select the **Allow incoming AMIS access to Broadcast distribution list** check box to allow delivery of incoming AMIS messages to the Broadcast Distribution List.
5. Select the **Allow incoming AMIS access to system distribution** list check box to allow delivery of incoming AMIS messages access to the System Distribution Lists.
6. Click **Save**.

16.3.2.2 Viewing a List of AMIS Systems

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **AMIS**. The **AMIS** page opens.

Note:
For descriptions of the columns on the AMIS page, see the following table.

Table 138: AMIS Page: List Pane

Column Name	Description
AMIS System	The name of the AMIS site.
Enabled	Indicates whether or not the AMIS system is enabled.
System ID	The System ID for the AMIS site.
Delivery Number	The number Mitel calls to send AMIS voice messages to the remote system.
Mailbox Length	The length of the remote site's mailboxes or extensions.
Call Back Number	The number on which you receive AMIS messages.

16.3.2.3 Adding or Editing an AMIS System

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **AMIS**. The **AMIS** page opens.
3. Do one of the following:

   - To edit an existing AMIS system, click the AMIS system in the **List** pane.
   - To create a copy of an existing AMIS system, click **Copy**.
   - To create a new AMIS system, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays the parameters for the new or existing AMIS system.

4. Review the parameters and specify values as appropriate.

> **Note**:
> For descriptions of the AMIS system parameters, see the table below.

5. Click **Save**.

Table 139: AMIS Page Parameters

Parameter	Description
Name	Specifies the name of the AMIS site.
System enabled	Select this check box to enable the named AMIS system. Outbound voice mail for this system is queued until the system is reset by selecting this check box.
Language	From the drop-down list, select the language of the AMIS system.

Parameter	Description
System ID	Specifies the system ID. The System ID defines the AMIS site where the voice mail for this system is delivered. The System ID consists of an access code plus a site identifier. The System ID plus a mailbox number identifies the site and the voice mail recipient. Plan the System ID to simplify the process of sending AMIS voice mail for your users. The System ID must begin with a digit reserved for trunk access codes, though it can be different from other trunk access codes. To make the System ID intuitive to voice mail users, choose a site identifier related to the public numbers used at the site. For example, if the voice mail delivery number is +1 (408) 555-1234, then System IDs such as 8555 or 9408555 would be intuitive to your users. Generally, the shorter the System ID number, the easier it is to use. The System ID plus the mailbox length cannot exceed 15 digits. System IDs are required and can be single digits. Each AMIS system you create must have a unique System ID.
Delivery number	Specifies the number Mitel calls to send AMIS voice messages to the remote system.
Call back number	Specifies the number on which you receive AMIS messages.
Mailbox length	Specifies the length of the remote site's mailboxes or extensions. If you use off-system extensions, the length must match the length of your extensions. The System ID plus the mailbox length cannot exceed 12 digits.

Parameter	Description
Lower/Upper OSE	If your system is using off-system extensions (OSEs), select the extension range from the Available list and use the right arrow button to move them to the Selected list. These extensions function as off-system mailboxes, allowing users to address voice mail to users on remote AMIS sites without entering a System ID. For more information, see Adding or Editing a Trunk Group on page 221.

16.3.3 Disabling or Deleting AMIS Systems

You can disable AMIS systems globally or by individual connection. When you disable AMIS, Mitel does not send or receive AMIS voice messages. Individual AMIS systems are automatically disabled when Mitel fails to complete a call to an AMIS system.

Users can address outgoing voice messages while the system is disabled. Outbound messages are queued until the individual AMIS system is re-enabled. Attempts to deliver to a disabled AMIS system fail.

16.3.3.1 Disabling All Configured AMIS Systems

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **Options**. The **Voice Mail Options** page opens.
3. Clear the **Enable AMIS** check box.
4. Click **Save**.

16.3.3.2 Disabling an Individual AMIS System

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **AMIS**. The **AMIS** page opens.
3. Click the name of the system you want to disable in the **List** pane.

Note:
The **General** tab in the **Details** pane displays the parameters for the selected AMIS system.

4. Clear the **System enabled** check box.
5. Click **Save**.

16.3.3.3 Deleting an AMIS System

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Voice Mail** > **AMIS**. The **AMIS** page opens.
3. Click the name of the system you want to disable in the **List** pane.

Note:
The **General** tab in the **Details** pane displays the parameters for the selected AMIS system.

4. Click **Delete**.
5. In the confirmation dialog, click **OK**.

Note:
The AMIS system is deleted and not longer appears in the **List** pane.

16.3.4 Designating an AMIS Test Mailbox

Mitel allows you to designate a mailbox that a remote AMIS system can use to test AMIS features. When you address a voice mail to the AMIS test mailbox, Mitel automatically replies with the same message.

16.4 Configuring Voicemail Delivery and Notification

You can configure various voicemail delivery parameters and escalation notifications.

16.4.1 Configuring Voicemail Delivery

You can specify whether and how voicemail messages are sent through emails. You can choose to send only an email or to include a WAV file of the voice mail message.

You can also set voicemail to automatically forward. That is, a mailbox may be configured to send any message it receives to another mailbox. The message sent to the original

mailbox can be automatically deleted as an option. The target mailbox for the forwarded messages may be of any user, a workgroup, a route point, an AMIS address, or a system distribution list other than a broadcast distribution list. A message announcing that the message has been automatically forwarded, including a time stamp, is prepended to the forwarded message. For example, the recipient of such a message might hear, “Auto-forwarded message received at 9:10 AM from Customer Support Mailbox.”

This feature might be used for handling the off-hours calls when few support staff are available. Off-hours calls may be routed to a back up extension. If no one is available to answer the back up extension, calls can end up in a voice mailbox that is not checked for hours. The back up extension can be set to automatically forward any calls that are received in its mailbox. Calls can be forwarded to a mailbox that is checked on a regular basis.

Automatic forwarding is available between distributed voicemail servers. The forwarded message is handled as any other message, including message waiting indicator, calling notifications, return receipt requests, or urgent markings. Automatically forwarded messages can be forwarded and replied to. If the target mailbox is full, the message is left in the sending mailbox. If a message is automatically forwarded to a list of mailboxes and one of these mailboxes is full, then the target is skipped.

16.4.1.1 Sending Email with Voicemail Link

You can configure to send an email notification that includes a link to play, download, and delete the voicemail message.

When you click the play link in the voicemail email, a new webpage appears with the **Play, Delete** and **Download** icon:

- If you play the voicemail message from the webpage, it autoplays the message, and is marked as heard in the voicemail system.

> **Note**:
> Internet Explorer 11 does not support the play voicemail feature.

- If you download the voicemail message from the webpage, the message is downloaded to the computer. The voicemail state does not change.
- If you delete the voicemail message from the webpage, the message is deleted from the voicemail system and moved to the deleted folder.

You can access the voicemail feature outside the enterprise network through the Connect Edge Gateway.

To configure the voicemail delivery option for a user:

1. Open Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**.

   The **User** page is displayed.
3. Click the name of the user for whom you want to configure the email delivery type.

   The **General** tab displays parameters for the selected user.
4. Click the **Voice Mail** tab.
5. For **Delivery type**, select **Email voicemail as link** from the drop-down menu to send an email notification with the voicemail link.

Note:
The email link points directly to the user's active voice mail server. If this voice mail box is moved to a different server, then the email link becomes invalid. However, the message is not lost; it can be accessed from Connect Client or the phone.

6. Click **Save**.

For information about configuring the voicemail delivery options, see Voice Mail Tab on page 515.

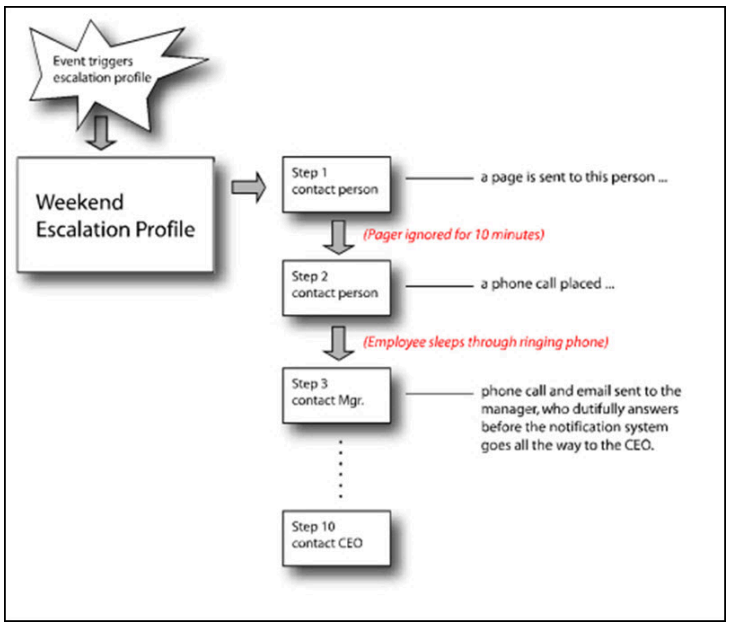
16.4.2 Configuring Escalation Notification

The MiVoice Connect system supports escalation notification. This voice mail feature allows your organization to know when your customers need help.

You can configure escalation profiles to notify employees when a voice mail is received, which can be helpful in providing superior service and support after hours. For example, if a customer calls into your system but no one answers the call, the customer can leave a voice message. If escalation profiles are configured, this message triggers the escalation notification process so that appropriate personnel are notified by email, phone, or pager.

If the first person does not respond to the notification by listening to the customer’s voice mail message within a certain time period, the next step in the escalation process is initiated and the designated person is contacted, and so on, until as many as 10 people have been contacted. The escalation notification process ends when someone dials into the MiVoice Connect system and listens to the customer's voice mail message or after the steps in the process have been repeated a specified number of times. Refer to the below figure for an example of the flow for an escalation profile event.

Figure 17: Example Escalation Profile



16.4.2.1 Configuring Escalation Profiles for a User

A maximum of nine notification profiles can be configured for each user. Each escalation profile has the following characteristics:

- A maximum of ten notification steps can be configured. Each step allows the system administrator to specify who is contacted and the method used to contact that person; the person can be contacted by phone call or pager notification. An email can be sent to that person in addition to or instead of the phone call or pager notification.
- Different escalation profiles can be associated with different availability states.
- If a message is left, and someone listens to it, the notifications stop. However, if someone marks a message unheard, the notification process restarts in the same way that receiving a new voice message triggers the process.
- Escalation notification is supported on all mailboxes, including mailboxes of extension and mailbox users, mailbox-only users, and SMDI mailbox-only users, as well as workgroup mailboxes.

Note:

Any steps within a configured profile that are not configured are skipped during the escalation process.

1. Launch Connect Director.

2. In the navigation pane, click **Administration** > **Users** > **Escalation Profiles**. The **Users Escalation Profiles** page opens.
3. Click the name of the user for whom you want to configure escalation profiles.

Note:
The escalation profiles for the selected user are displayed.

4. Review the parameters and specify values as appropriate.

Note:
For descriptions of the escalation profile parameters, see Users Escalation Profiles Page: Escalation Profiles Tab

5. Click **Save**.

Note:
The parameters on the **Users Escalation Profiles** page are described in Users Escalation Profiles Page: Escalation Profiles Tab.

Table 140: Users Escalation Profiles Page: Escalation Profiles Tab

Parameter	Description
Escalation notification options	Select one of the following options: • **Escalate for each message** - to begin escalation notification each time a new voice mail message arrives in the voice mailbox. If several messages arrive within a short period of time, users who are notified will receive multiple notifications. • **Escalate for first unheard message** - to begin escalation notification only when the first unheard voice mail message arrives in the voice mailbox. Subsequent unheard messages do not trigger another wave of notifications as long as the first message remains unheard.
Profile subtabs	

Parameter	Description
Profile name	Specifies the name of the escalation profile.
Repeat count	Specifies the number of times the system loops through the 10 steps of this profile before it stops trying to contact the various notification members. Select 0 to execute the escalation profile steps once without repeating. Select one to execute the steps of the profile twice — the initial execution and one repetition. **Note**: This parameter does not apply if you select one of the Notification by email options.
Step subtabs	There is a subtab for each step in a profile; there are a maximum of 10 steps for each escalation profile.
Timeout	Specifies the amount of time, in minutes, that elapses before the next step in the profile is executed. This is the amount of time a message recipient has to respond to the original voice mail before escalation occurs.
Urgent only	Select this check box to send notification only when the escalation is determined to be urgent.
Notification by email	

Parameter	Description
Deliver message as email	Select one of the following three email delivery options: • **Disabled** - to not send email notification. • **Email text only** - to send a text email to the designated user's email inbox. The email message contains basic information about the voice mail message, such as the time, duration, and Caller ID of the message that was recorded. • **Attach WAV file** - to send an email containing a copy of the recorded voice mail message to the designated user's email inbox. The recipient can play the message on his or her PC.
Email address	Specifies the email address to send notification to.
Notification by phone	
Voice mail notification method	Select one of the following phone notification methods: • **Pager** • **Phone** • **None**
Notification number	Specifies the phone or pager number to send notification to.
Pager ID	Specifies the pager pin number required to access the recipient.
Pager data	Specifies the code the recipient requires to indicate that a page is waiting.

16.4.2.2 Linking an Escalation Notification Profile to an Availability State

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the user for whom you want to link an escalation notification profile to an availability state.

Note:
The **General** tab displays the parameters for the selected user.

4. Click the **Routing** tab, and then the click the **Availability States** subtab.

Note:
The **Availability States** subtab displays the parameters for the Available availability state.

5. Click the subtab for the availability state that you want to edit.

   The parameters for the selected availability state are displayed.
6. In the **Voice mail escalation profile** list, select the escalation profile that you want to associate with this availability state.
7. Click **Save**.
8. Repeat this process to associate different escalation profiles with each of the different availability state as needed.

16.4.3 Configuring Notifications for Full Voice Mailbox

You can configure automatic message forwarding and email delivery options for a user so that users are notified when their voice mailboxes are almost full.

When a user's mailbox approaches its maximum capacity, the system sends the user a notice that their mailbox is almost full. Each time a user whose mailbox is almost full logs into voice mail, the user receives a notice telling them how much space remains. In this way, mailbox owners are given adequate notice to clean up their mailboxes and can avoid an unexpected “mailbox full” notification.

Be aware of the following operational details for full voice mailbox notifications:

- The maximum number of messages a user can receive ranges from 0 to 500, depending on the value set in the **Incoming max. messages** field on the Voice Mail Permissions page. Because this is a class of service setting, the limit can vary among users in the system.
- As a user's mailbox approaches its limit, a warning message is played indicating that the user has room for only “n” number of messages, where the value “n” counts down from 10 to 0. This message is played when a user logs into the mailbox via the telephone user interface or Connect client.
- The threshold for triggering this mailbox-full notification is when there is enough space for only 10 additional messages. This non-configurable threshold is the same for all users, regardless of total mailbox capacity.
- The “almost full” notification is played until a user deletes messages, thereby reducing the number of messages below the threshold.
- When a mailbox reaches its limit, the mailbox owner is notified, if notification has been enabled for this user, and a warning event is logged. For information about sending email notification of a full mailbox, see Configuring Mailbox Full Notifications on page 604.
- When a message is deleted, it is no longer counted against the total capacity for a user's mailbox.
- Deleted messages are temporarily held in a deleted messages folder. Up to 200 deleted messages can be temporarily held. When this limit is reached, the mailbox is considered full and the user is unable to receive new messages until the deleted messages have been purged. If this happens, the mailbox owner receives the following notification: “Your mailbox is full. No more messages will be accepted until you purge your deleted messages.”
- Deleted messages can be manually purged by the user or automatically by the system. Automatic purging occurs on a nightly basis.

16.4.3.1 Moving Voice Mailbox to a New System

The Move Voice Mailbox feature offers a way for users to move their voice mailbox to a new system.

Complete the following steps to move the voice mailbox to a new system:

1. Take a backup of the VMB and delete the existing VMB from the old system.
2. Perform a “Full” factory reset of a VMB by pressing the factory reset button for more than 10 seconds.
3. Add a VMB to the new system.
4. Plug-in the VMB into the new system.

16.4.3.2 Configuring Mailbox Full Notifications

You can enable mailbox-full notifications for any user. When this feature is enabled and a user's voice mailbox reaches maximum capacity, the user receives an email notification that the voice mailbox is full.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Click the name of the user for whom you want to enable notifications for

Note:
The **General** tab displays parameters for the selected user.

4. Click the **Voice Mail** tab.
5. Select the **Send email warning when mailbox is full** check box to enable notification.
6. Click **Save**.
7. Repeat this process for each user you want to configure mailbox-full notifications for.

16.5 Voice Mail Status Information

You can view status information about voice mail servers from the Maintenance menu. For details, see Monitoring Voice Mail Status on page 813.

16.6 Voice Mail Synchronization with Gmail for Business

The Synchronization with Gmail for Business feature automatically synchronizes the state of a Mitel user's voice mail with the state of each corresponding email when voice mail status is sent via Mitel's email notification. The Headquarters or DVS server monitors the state of a user's voice mails and emails and synchronizes those states. For example, when a user opens the voice mail notification email, the voice mail is marked heard on the voice mail system, and the message-waiting indicator on the phone is turned off.

A user account can be configured so that the user receives email notification of a new voice message. This email notification can also arrive with an attached WAV file of the actual voice message. The user can receive both the notification and the voice mail in the email client.

To monitor the status of email, Synchronization with Gmail for Business uses the IMAP4 and OAuth2 protocols to access and authenticate with Gmail server. The Secure Sockets Layer (SSL) protocol is used to secure pertinent communications on the network.

Note:

Google Gmail is the only email server that a MiVoice Connect system can interoperate with for synchronization of voice mail status. The feature currently works on Gmail Premier and Educational email accounts only. These accounts have the APIs that are necessary for the integration to work.

16.6.1 Overview

Synchronization Service

The service runs on the Headquarters server and all DVS servers. The name of the service is Mitel-VmEmSync.

Each service is responsible for synchronizing the mailboxes that are on the same server. For example, the service running on the Headquarters server syncs the mailboxes located on the Headquarters server.

In the case of mailboxes on a Voice Mailbox Server switch (VMB switch), the synchronizing is done by the VmEmSync service that is running on the same server as the TMS that manages the VMB.

16.6.1.1 Synchronization Rules

The synchronization rules depend on whether an email notification has the attached WAV file and whether the server is synchronizing during Mitel-VmEmSync service startup or during normal operation.

16.6.1.1.1 Synchronization On Startup

Start-up synchronization refers to initialization of the Mitel-VmEmSync service. This service gathers information on all voice mail and related email for each user and then synchronizes the states based on the rules in either in the following table, which is for email text only, or in the below table, which is for email with WAV file attachment.

Table 141: Start-up Synchronization with Email-only Text

Voice Mail State	Email State	Sync Action
Deleted	Not Deleted	Delete Email
Heard	Unread	Mark Email Read
All other states	Any state	No action

Table 142: Start-up Synchronization with WAV File Attachment

Voice Mail State	Email State	Sync Action
Heard	Unread	Email Read
Unheard	Read	Mark Voice Mail Heard
Deleted	Not Deleted	Delete Email
Not Deleted	Deleted	Delete Voice Mail

16.6.1.1.2 Synchronization During Normal Operation

Synchronization during normal operation is triggered when a user makes a change to a voice mail or email. In the following tables, the voice mail change is listed in the “Event” column, and the consequence for the voice mail or email is listed in the “Sync Action” column.

Table 143: Sync with Email-only Text during Normal Operation

Event	Sync Action
Voicemail is deleted.	Delete email.
Voicemail is heard	Mark email as read.
All other events.	No sync action.

Table 144: Sync with WAV File Attachment during Normal Operation

Event	Sync Action
Voicemail is deleted.	Delete email.
Voicemail is heard.	Mark email as read.
Voicemail is undeleted.	Move email to Inbox. Mark email as unread if voice mail is unheard.
Voicemail is marked unheard.	Mark email as unread if voicemail is in “NEW” folder.
Email is deleted.	Delete voicemail.
Email is read.	Mark voicemail as heard.
Email is undeleted.	Move voicemail to “Saved” folder.
Email is marked unread.	Mark voicemail as unheard if email is not in “Trash” folder.

16.6.1.2 Impact on Network Resources

Before setting up this feature, consider its impact on network resources. The MiVoice Connect system monitors the state of all user messages so that, for example, when a voice message is heard, the system reflects the state change in a timely manner. To ensure timely updates to the status of all messages, the system uses network bandwidth in proportion to the number of messages.

For example, consider a Mitel deployment that supports 1000 users and that each user has 5 messages. The state of 5000 messages total is monitored by the MiVoice Connect system. For monitoring the state of 5000 messages, the required bandwidth is 75 Kbytes per second. In this scenario, the time to synchronize a message’s state change between voice mail and email is less than 20 seconds.

In the event of a server restart, the initial synchronization time for a system with up to 1000 users is less than 3 minutes.

16.6.1.3 Synchronization Criteria

Synchronization is automatically enabled for a user if both of the following are true:

1. The user is configured to receive email notifications. The email address must be the same as the user's Premier/Education Gmail account.
2. The system administrator configured an email server with the domain for the user's email address by using OAuth2 client email and private key. For example, the system administrator configured OAuth2 access with the domain for the user's email address. See Configuring the Google OAuth2 Settings on page 608 and Configuring Gmail Synchronization in Connect Director on page 610 for more information.

16.6.1.4 Use of the OAuth2 Protocol

The OAuth2 protocol lets a third party gain access to a user's account without needing the user's password. By relying on OAuth2, the Mitel-VmEmSync service can use the IMAP4 AUTHENTICATE command to examine a user's email without logging in as the user. Gmail and most Google APIs support OAuth2.

For the Premier and Education versions of Gmail, OAuth2 is set up by the system administrator. The administrator enables certain capabilities and acquires a system-generated private key at the Google OAuth2 management web page. The system administrator must first perform these actions in the applicable Google page before providing access to all accounts on a domain.

The private key from Google OAuth2 management and the client email allow the Headquarters server or DVS to:

- Authenticate with Google mail servers without needing the user passwords.
- Establish a trusted host relationship between the two servers.

16.6.2 Configuring Synchronization with Gmail

Mitel synchronization with Gmail Premier and Education Services utilizes Google Apps OAuth2 client email, private key, and domain name. The following sections describe how to generate the OAuth2 client email and private key and configure the required parameters in Connect Director.

16.6.2.1 Configuring the Google OAuth2 Settings

The following section describes the steps that a system administrator must perform before configuring Gmail synchronization in Connect Director.

1. Launch a web browser and navigate to the Google Developers Console at **https://console.developers.google.com.**
2. From the Google Developers Console bar, click to open the **Products & services menu**, and then click **Permissions**.

   The Permissions page is displayed.
3. Click the **Service accounts** tab, and then click Create service account.
4. In the **Create service account** dialog box, do the following:

   a. In the **Name** field, enter a name for the service account.

      The Service account ID is automatically populated.
   b. Select the **Furnish a new private key** check box, and leave **JSON** selected.
   c. Select the **Enable Google Apps Domain-wide Delegation** check box to grant Google Apps domain-wide authority to the service account.
   d. Click **Create**.

   Your new private key pair is generated and downloaded to your machine. Make note of where this file is located; you will need information in this file to configure Gmail synchronization in Connect Director.

   For the latest information about the registration process, refer to the Google OAuth2 service accounts page.
5. Navigate to the following URL: **https://admin.google.com**
6. Select **Security** from the list of controls. If you do not see **Security** listed, select **More controls** from the gray bar at the bottom of the page and then select Security from the list of controls.

   If you do not see the controls, make sure you are signed in as an administrator for the domain.
7. Click **Show more**, and then click **Advanced settings** from the list of options.
8. Click **Manage API client access** in the **Authentication** section.
9. In the **Client Name** field, enter the **Client ID** for the service account.

   You can find the client ID on the **Service accounts** tab, on the **Permissions** page of the Google Developers Console.
10. In the **One or More API Scopes** field, enter **https://mail.google.com/**
11. Click **Authorize**.

16.6.2.2 Configuring Gmail Synchronization in Connect Director

When configuring synchronization with Gmail in Connect Director, you will need the OAuth2 client email, private key, and premier or educational Gmail account domain name provided in the JSON file that downloaded to your machine when you created the service account. See Configuring the Google OAuth2 Settings on page 608 for more information.

1. Navigate to and open the JSON file that was downloaded when you created the service account.
2. Launch Connect Director.
3. In the navigation pane, click **Administration** > **System** > **Additional Parameters**. The **Additional Parameters** page opens.
4. Under **Gmail configuration**, in the **Client Email** field, enter the OAuth2 client email specified in the JSON file.
5. In the **Private Key** field, enter the private key specified in the JSON file.
6. In the **Domain Name** field, enter the domain of your premier or educational Gmail account.
7. Click **Save**.

Configuring the Auto Attendant 17

This chapter contains the following sections:

This chapter describes how to configure the auto attendant.

17.1 Overview

An Auto-Attendant is a program that answers and handles inbound calls without human intervention. Auto attendants typically provide menu-driven options through which callers can obtain information, perform tasks, or connect to a requested extension.

The Auto-Attendant can answer incoming calls and transfer callers to an extension, a mailbox, another menu, a workgroup, or a route point. It also includes a dial-by-name feature that transfers callers to the system directory, where they can connect to an extension by dialing the user's name.

17.1.1 Auto-Attendant Operating Modes

In MiVoice Connect, new or existing Auto-Attendant menus can have any of the following operating modes.

- On-Hours mode lets you configure the Auto-Attendant to handle incoming calls during regular office hours.
- Off-Hours mode covers all hours not scheduled in other modes. This is typically when the office is closed for the evening and weekend.
- Holiday mode lets you configure how the Auto-Attendant functions on holidays.
- Custom mode is used for single days that are not covered by the other modes such as a company special event.

You can configure these modes for different situations, and each mode has a configuration page. Schedules are set using the **Schedule** parameter.

Note:

For information about establishing schedules, see Overview on page 621.

The following logic determines which schedule is active:

1. The Auto-Attendant first checks for the Custom schedule.
2. If the Custom schedule is not available, the Auto-Attendant checks for the Holiday schedule.
3. If the Custom or Holiday schedule is not available, the Auto-Attendant checks for the On-Hours schedule.
4. If the Custom, Holiday, or On-Hours schedule is not available, the Auto-Attendant checks for the Off-Hours schedule. Connect Director forms the Off-Hours schedule from all the hours not scheduled in the other modes. If you do not create a schedule for at least one of the other modes, the On-Hours schedule is in effect.

17.1.2 Multiple Auto Attendants

Multiple Auto-Attendants can be configured for different user groups or departments, and each Auto-Attendant configuration can have multiple levels of menu options.

There are no hard limits to the number of Auto-Attendants that can be configured in a MiVoice Connect system. However, in most installations, the system can support up to 500 Auto-Attendant menus. However, this number may be affected by the complexity of your dialing plan.

When a caller reaches the main Auto-Attendant, it provides options for forwarding calls to individual user extensions. It can also provide options for forwarding calls to the sales department and customer operations department Auto-Attendants. From the sales or customer operations Auto-Attendants, callers can be given options that transfer calls to the appropriate extension.

The dial-by-name operation of the Auto-Attendant transfers callers to the system directory, where they can connect to an extension by dialing the user's name. The dial-by-name operation can be limited to a department or other organizational sub-group by associating the operation with an extension list. To create extension lists, refer to Extension Lists on page 546. Only users that have been configured to be included in the dial-by-name list will be included. For more information, refer to Configuring a User Account on page 488.

When callers are transferred back to the Auto-Attendant, either willingly or because of an error, they are returned to the default Auto-Attendant menu on the associated server.

17.2 Configuring Auto-Attendant Menus

To configure a new **Auto-Attendant** menu or edit an existing menu, you use the **Auto-Attendant** page.

17.2.1 Viewing Auto-Attendant Menus

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Auto-Attendant**. The **Auto-Attendant** page opens.

Note:
The columns in the list pane are described in the following table.

Table 145: Auto-Attendant List Pane

Column	Description
Name	The name of the Auto-Attendant menu.
Extension	The extension that is associated with the Auto-Attendant menu.
On-Hours	The name of the On-Hours schedule, if any, that is associated with the Auto-Attendant menu.
Holiday	The name of the Holiday schedule, if any, that is associated with the Auto-A ttendant menu.
Custom	The name of the Custom schedule, if any, that is associated with the Auto-At tendant menu.

17.2.2 Adding or Editing an Auto-Attendant Menu

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Auto-Attendant**. The **Auto-Attendant** page opens.
3. Do one of the following:
   - To edit an existing Auto-Attendant menu, click its name.
   - To create a new Auto-Attendant menu, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing auto-attendant menu.

4. Review the parameters on the **General** tab, and specify or edit values as appropriate.

Note:
For more information about the parameters on the **General** tab, see Auto Attendant Page: General Tab.

5. For each auto-attendant menu that you want to create or modify, select the relevant tab and specify or edit parameters as necessary.

Note:
For more information about the parameters on the On-Hours, Off-Hours, Holiday, Custom, DNIS tabs, see Auto Attendant Page: On-Hours, Off-Hours, Holiday, and Custom Tabs and Auto Attendant Page: DNIS Tab.

6. Click **Save**.

Table 146: Auto Attendant Page: General Tab

Parameter	Description
Name	The name of the auto-attendant menu.
Extension	The extension number associated with the auto-attendant menu. Refer to Setting Dial Plan Parameters
Show References	Click to display a list of everywhere this extension is used.
DID Settings	Click **change settings** to display the following DID settings: • Enable DID • DID Range • DID number
Language	From the drop-down list, select a language to be used by the auto-attend ant menu for responses such as invalid entry. Greetings must be recorded in this language.
Enable DID	When this check box is selected, a DID number is used to access the associated auto-attendant menu. If you select this check box, enter a nu mber in the DID number field.
DID Range	From the drop-down list, select a DID range from which the entity's DID number will be selected. Each DID range corresponds to a trunk group and lists the number of available numbers.
View System Directory for DID usage	Click this link if you want to view the System Directory page to find an ava ilable DID number.
DID number	If DID is enabled, provide a DID number for the auto-attendant menu. The prefix located to the left of the data entry field and the range located to the right of the data entry field are based on the selected DID range.

Parameter	Description
Max time to enter multiple digits	Specifies the amount of time (in milliseconds) the system waits for an a dditional digit to be pressed when a multiple digit operation is configured for an Auto Attendant schedule.
Make extension private	Select this check box to remove this number from the system directory an d call routing destination lists.
Allow prompt recording using telepho ne	Select this check box to enable users to record auto-attendant prompts through the voice mail system they access through the telephone. When this option is enabled, users can dial into the system to record auto-attendant prompts in the same way that they would change their personal mailbox greeting, modifying the greeting without having to access the recording interface through Connect Director. With this capability, administrators can delegate the task of recording auto-attendant menus to more appropriate team members.
Menu password	A separate voice mailbox is created for each auto-attendant menu, allowing users to dial into the system to change the menu prompts. Each auto-attendant menu may have its own password and a unique, dialable number. If a password is desired, enter the password in the field provided, and enter it a second time to confirm.

Table 147: Auto Attendant Page: On-Hours, Off-Hours, Holiday, and Custom Tabs

Parameter	Description
Schedule	From the drop-down list, select a schedule to apply to the auto-attendant menu. Any available schedules of the type matching the tab name (On-Ho urs, Holiday, or Custom) are included in the list. For information about set ting up schedules, see Overview.
View schedule	Click this link to view the selected schedule.

Parameter	Description
Disable monitor/record warning tone	This check box can be used to stop playing the warning tone for call monitoring and recording if the tone is enabled on the Call Control Options page. For details, see Configuring Call Control Options on page 427. Before disabling the warning tone, you may wish to consult with legal counsel regarding your intended use. **WARNING**: Mitel does not warrant or represent that your use of call monitoring or recording features of the Software will be in compliance with local, state, federal, or international laws that you may be subject to. Mitel is not responsible for ensuring your compliance with all applicable laws.
Timeout	The amount of time the caller has to perform an action. Specify 0-30000 milliseconds.
Prompt text	Before recording a prompt for a new or existing auto-attendant menu, enter the prompt text in this field. This text provides a convenient record of your prompt if you should ever need to re-record the prompt. This parameter is optional. Prompts on the Mitel system can be imported into the system using µ-law, WAV file format. If you would like your prompts to match the voice of the Mitel system, contact Worldly Voices at www.worldlyvoices.com and request that “Connie” record your prompts. Worldly Voices provides this service with a rapid turnaround time for a nominal fee.

Parameter	Description
Recorded prompt	Click any of the following buttons to perform tasks related to the auto-attendant menu prompt: • Click **Play** to hear the prompt. • Click **Record** to record the prompt. **Note**: You cannot record prompts if you log in to Connect Director in Https or Http mode. This issue also occurs when you log in using Internet Explorer. To resolve this issue, do the following: • For Https mode, log in to Remote Desktop and open Connect Director in Https mode using Chrome as the browser. • For Http mode, log in to Remote Desktop or outside the Remote Desktop connection and open Connect Director in Http mode using either Internet Explorer or Chrome as the browser. • Click **Import** and select the file from the appropriate directory to import a prerecorded prompt from a WAV file. • Click **Preferences** to specify whether the recorded prompt should be played through a PC or a phone and what extension or external number should be the source of the recording. • Click **Erase** to erase it.

Parameter	Description
Operation	Each item in the Operation drop-down list lets you select the action that is associated with its key pad number. This number is located to the left of each Operation drop-down list. When prompted by the auto attendant, the caller is asked to enter this number. • **Dial by first name** lets the caller spell the user's first name from the key pad. The auto attendant then transfers the caller to the user's extension. To limit the dial list to a department or other organizational sub-group, select an extension list from the dropdown list in the **Destination** field. Select **<None>** to remove the limit and allow callers to connect to any user in the System Directory. • **Dial by last name** lets the caller spell the user's last name from the key pad. The auto attendant then transfers the caller to theuser's extension. To limit the dial list to a department or other organizational sub-group, select an extension list from the drop down list in the **Destination** field. Select **<None>** to remove thelimit and allow callers to connect to any user in the System Directory. • **Go to extension** lets the caller enter an extension. This functions the same as a transfer but without a voice prompt.
Operation (continued)	• **Go to menu** transfers the caller directly to the user's voice mailbox without ringing the user's extension. This is also used to send the caller to another menu. You must specify an extension in the field to the right of this drop-down list item. • **Hang up** lets the caller disconnect the call. • **Repeat prompt** lets the caller hear the prompt again. • **Take a message by first name** lets the caller leave a message by spelling the user's first name from the key pad. The auto attendant then transfers the caller to the user's voicemail. To limit the dial list to a department or other organizational sub-group, select an extension list from the drop-down list in the **Destination**field. Select **<None>** to remove the limit and allow callers to connect to any user in the System Directory.

Parameter	Description
Operation (continued)	• **Take a message by last name** lets the caller leave a message by spelling the user's last name from the key pad. The auto attendant then transfers the caller to the user's voicemail. To limit the dial list to a department or other organizational sub-group, select an extension list from the drop-down list in the **Destination** field. Select **<None>** to allow callers to connect to any user in the System Directory. • **Transfer to extension** transfers the caller to the designated extension where he or she can speak with the person or leave a message if the person does not answer. You must specify an extension in the **Destination field**.
Time out	From the drop-down list, select the action that the Auto-Attendant takes when the caller does not press a key within a system-defined period of time. Typically, the action is Repeat Prompt.
Too many errors	From the drop-down list, select the action that the Auto-Attendant takes when the caller presses an invalid key too many times in a row. You might specify a user extension, such as the operator, for this. Typically, the acti on is Hang Up. If no action is specified, Hang Up is invoked by default.
Invalid entry	From the drop-down list, select the action to take when a key is pressed that the auto attendant does not recognize. Typically, the action is Repeat Prompt.
Multiple digits	In the drop-down list, select one of the following actions to take when a caller enters multiple digits: • **None** (the default) assigns no multiple-digit operation to the menu. • **Go to extension** assigns a multiple-digit operation to the menu and lets the caller enter an extension. This functions the same as a transfer but without a voice prompt.
Extension list	In the drop-down list, select the extension list to use as the auto-attendant.

Parameter	Description
Multiple digits (continued)	• **Go to menu** assigns a multiple-digit operation to the menu and transfers the caller directly to the user's voice mailbox without ringing the user's extension. This is also used to send the caller to another menu. You must specify an extension in the field to the right of this drop-down list item. • **Take a message** assigns a multiple-digit operation to the menu and lets the caller leave a message by selecting a user's extension. • **Transfer to extension** assigns a multiple-digit operation to the menu and transfers the caller to the designated extension where he or she can speak with the person or leave a message. You must specify an extension in the field to the right of this drop-down list item.

Table 148: Auto Attendant Page: DNIS Tab

Parameter	Description
Add	To associate the Auto-Attendant menu with a DNIS, click Add and provide details for the DNIS mapping in the displayed fields.
Trunk group name	From the drop-down list, select the trunk group for the DNIS mapping.
Digits	Enter the DNIS number.
Description	Provide a description for the DNIS number. This description is seen by c all recipients and in call detail reports (CDRs). The description length can be up to 26 characters.
Music on Hold	From the drop-down list, select a file-based MOH resource.
Remove	If you want to remove a DNIS system that is configured for this auto-att endant menu, click Remove.

Configuring Schedules 18

This chapter contains the following sections:

This chapter describes how to create schedules for the MiVoice Connect system.

18.1 Overview

Schedules let you define business hours and can facilitate proper routing of inbound calls. Schedules can be used by hunt groups and by the auto attendant.

The MiVoice Connect system supports the following types of schedules:

- On-Hours
- Holiday
- Custom
- Off-Hours

Hours for on-hours and custom schedules are configurable. Holiday schedules let you identify the days when your organization is otherwise not open for business. Off-hours are considered all time that is not entered in the other schedules.

The following logic determines which schedule is active:

1. The auto attendant first looks for the Custom schedule.
2. If a Custom schedule has not been configured, the auto attendant or hunt group looks for the Holiday schedule.
3. If the Custom or Holiday schedule have not been configured, the auto attendant or hunt group looks for the On-Hours schedule.
4. If the Custom, Holiday, or On-Hours schedule have not been configured, the auto attendant or hunt group looks for the Off-Hours schedule.

Connect Director forms the Off-Hours schedule from all the hours not scheduled in the other modes. If you do not create a schedule for at least one of the other modes, the On-Hours schedule includes all hours.

18.2 Configuring the On-Hours Schedule

The default On-Hours schedule does not specify any days or hours. To use the default schedule (On-Hours), you must populate it by clicking Add to add days and editing the Start time and Stop time for each day as appropriate.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Schedules** > **On-Hours**. The **On-Hours** page appears.
3. Do one of the following:

   - To create a new schedule, click **New**.
   - To edit an existing on-hours schedule, click the name of the schedule.

Note:

In the **Details** pane, the **General** tab displays parameters for the new or existing schedule. For details about the parameters, see On-Hours Page: General Tab.

4. Provide or edit the values on the **General** tab as follows:

   - For a new schedule, do the following:

     - Provide a name in the **Name** field.
     - Optionally, select the time zone from the **Time zone** drop-down list.
     - Remove days from the schedule by clicking **Remove** on the row for that day.
     - Change the **Start time** and **Stop time** for each day as desired, or click **All Day** to specify a 24-hour period on a particular day.
   - To edit an existing schedule, do any of the following:

     - If desired, change the schedule name in the **Name** field.
     - If desired, select a different value from the **Time zone** drop-down list.
     - Add or remove days by clicking **Add or Remove** and selecting a day from the drop-down list.
     - If desired, change the **Start time** and **Stop time** for each day, or click **All Day** to specify a 24-hour period on a particular day.

Note:
You can schedule multiple start and stop times in one day by clicking Add to add more rows and modifying the Start time and Stop time in each row accordingly. For example, on Monday, you can set the schedule to start at 8:00 A.M. and stop at 11:30 A.M. and then add another row for Monday that starts at 1:30 P.M. and stops at 5:30 P.M.

5. Click **Save**.

Table 149: On-Hours Page: General Tab

Parameter	Description
Name	The name of the On-Hours schedule. You can enter a name in this field for a new schedule or edit it for an existing On-Hours schedule.
Time zone	The time zone that applies to the schedule. This option allows you to create a schedule that differs from the server's time zone. Select a value from the drop-down list.
Add	Click **Add** to add a new element in the On-Hours schedule. A new row appears on the page, and you can enter details for the schedule element.
Day	The day of the week to be included in this On-Hours schedule. By default, all seven days of the week are included, but you can add or delete days as needed.
All Day	Click **All Day** to change both the start and stop times to 12:00 am, indicating a 24-hour period of time.
Start Time	This displays the start time of this element of the On-Hours schedule. Enter the start time of a new On-Hours schedule element or edit the start time of an existing schedule element. The format is HH:MM:SS am or pm.

Parameter	Description
Stop Time	This displays the end time of a Custom schedule. Enter the end time of a new Custom schedule or edit the end time of an existing schedule. The format is HH:MM:SS am or pm.
Remove	Click **Remove** to remove a schedule row from the page.

18.3 Configuring the Holiday Schedule

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Schedules** > **Holiday**. The **Holiday** page is displayed.
3. Do one of the following:
   - To create a new Holiday schedule, click **New**.
   - To edit an existing Holiday schedule, click the name of the schedule.

> **Note**:
> In the **Details** pane, the **General** tab displays parameters for the new or existing schedule.

4. Provide or edit the values on the **General** tab as follows:
   - For a new Holiday schedule, do the following:
     - Provide a name in the **Name** field.
     - Optionally, select the time zone from the **Time zone** drop-down list.
     - Click **Add** to add a holiday, and repeat as necessary.
     - Provide values for the parameters described in the following table.
   - To edit an existing Holiday schedule, do any of the following:
     - Change any of the values as desired.
     - Add or remove holidays by clicking **Add** or **Remove**.
5. Click **Save**.

Table 150: Holiday Page: General Tab

Parameter	Definition
Name	Displays the name of the Holiday schedule. You can enter a name in this field for a new schedule or edit it for an existing Holiday schedule.
Time zone	Select the appropriate time zone from the drop-down list.
Add	Click **Add** to add a row for a holiday to the page.
Holiday	The name of the holiday
Yearly	Select this check box for holidays that you want to observe every year.
Date	Click in the data entry field to select a date from the calendar that is displayed or type a date in the format MM/DD or MM/DD/YYYY. If you enter only MM/DD, the same day and month is repeated every year.
Remove	Click **Remove** to delete a holiday from the page.

18.4 Configuring a Custom Schedule

1. Launch Connect Director.
2. In the navigation pane, click **Administration** >**Features** > **Schedules** > **Custom**. The **Custom** page is displayed.
3. Do one of the following:

   - To create a new Custom schedule, click **New**.
   - To edit an existing Custom schedule, click the name of the schedule.

Note:
In the **Details** pane, the **General** tab displays parameters for the new or existing schedule.

4. Provide or edit the values on the **General** tab as follows:

   - For a new Custom schedule, do the following:
     - Provide a name in the **Name** field.
     - Optionally, select the time zone from the **Time zone** drop-down list.
     - Click **Add** to add a row for the custom schedule, and repeat as necessary.
     - Provide values for the parameters described in the following table.
   - To edit an existing Custom schedule, do any of the following:
     - Change any of the values as desired.
     - Add or remove custom entries by clicking **Add** or **Remove**.

5. Click **Save**.

Table 151: Custom Page: General Tab

Parameter	Definition
Name	The name of the Custom schedule. You can enter a name in this field for a new schedule or edit it for an existing Custom schedule.
Time zone	Select the appropriate time zone from the drop-down list.
Add	Click **Add** to add a new element in the custom schedule. A new row appears on the page, and you can enter details for the schedule element.
Name	The name of the Custom schedule. Enter the name of a new Custom schedule or edit the name of an existing schedule in this field.

Parameter	Definition
Date	The date when the Custom schedule is to be used. Enter the date a new Custom schedule or edit the date of an existing schedule in this field. The format is MM/DD or MM/DD/YYYY. If you enter only MM/DD, the same day and month is repeated every year.
Start Time	This displays the start time of a Custom schedule. Enter the start time of a new Custom schedule or edit the start time of an existing schedule. The format is HH:MM:SS am or pm
Stop Time	This displays the end time of a Custom schedule. Enter the end time of a new Custom schedule or edit the end time of an existing schedule. The format is HH:MM:SS am or pm
Remove	Click **Remove** to remove a schedule row from the page.

Configuring Workgroups 19

This chapter contains the following sections:

This chapter describes how to create a workgroup and configure all parameters that relate to workgroups.

19.1 Overview

A workgroup is a group of agents that receives incoming calls. Workgroups use Automatic Call Distribution (ACD) to distribute incoming calls to the workgroup members. In a large enterprise, a workgroup can function as a small to medium-sized contact center.

A maximum of 256 workgroups can be created on each MiVoice Connect system.

The Mitel Workgroups feature provides the following functionality:

- Distributes calls to agents within a workgroup and places calls in a call waiting queue as needed
- Supports workgroups with a maximum of 300 members, including agents and supervisors
- Provides reports on workgroup activity

Note:
The Mitel Workgroups feature is not available for conference calls.

Example:

Assume that System #1 has two Workgroup agents/members, which are members of 100 different Workgroups. Each Workgroup membership is counted to be within the 300 member maximum. Therefore, System #1 has used 200 agents/members and 100 of the maximum number of created Workgroups (100 Workgroups out of 256 maximum limit). System #1 is within specifications.

Assume that System #2 has configured two Workgroup agents/members, which are each joined to 200 different Workgroups. Therefore, System #2 has 400 enrolled Workgroup

agents total, which exceeds the maximum number of agents/members (which is, 300). Therefore, System #2 is out of specification because it exceeds the maximum number of agents/members, even though the number of Workgroups created is acceptable (200 Workgroups of 256 maximum limit).

19.1.1 Call Routing for Workgroups

In general, callers reach a workgroup in one of the following ways:

- By calling through a dedicated trunk that connects at the workgroup site
- By calling a Direct Inward Dialing (DID) number or Dialed Number Information Services (DNIS) number that is directed to the workgroup
- Through an auto-attendant menu
- By dialing an internal extension

19.1.1.1 Call Distribution

The Workgroups feature has flexible boundaries for distributing calls to a workgroup. The system can be configured to send a warning to the workgroup if inbound calls reach excessive levels or stay in the call-waiting queue too long. The system administrator defines the thresholds for sending warnings.

Mitel's implementation of Automatic Call Distribution (ACD) supports four configurable patterns for distributing inbound calls to agents in a workgroup. When no agent is available, calls can be directed to a voice mailbox for the workgroup, which all agents can access, or to a queue where calls wait until an agent is available.

The following call distribution options are available:

- **Top Down** always starts with the first agent in the active agent list and sequentially searches through the list until an available agent is found.
- **Round Robin** starts with the next available agent in the active agent list and sequentially searches through the list until an available agent is found. The search starts with the agent that is next in the list after the agent that last received a call. If an available agent is not found, the search starts again at the beginning of the active agent list.
- **Longest Idle** sends the call to the agent with the longest idle time.
- **Simultaneous** sends the call to all available agents simultaneously.

Agents are available to receive calls when they have a status of logged in; agents with a status of logged out or wrap-up do not receive calls.

When no agents are available to take a call, the following call overflow options are available:

- **Forward** to forwards calls to a specified extension or external number.

- **Queue** sends calls to the call-waiting queue.

Note:

The following registry key must be created and set to 1 for transferring workgroup queue calls to call forwarding logged out destination when all the agents are logged out.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\WGSvc type
REG_DWORD EnableAllAgentsLoggedOutTransfer = 1.
```

19.1.2 Connect Client Workgroups

The Connect client provides the call-related information that contact center representatives need. The Connect client also provides point-and-click control of voice communication with callers and a large number of customizable buttons whose functions are specific to workgroups.

Connect client provides real-time call information such as Caller ID, call duration, and call states to agents and supervisors. A call's detailed routing information also appears globally so that agents know about every other employee in the enterprise with whom the current caller spoke before reaching the contact center. Additionally, the contact center's mailbox appears to every agent for accessing and helping a caller who chooses to leave a message rather than wait for an agent.

Agents and supervisors have access to the real-time Queue Monitor function. This function provides current information on the activities of the contact center queue. It displays the number of callers, information about each caller, and the time callers have been waiting.

The Agent Monitor lets the supervisor manage the workgroup agents. It lets the supervisor see the current login status of all agents and the state of the agents' call involvement. Agent Monitor also lets the supervisor change the status of any agent.

The following sections summarize the Connect client workgroup features.

19.1.2.1 Connect Client Applications

- Display Caller ID, call duration, and call state
- Display detailed routing information for calls
- Display and access the shared contact center voice messages
- Provide point-and-click access to the system's call routing features

- Log in and log out of the workgroup call flow

19.1.2.2 Real-Time Queue Monitor

- Display a summary of the number of callers waiting and the longest wait time
- Show a detailed view of the information about each waiting call
- Display or control the availability state
- Display warnings when the number of calls or longest wait time exceeds the supervisor's thresholds

19.1.2.3 Supervisor's Agent Monitor

- Display the current login status of the agents in the workgroup
- Show whether agents are on a call and how long they have been talking
- Control agent's login status from the supervisor's position

19.1.3 Workgroup Reports

The MiVoice Connect system tracks all call activity and places Call Detail Records (CDRs) in a database and a text file on the server. The system uses the records to generate CDR reports. This information can help a supervisor manage call flows and workgroup resources. The log for each call shows the following information:

- How long the call stayed in the queue
- How the call ended
- Which agent took the call
- How long the call lasted

The following workgroup reports are available:

- Agent Summary Report
- Agent Detail Report
- Service Level Summary Report
- Queue Summary Report

See CDR Reports on page 993for more information about workgroup reports.

19.2 Configuring Workgroups

This section describes how to add or modify a workgroup. For information about configuring distributed workgroups, see Distributed Workgroups on page 658.

19.2.1 Viewing Workgroups

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Workgroups**. The **Workgroups** page opens.

Note:
For descriptions of the columns in the list pane on the Workgroups page, see the following table.

Table 152: Columns in the List Pane on the Workgroups Page

Parameter	Definition
Name	Name of the workgroup.
Extension	The workgroup extension.
Workgroup Server	The server that hosts the workgroup.
Mailbox Server	The server that hosts the workgroup's mailbox.
Agents	The number of agents in the workgroup. The maximum number of agents for a Mitel system is 300; a single workgroup can have a maximum of 300 members, including agents and supervisors. However, if the workgroup has the Class of Service (COS) configured with the telephony feature **Allow additional phones to ring simultaneously and to move calls** enabled, the maximum number of agents for the workgroup is 16. Agents can belong to multiple workgroups. For example, an agent can belong to a workgroup that has this telephony feature enabled and to a different workgroup that does not have this feature enabled.

Parameter	Definition
Availability	The schedule currently in use by the workgroup.
On-Hours	The On-Hours schedule selected for the workgroup.
Holiday	The Holiday schedule selected for the workgroup.
Custom	The Custom schedule selected for the workgroup.

19.2.2 Adding or Editing a Workgroup

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Workgroups**. The **Workgroups** page opens.
3. Do one of the following:

   - To edit an existing workgroup, click the name of the workgroup in the list pane.
   - To create a copy of an existing workgroup, click **Copy**.
   - To create a new workgroup, click **New**.

   Note:
   The **General** tab in the **Details** pane displays parameters for the new or existing workgroup.

4. Review the parameters on all of the tabs in the details pane, and specify values as appropriate.

   Note:
   For more information about all of the workgroup parameters on the various tabs of the details pane, see Workgroup Parameters on page 634.

5. Click **Save**.

19.2.3 Workgroup Parameters

A workgroup has many details. You configure workgroup parameters on the following tabs, which you can access on the details pane for a particular workgroup:

- General Tab on page 634
- Routing Tab on page 639
- Voice Mail Tab on page 645
- Members Tab on page 649
- Queue Handling Tab on page 651
- DNIS Tab on page 656

19.2.3.1 General Tab

General information about new and existing workgroups is provided on the **General** tab of the **Workgroups** page.

The following table describes the parameters on the **General** tab of the **Workgroups** page.

Table 153: Workgroups Page: General Tab

Parameter	Definition
Name	Specifies the name of the workgroup.
Extension	Specifies the workgroup's extension. **Note**: Each workgroup must have a unique extension number. A MiVoice Connect system can support up to 256 workgroup extensions.
Show References	Click to display a list of everywhere this extension is used.

Parameter	Definition
Backup extension	Specifies the workgroup's backup extension. The backup extension supports back-up call routing in case of a system failure. This extension can be a hunt group, another workgroup, an agent's extension, or an auto attendant. If a call is not answered by the workgroup because of a system malfunction such as an unavailable server or network problem, the call is routed to the backup extension. The type of extension to use for backup depends on the expected traffic volume. • If expected call volume is low, the backup extension can direct to a single agent extension. • If expected call volume is high, it is recommended that the backup extension direct to a must-answer line with a distinctive ring. Agents can use the call pickup feature to answer calls from the must-answer line if the workgroup server is unavailable.
Include in System Dial By Name directory	Select this check box if you want the workgroup to be included in the auto-attendant's dial-by-name directory.
Make extension private	Select this check box to remove this number from the system directory and call routing destination lists. For more information about private numbers, see Configuring Private Extensions on page 547.
DID Settings	Click **change settings** to display the following DID settings: • Enable DID • DID Range • DID number
Enable DID	Select this check box to authorize a workgroup to use a DID number.

Parameter	Definition
DID Range	If a workgroup is authorized for a DID, in the drop-down list select a DID range for the user. Before you can specify a DID range, DID services must be configured for the desired trunk group, which is enabled by default if a DID trunk group is configured.
View System Directory for DID usage	Click this link to view the System Directory page, with directory details for this workgroup.
DID number	Specifies the DID number for the workgroup.
User group	In the drop-down list, select the user group to associate with the workgroup. The workgroup inherits Class of Service (COS) permissions from the selected user group. For information about selecting the COS for a user group, see Specifying a Class of Service on page 461.
Server	In the drop-down list, select the server to host the workgroup. **Note**: If Distributed Database is enabled, only the Headquarters server can host the workgroup.
Language	In the drop-down list, select the language to use for Workgroup prompts.

Parameter	Definition
Enable mailbox	Select this check box to enable voice mail for the workgroup. **Note**: If a system administrator changes the extension number of a workgroup that has an associated mailbox, the system retains the voice mail messages.
Mailbox server	In the drop-down list, select the server to host the workgroup's voice mailbox. The server hosting the workgroup can also host the workgroup's voice mailbox. If later, the mailbox server is changed to another server, all voice mail messages are automatically moved to the new mailbox server. Calls to a workgroup that are directed to voice mail go to the workgroup voice mailbox. Calls that are forwarded out of the workgroup to another extension and then are directed to voice mail go to the individual voice mailbox for that extension. All workgroup members running the Workgroup Agent, Supervisor Client, and Connect client share access to the workgroup voice mailbox. Workgroup members can log in to the workgroup voice mailbox from a phone using the mailbox number and voice mail password.

Parameter	Definition
Workgroup name	Use the following buttons to record, import, and play back the workgroup name: • Click **Record** to record the workgroup name. **Note**: You cannot record prompts if you log in to Connect Director in Https or Http mode. This issue also occurs when you log in using Internet Explorer. To resolve this issue, do the following: • For Https mode, log in to Remote Desktop and open Connect Director in Https mode using Chrome as the browser. • For Http mode, log in to Remote Desktop or outside the Remote Desktop connection and open Connect Director in Http mode using either Internet Explorer or Chrome as the browser. • Click **Play** to listen to the recording. • Click **Import** to import a recording of the workgroup name from an existing file. **Note**: Imported prompts must be CCITT µ-Law, 8 KHz, 8-bit, mono WAV files. By using the system recorder and a plug-in microphone, the recording meets these requirements by default. • Click **Preferences** to select whether to use your PC or your phone to play back your recording; you can also select a phone extension or external number to use to record the workgroup name. This recording of the workgroup name is used as a part of the default mailbox greeting, as well as for the Dial By Name directory.

Parameter	Definition
Enable automatic agent logout on ringno answer	Select this check box to automatically log out agents who do not answer a workgroup call after a specified number of rings. **Note**: The purpose of this function is to prevent calls from repeatedly being routed to an agent who is logged in to the workgroup but is not answering calls.
Wrap up time	Specifies the number of seconds to allow for an agent to wrap up after each call. This allows the agent time to complete post-call tasks before the system presents another call. A wrap-up time of 0 disables the wrap-up feature.
Current schedule	Displays the schedule currently in use by the workgroup.

19.2.3.2 Routing Tab

Information about call routing features for workgroups is provided on the **Routing** tab in the details pane of the **Workgroups** page. Routing is configured separately for different schedules using the schedule subtabs. The **Routing** tab includes the following subtabs:

- On-Hours
- Off-Hours
- Holiday
- Custom

For information about configuring schedules, see Overview on page 621.

The following table describes the parameters on the **Routing** tab of the **Workgroups** page.

Table 154: Workgroups Page: Routing Tab

Parameter	Definition
Schedule	(Not available for Off-Hours) In the drop-down list, select the schedule to use for the workgroup. Click **View schedule** to view details for the selected schedule.
Distribution pattern	Select one of the following options for distributing incoming calls to agents in the workgroup: • **Top Down** starts with the first agent in the active agent list and sequentially searches through the list until an available agent is found. • **Round Robin** starts with the next available agent in the active agent list and sequentially searches through the list until an available agent is found. The search starts with the agent that is next in the list after the agent that last received a call. If an available agent is not found, the search starts again at the beginning of the active agent list. • **Longest Idle** sends the call to the agent with the longest idle time. • **Simultaneous** sends the call to all available agents simultaneously. • For information about changing the order of the active agent list, see Changing the Position of an Agent in the Active Agent List on page 650.
Call forward	Select one of the following options for forwarding calls for the selected schedule: • **Always** automatically forwards all calls to the specified destination. • **No Answer/Busy** forwards the call to the specified destination if the line is busy or the call goes unanswered after the specified number of rings.

Parameter	Definition
Always	Specifies the destination for forwarded calls. The destination can be an extension or an external number. If the destination is an external number, the access code must be included. **Note**: This option is available only when the **Call forward** parameter is set to **Always**.
Busy	Select one of the following destinations for forwarded calls when all agents are busy: • **Forward to** forwards calls to a specified extension or external number; if the destination is an external number, the access code must be included. • **Queue** sends calls to the call waiting queue. For more information about the call waiting queue, see Queue Handling Tab on page 651. **Note**: These options are available only when the **Call forward** parameter is set to **No Answer/Busy**.

Parameter	Definition
No answer	Select one of the following destinations for forwarded calls when a call goes unanswered: • **Forward to** forwards calls to a specified extension or external number; if the destination is an external number, the access code must be included. • **Queue** sends calls to the call waiting queue. For more information about the call waiting queue, see Queue Handling Tab on page 651. **Note**: These options are available only when the **Call forward** parameter is set to **No Answer/Busy**.
Forward after	Specifies the number of times to ring the line before forwarding the call. The call is forwarded as defined by the **No answer** parameters. **Note**: This option is available only when the **Call forward** parameter is set to **No Answer/Busy**.
Rings per agent	Specifies the number of times to ring an agent's phone before forwarding the call to the next available agent. **Note**: This option is only available when **Call forward** is set to **Answer/Busy**.

Parameter	Definition
Logged out	Select one of the following destinations for calls when all agents are logged out: • **Forward to** forwards calls to a specified extension or external number; if the destination is an external number, the access code must be included. • **Queue** sends calls to the call waiting queue. For more information about the call waiting queue, see Queue Handling Tab on page 651.
Escalation profile	In the drop-down list, select the escalation profile for the selected schedule. For more information about escalation profiles, see Configuring Escalation Notification on page 597.

Parameter	Definition
Workgroup greeting	Use the following buttons to record, import, and play back the workgroup greeting for the selected schedule: • Click **Record** to record the mailbox greeting. **Note**: You cannot record prompts if you log in to Connect Director in Https or Http mode. This issue also occurs when you log in using Internet Explorer. To resolve this issue, do the following: • For Https mode, log in to Remote Desktop and open Connect Director in Https mode using Chrome as the browser. • For Http mode, log in to Remote Desktop or outside the Remote Desktop connection and open Connect Director in Http mode using either Internet Explorer or Chrome as the browser. • Click **Play** to listen to the recording. • Click **Import** to import a recording of the workgroup greeting from an existing file. **Note**: Imported prompts must be CCITT µ-Law, 8 KHz, 8-bit, mono WAV files. By using the system recorder and a plug-in microphone, the recording meets these requirements by default. • Click **Preferences** to select whether to use your PC or your phone to play back your recording; you can also select a phone extension or external number to use to record the workgroup greeting. This recording of the workgroup greeting is used the default workgroup mailbox greeting.

Parameter	Definition
Assistant	Specifies the workgroup assistant extension. When a caller connects to the workgroup's voice mail and presses "0," the call is forwarded to the specified extension.
Enable message notification	Select this check box to activate message notification for the workgroup's voice mailbox for the selected schedule. **Note**: This option must be enabled in order for escalation profile to work.

19.2.3.3 Voice Mail Tab

Voice mail information for new and existing workgroups is provided on the **Voice Mail** tab on the **Workgroups** page. This tab contains the **Mailbox** and **Escalation Profiles** subtabs.

19.2.3.3.1 Mailbox Subtab

The following table describes the parameters on the **Voice Mail** tab and **Mailbox** subtab of the **Workgroups Details** pane.

Table 155: Workgroups Page: Voice Mail Tab, Mailbox Subtab

Parameter	Description
Voice mail password	Specifies the password that users enter when logging into the workgroup voice mailbox from the telephone. Characters in this field appear as asterisks. For more information about setting passwords, see Voice Mail Password Recommendations on page 517
Accept broadcast messages	Select this check box to allow the workgroup to receive broadcast messages. This is enabled by default.

Parameter	Description
Email address	Indicates the user's email address, which was configured on the **General** tab of the Users page.
Delivery type	Specifies whether and how voice mail messages are sent through email. Select one of the following options: • **Disabled**: Voice mail messages are not sent. • **Email text only**: The system sends an email message that notifies the user of the time, duration, and caller ID for the message that was recorded. • **Attach WAV file**: The system attaches the voice mail message to an email message as a WAV file.
Mark message as heard	Select this check box to have the system mark emailed messages as heard.
Send email warning when mailbox is full	Select this check box to have the system send users a notice informing them that their mailbox is almost full.
Automatic message forwarding	
Destination	Specifies the destination for forwarded voice mail messages. Select one of the following options: • **None**: Voice mail messages are not forwarded. • **Mailbox**: Specify the target mailbox for forwarded messages. • **AMIS Mailbox**: Specify the target AMIS mailbox for forwarded messages.
Delete message after forwarding	Select this check box to automatically delete each message after it is forwarded. This option is disabled by default, meaning messages are not deleted after forwarding.

19.2.3.3.2 Escalation Profiles Subtab

The following table describes the parameters on the **Voice Mail** tab and **Escalation Profiles** subtab of the **Workgroups Details** pane.

Table 156: Workgroups Page: Voice Mail Tab, Escalation Profiles Subtab

Parameter	Description
Escalation notification options	Select one of the following options: • **Escalate for each message** - to begin escalation notification each time a new voice mail message arrives in the voice mailbox. If several messages arrive within a short period of time, users who are notified will receive multiple notifications. • **Escalate for first unheard message** - to begin escalation notification only when the first unheard voice mail message arrives in the voice mailbox. Subsequent unheard messages do not trigger another wave of notifications as long as the first message remains unheard.
Profile subtabs	
Profile name	Specifies the name of the escalation profile.
Repeat count	Specifies the number of times the system loops through the 10 steps of this profile before it stops trying to contact the various notification members. Select 0 to execute the escalation profile steps once without repeating. Select one to execute the steps of the profile twice — the initial execution and one repetition. **Note**: This parameter does not apply if you select one of the Notification by email options.

Parameter	Description
Step subtabs	There is a subtab for each step in a profile; there are a maximum of 10 steps for each escalation profile.
Timeout	Specifies the amount of time, in minutes, that elapses before the next step in the profile is executed. This is the amount of time a message recipient has to respond to the original voice mail before escalation occurs.
Urgent only	Select this check box to send notification only when the escalation is determined to be urgent.
Notification by email	
Deliver message as email	Select one of the following three email delivery options: • **Disabled** - to not send email notification. • **Email text only** - to send a text email to the designated user's email inbox. The email message contains basic information about the voice mail message, such as the time, duration, and Caller ID of the message that was recorded. • **Attach WAV file** - to send an email containing a copy of the recorded voice mail message to the designated user's email inbox. The recipient can play the message on his or her PC.
Email address	Specifies the email address to send notification to.
Notification by phone	
Voice mail notification method	Select one of the following phone notification methods: • **Pager** • **Phone** • **None**

Parameter	Description
Notification number	Specifies the phone or pager number to send notification to.
Pager ID	Specifies the pager pin number required to access the recipient.
Pager data	Specifies the code the recipient requires to indicate that a page is waiting.

19.2.3.4 Members Tab

On the Members tab of the **Workgroups** page, you can add and remove agents from a workgroup, change the order of the active agent list, and change an agent's status.

Note:
A single workgroup can have a maximum of 300 members. However, if the workgroup has the Class of Service (COS) configured with the telephony feature **Allow additional phones to ring simultaneously and to move calls** enabled, the maximum number of agents for the workgroup is 16.

The Workgroups Page: Members Tab describes the parameters on the **Members** tab of the **Workgroups** page.

19.2.3.4.1 Adding or Removing an Agent from the Workgroup

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features**> **Workgroups**. The **Workgroups** page opens.
3. In the **Details** pane, click the **Members** tab.
4. Do one of the following:

   - To add an agent to the workgroup, select the agent in the **Available** list and click the right arrow button to move the agent to the **Selected** list.
   - To remove an agent from the workgroup, select the agent in the **Selected** list and click the left arrow button to move the agent to the **Available** list.

5. Click **Save**.

19.2.3.4.2 Changing the Position of an Agent in the Active Agent List

If the call distribution pattern is **Top Down** or **Round Robin**, the position of the member in the workgroup list can affect how likely that user is to receive an incoming call.

When **Top Down** is selected, it is more likely that agents closer to the top of list will be selected to receive a call. This is because for each new call, the hunt for a free agent always begins at the top of the list.

When **Round Robin** is selected, the position of an agent in the list can also affect the likelihood that the particular agent will be selected to receive a call. This is because for each new call, the hunt for a free agent moves down the list, starting with the agent that immediately follows the last agent to accept a call. For example, if Agent 12 is higher in the list than Agent 18 and Agent 19, and if a call comes into the workgroup while Agent 12 is busy and Agent 18 and Agent 19 are free, Agent 18 is more likely to receive the call.

For information about changing the call distribution pattern, see Routing Tab on page 639.

To change the position of an agent in the active agent list:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Workgroups**. The **Workgroups** page is displayed.
3. In the **Details** pane, click the **Members** tab.
4. Select the agent to move in the **Selected** list, and then do one of the following:
   - Click the up arrow button to move the agent up in the list.
   - Click the down arrow button to move the agent down in the list.
5. Click **Save**.

19.2.3.4.3 Changing an Agent's Log In Status

1. Launch Connect Director.
2. In the navigation pane, click **Administration** >**Features** > **Workgroups**. The **Workgroups** page opens.
3. In the details pane, click the **Members** tab.
4. Select the agent in the **Selected** list.
5. Under **Select agent state**, select the desired status for the agent.

The following table describes the parameters on the **Members** tab of the **Workgroups** page.

Table 157: Workgroups Page: Members Tab

Parameter	Definition
Available	Displays the extension and name for each user that is available to add to the workgroup.
Selected	Displays the extension and name for each user that is a member of the workgroup.
Select agent state	Specifies the agent's status: • **Logged Out** • **Logged In** • **In Wrap Up**

19.2.3.5 Queue Handling Tab

Call queue configuration provides additional flexibility for managing the call flow. Incoming calls to a workgroup enter the call queue and remain in the queue until an agent takes the call. Calls are routed to the call queue according to the routing parameters. For more information about call routing, see Routing Tab on page 639.

Queue handling information for new and existing workgroups is provided on the **Queue Handling** tab on the **Workgroups** page.

The following table describes the parameters on the **Queue Handling** tab.

Table 158: Workgroups Page: Queue Handling Tab

Parameter	Definition
Calls in queue warning	Specifies the threshold for the number of calls in the queue. Once this threshold is met, a warning is sent via the Connect client to all agents in the workgroup. This value must be a number 1-999.

Parameter	Definition
Calls waiting time warning	Specifies the threshold for the waiting time of calls in the queue. Once this threshold is met, a warning is sent via the Connect client to all agents in the workgroup. This value must be a number 0-3600.
Allow agents to pick up from queue	Select this check box to allow agents to answer a specific call in the queue. **Note**: If this check box is cleared, agents can still view all calls in the queue, but cannot select a call to answer. Calls continue to be distributed according to the routing parameters.

19.2.3.5.1 Queue Handling Tab, Step *n* Subtab

There are a maximum of five steps that a call can be routed through once the call reaches the call queue. Each of the subtabs on the **Queue Handling** tab represents one of the five steps.

Each step requires a recorded prompt and can specify different caller interactions and give the caller the ability to select where the call is routed. Only Step 5 is required; any of the first four steps can be skipped.

The following table describes the parameters on the **Queue Handling** tab and Step *n* subtabs of the **Workgroups** page.

Table 159: Workgroups Page: Queue Handling Tab, Step n Subtab

Parameter	Definition
Skip this step	Select this check box to skip the selected step. **Note**: This option is not available for step 5, the final step.
Announce estimated wait time	Select this check box to announce the estimated wait time to callers in this step of the queue. For information about how the system calculates wait time, see Computing the Estimated Wait Time on page 657.
Time until next step	Specifies the number of seconds that the system waits before sending the call to the next step in the queue. Callers hear the main site's music on-hold (MOH) during this period and cannot initiate operations using the phone buttons.
Prompt text	Specifies the content of the recorded prompt. This is useful when recording prompts from a PC.

Parameter	Definition
Workgroup greeting	Use the following buttons to record, import, and play back the prompt for the selected step in the queue: • Click **Record** to record the prompt. **Note**: You cannot record prompts if you log in to Connect Director in Https or Http mode. This issue also occurs when you log in using Internet Explorer. To resolve this issue, do the following: • For Https mode, log in to Remote Desktop and open Connect Director in Https mode using Chrome as the browser. • For Http mode, log in to Remote Desktop or outside the Remote Desktop connection and open Connect Director in Http mode using either Internet Explorer or Chrome as the browser. • Click **Play** to listen to the recording. • Click **Import** to import a recording of the prompt from an existing file. **Note**: Imported prompts must be CCITT µ-Law, 8 KHz, 8-bit, mono WAV files. By using the system recorder and a plug-in microphone, the recording meets these requirements by default. • Click **Preferences** to select whether to use your PC or your phone to play back your recording; you can also select a phone extension or external number to use to record the prompt.

Parameter	Definition
Operation/Destination	Specifies the actions that result from a caller pressing a button on the phone. **Note**: A prompt must be added for the selected step in order for assigned caller operations to function. Select one of the following operations for each phone button (0-9, *, and #): • **None** specifies that no operation occurs when the user presses this button. • **Repeat prompt** specifies that the recorded prompt is repeated when the user presses this button. • **Go to menu** specifies that the call is forwarded to the specified auto-attendant when the user presses this button; type the desired extension for the auto-attendant in the **Destination** column. • **Transfer to extension** specifies that the call is forwarded to the specified extension when the user presses this button; type the desired extension in the **Destination** column. • **Take a message** specifies that the call is forwarded to the specified voice mailbox extension when this button is pressed; type the desired extension in the **Destination** column. • **Hang up** specifies that the call ends when the user presses this button.

Parameter	Definition
Overflow/Interflow	(Available only for Step 5, the final step) Specifies the overflow or interflow extension to forward calls to after the calls have gone through all configured steps in the workgroup queue. • Overflow is a transfer from one workgroup queue to another, higher priority workgroup queue. • Interflow is a transfer to any external number; for example, a cell phone number for a supervisor. Typically an interflow extension is used after a series of overflows as the last step in a workgroup queue.
Maintain wait time	(Available only for Step 5, the final step) Select this check box to maintain total wait time when a call moves from one queue to another. If this check box is cleared, wait time for the call restarts when the call changes queues. **Note**: This feature is not available when a call interflows to an external number.

19.2.3.6 DNIS Tab

The following table describes the parameters on the **DNIS** tab on the Workgroups page.

Table 160: Workgroups Page: DNIS Tab

Parameter	Description
Add	To associate the workgroup with a DNIS, click **Add** and provide details for the DNIS mapping in the displayed fields.

Parameter	Description
Trunk group name	From the drop-down list, select the trunk group for the DNIS mapping.
Digits	Enter the DNIS number.
Description	Provide a description for the DNIS number. This description is seen by call recipients and in call detail reports (CDRs). The description length can be up to 26 characters.
Music on Hold	From the drop-down list, select a file-based MOH resource.
Remove	If you want to remove a DNIS system that is configured for this workgroup, click **Remove**.

19.2.4 Computing the Estimated Wait Time

You can choose to announce the estimated wait time to callers in the call waiting queue. This option can be configured for each step in the queue. The estimated wait time can be maintained throughout each step of the queue or can restart each time the call moves to the next step. For information about configuring the wait-time options, see Queue Handling Tab on page 651.

The approximate wait time is a moving average that depends on the duration of the previous calls. The wait time is approximate; the system rounds off the wait time to the nearest minute. The wait time is announced as a number of minutes, not a number of seconds.

The estimated wait time is determined based on the following two formulas in this order:

1. Average wait seconds = ((“Average wait seconds” * 9) + *“New wait time”*) / 10

   Where *New wait time* is the number of seconds the last caller waited before reaching an agent.
2. Announced wait time = *“Position in queue”* * “Average wait seconds”

   Where *Position in queue* refers to the position of the call in relation to other calls in the queue.

For example, after 10 calls, 61% of the calculated wait time depends on the 10 most recent calls. After 20 calls, 86% of the time is based on the last 20 calls. The announced wait time might be inaccurate during periods of low call volume or when call volume increases rapidly.

19.3 Distributed Workgroups

This section describes the operation and configuration of distributed workgroups. A distributed workgroup has greater availability and resilience than a regular workgroup because it has a significant level of independence from the Headquarters server.

The database of real-time and historical records resides on the Headquarters server, but if a remote server is disconnected from the Headquarters server, the agent logs remain in a buffer until the Headquarters server and the remote server reconnect. After the servers reconnect, the DVS sends the logs to the Headquarters server.

The following two types of distributed workgroups are available:

- A site-specific workgroup runs on a local DVS at a remote site. No part of this workgroup resides at other sites.
- A multi-site workgroup has the following features:
  - Spans multiple sites and servers (These servers can act as backup servers for each other).
  - Uses the Hunt Group feature to link workgroups into a single hunt group.

Note:

If a distributed workgroup loses connectivity to the Headquarters server, the agent members of that workgroup who were logged in at the time connectivity was lost continue to receive calls. In addition, any wrap-up time configured for those agents continues to be available to them.

No supervisor or system administrator can change an agent's state in the absence of Headquarters server connectivity. Furthermore, an agent's Connect client availability state cannot change in the absence of Headquarters connectivity; for example, an agent's availability state cannot change from Available to Do Not Disturb.

Two Mitel technologies enable distributed workgroups:

- The ability of a DVS to host a workgroup
- The ability of the Hunt Group feature to manage a multi-site workgroup

Note:

Voice mail switches can host a hunt group in support of distributed workgroups. However, these switch types cannot host the actual workgroup.

For general backup purposes, a backup extension can direct to a workgroup, hunt group, menu, or any system extension. However, to use a workgroup as a backup for another workgroup, the backup extension must direct to a hunt group.

The distributed workgroup capability is either on or off. If it is on, site-specific and multi-site workgroups are possible.

A MiVoice Connect system can support either distributed workgroups or Distributed Database (DDB), but not both at the same time. If a DVS is running a DDB, the DVS is not available for selection as a Workgroup server. If DDB is enabled, the distributed workgroups cabability is disabled and the Headquarters server manages all workgroup calls whether the workgroup is on the Headquarters server or a DVS. In this case, if the Headquarters server becomes unavailable, all workgroups in the network are also inoperative.

Note:

To verify that a DVS is not running a distributed database, click **Maintenance > Status > Servers** to display the Servers status page. If the DVS is running a distributed database, there is a green database icon in the DB column. For more information about distributed databases, see Mitel Distributed Database on page 140.

19.3.1 How Hunt Groups Facilitate Multi-Site Workgroups

This section describes the benefits of using the Hunt Group feature to support a distributed workgroup. Using a hunt group to support a distributed workgroup can keep a multi-site workgroup in operation when it would otherwise fail if only supported by the Headquarters server.

The following figure shows three separate workgroups (250, 251 and 252). These workgroups are part of a distributed workgroup because they are not on the Headquarters server. However, these workgroups are set up to back up each other using backup extensions as follows:

- Workgroup 250 is on SVR1. The backup for this workgroup is Workgroup 251.

- Workgroup 251 is on SVR2. The backup for this workgroup is Workgroup 252.
- Workgroup 252 is on SVR3. The backup for this workgroup is Workgroup 250.

Link failures in the following two scenarios illustrate the limitations of this type of backup when connectivity to the WAN is lost. In the first example, Link 1 fails. In the next example, Link 3 fails.

If WAN Link 1 fails, the following applies:

- The server and switches still connect to each other; Trunk Group 1 can still reach all the agents that SVR1 manages.
- Agents on the switches that SVR2 and SVR3 manage are not available to SVR1.

If WAN Link 1 fails and a call arrives on Trunk Group 2, the following applies:

- The call is unable to reach Workgroup 250 on SVR1.
- The switch routes the call to the backup workgroup, Workgroup 251 on SVR2.
- Across the WAN, the agents that SVR3 manages are unavailable.

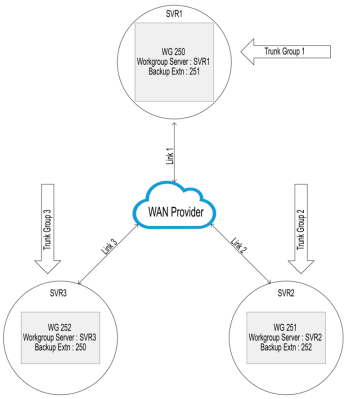
If WAN Link 1 fails and a call arrives on Trunk Group 3, the following applies:

- The call for Workgroup 250 is unable to reach Workgroup 250 on SVR1.
- The switch routes the call to the backup workgroup, Workgroup 251 on SVR2.

In the next example, WAN Link 3 in the below figure is down. A call arrives on Trunk Group 1 and Trunk Group 2 for Workgroup 250:

- The call is unable to reach agents at SVR1 and SVR2.
- Any agent that SVR3 manages is unavailable.
- Furthermore, a call that arrives on Trunk Group 3 for Workgroup 250 is unable to reach Workgroup 250 on SVR1. The backup extension for Workgroup 250 is Workgroup 251, but Workgroup 251 is also unavailable. In this situation, calls eventually go to the backup auto attendant on the switch.

Figure 18: Lost Connectivity without a Distributed Work Group



As the below figure shows, the members of Hunt Group 261 are workgroups 250 and 251.

For the calls that arrive on Trunk Group 2:

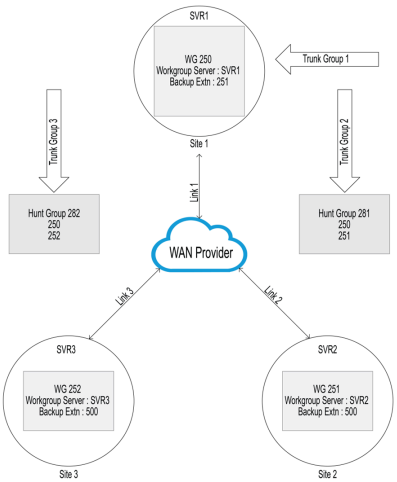
- The calls go to Hunt Group 261.
- Initially, Hunt Group 261 forwards the calls to Workgroup 250.
- If no agents in Workgroup 250 answer a call (for any reason), the switch with Hunt Group 261 forwards the call to Workgroup 251 at Site 2.

At Site 3 in the following figure, Hunt Group 262 supports workgroups 250 and 252. Calls enter the network on Trunk Group 3 and go to Hunt Group 262. Calls that arrive on Trunk Group 3 go to Workgroup 250. If no agent in Workgroup 250 answers the call, it goes to Workgroup 252 at Site 3.

Returning to the scenario with WAN Link 1 down but with Hunt Groups providing the Distributed Workgroup capability, again refer to the below figure:

- Calls that arrive on Trunk Group 3 go to Workgroup Extension 252.
- Calls that arrive on Trunk Group 2 got to Workgroup Extension 251.
- Notice that if the Mitel loses connectivity to the WAN, calls still enter the local workgroup at the local site.

Figure 19: Hunt Groups Supporting Distributed Workgroups



19.3.2 Configuring a Distributed Workgroup

This section describes how to configure a site-specific workgroup and a multi-site workgroup.

19.3.2.1 Configuring a Site-Specific Workgroup

With a site-specific workgroup, the local switch forwards an incoming call to the workgroup's extension. If the workgroup extension is unreachable because of a server or WAN failure, the switch routes the call to the backup extension. This backup extension can direct to a workgroup, hunt group, menu, or any agent or system extension.

To configure a site-specific workgroup:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Do one of the following:

   - To edit an existing DVS, click the name of the DVS in the list pane.
   - To add a new DVS, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the new or existing DVS.

4. Verify that the **Enable local database** check box is not selected, as explained in Distributed Workgroups on page 658.
5. After configuring all desired parameters for the DVS, click **Save**.

> **Note**:
> For information about configuring the remaining parameters for the DVS, see Overview on page 115.

6. In the navigation pane, click **Administration** > **Features** > **Workgroups**. The **Workgroups** page opens.
7. Do one of the following:

   - To edit an existing workgroup, click the name of the workgroup in the list pane.
   - To create a copy of an existing workgroup, click **Copy**.
   - To create a new workgroup, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing workgroup.

8. In the **Backup extension field**, enter the extension to support back-up call routing in case of a system failure.

Note:
For more detailed information about the backup extension, see General Tab on page 634.

9. In the **Server** drop-down list, select the local DVS to host the workgroup.

Note:
If a DVS is running a DDB, the DVS is not available in the Server drop-down list.

10. Review the parameters on all of the tabs in the details pane, and specify values as appropriate.

Note:
For more information about all of the workgroup parameters on the various tabs of the details pane, see Workgroup Parameters on page 634.

11. Click **Save**.

19.3.2.2 Configuring a Multi-site Workgroup

For a multi-site workgroup, you must configure all of the following system components in the following order:

1. Configure the servers. (For details, see Configuring Servers for a Multi-Site Workgroup on page 664).
2. Configure workgroups.

   For each workgroup in a multi-site workgroup, set the value of the **Backup extension** field to the hunt group extension. For a description of each parameter in a workgroup configuration, see Workgroup Parameters on page 634.

3. Configure hunt groups. For details, see Configuring Servers for a Multi-Site Workgroup on page 664. The steps in this section are for selecting the workgroup extensions that are to be members of the hunt group. A hunt group can have up to 24 workgroup members).

Note:

If at least one workgroup exists in a hunt group's membership list, the hunt group can use only the Top Down distribution pattern. Simultaneous distribution pattern can be used only if the hunt group members list contains no workgroups, route points, menus, or other hunt groups

19.3.2.2.1 Configuring Servers for a Multi-Site Workgroup

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Do the following for each DVS that will be part of the workgroup:

   a. Do one of the following:

   - To edit an existing DVS, click the name of the DVS in the **List** pane.
   - To add a new DVS, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing DVS.

   b. Verify that the Enable local database check box is not selected, as explained in Distributed Workgroups on page 658.

   c. After configuring all desired parameters for the DVS, click **Save**.

Note:
For information about configuring the remaining parameters for the DVS, see Overview on page 115.

19.3.2.2.2 Configuring Hunt Groups for a Multi-Site Workgroup

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Hunt Groups**. The **Hunt Groups** page opens.
3. Do one of the following:

   - To edit an existing hunt group, click the name of the hunt group in the **List** pane.
   - To create a copy of an existing hunt group, click **Copy**.
   - To add a new hunt group, click **New**.

   Note:
   The **General** tab in the **Details** pane displays parameters for the new or existing hunt group.

4. For the **Distribution pattern** option, select **Top-down**.
5. In the **On-hours schedule** drop-down list, select the desired on-hours schedule.

   Note:
   If **None** is selected, all calls are treated as if the schedule is on-hours.

6. On the **Members** tab, add the desired workgroup and other extensions to the hunt group.

   Note:
   For detailed information about adding hunt group members and changing the position of a member in the list, see Configuring Hunt Groups on page 389.

7. Click **Save**.

19.3.3 Important Considerations for Distributed Workgroups

This section describes operational details about the distributed workgroups.

19.3.3.1 Call Detail Record Reports

The remote server sends Call Detail Record (CDR) reports to the Headquarters server. If the remote server loses connectivity to the Headquarters server, the records enter a queue on the remote server until connectivity with the Headquarters server is regained. Remote servers keep the CDR records for a limited time while the Headquarters server is unavailable. The remote server uses the same time limit that the Telephony Management System (TMS) uses.

19.3.3.2 Call Routing Scheduling

For workgroups, call routing can vary with the system schedule. A user cannot use Connect client or an IP phone to initiate local changes to the call routing.

The call routing specifications combine with the system's scheduling facility to provide different responses to callers at different times. Each mode can support different options and transfer callers to different destinations when no agents are available. The scheduling facility determines the start and stop time of each call routing mode.

19.3.3.3 Hunt Group and Workgroup Scheduling

Scheduling for workgroups and hunt groups involves the calculation of the time zone offset that is necessary for the hunt group to be active at the same time as the workgroup.

Hunt Group schedule times depend on the Headquarters server time. Workgroup schedule times depend on the workgroup server time.

19.3.3.4 When the Headquarters Server Is Unavailable

Because distributed workgroups and distributed database are mutually exclusive, during a communication break from the Headquarters server, workgroup agents change states according to the configuration on the remote server. For example, if the workgroup wrap-up time is 10 seconds, that setting remains in effect. However, changes to agent states are not visible to monitors. In addition, neither the system administrator nor the agent can manually change the agent's state through either Connect client or an IP phone. Therefore, in effect, the remote workgroup uses the workgroup configuration to run automatically while the Headquarters server is unavailable.

Local IP phones and Connect client applications do not show the agent enter and leave wrap-up. If an agent is in a workgroup that is managed by a server that is outside the off-line site — in a multi-site workgroup, for example — the outside server also is not informed of agent state changes on the isolated, remote site.

Managing the System Directory 20

This chapter contains the following sections:

This chapter describes how you can view and manage the System Directory by using the Connect Director.

20.1 Overview

The system directory is a list of users and off-system contacts across your organization. This directory is read-only for general users. Only users with administrative privileges can make changes to the system directory.

The Connect client instantly populates each user's Quick Dialer with contacts from the system directory, the user's personal directory, and all Microsoft Outlook Contact folders. This includes each user's personal contacts as well as any contacts on the Microsoft Exchange Server.

By using Connect Director, you can view, create, edit, copy, export, and delete system directory contacts as explained in subsequent sections. This chapter does not deal with the creation of user accounts, which is explained in Configuring a User Account on page 488.

20.2 Viewing a System Directory Contact

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **System Directory**.

Note:
The **System Directory** page that is displayed is split into the **List** pane (top) and the **Details** pane (bottom). The **List** pane displays all the contacts in the system directory, with parameters as described in System Directory Page Parameter Descriptions. The **Details** pane allows you to view the details for a selected contact.

Note:
If you do not select a contact, by default the details of the first contact in the list are displayed.

You can sort the system directory by any of the parameters described in the table below, in the order of your choice (ascending or descending).

Table 161: System Directory Page Parameter Descriptions

Parameter	Definition
First Name	The first name of a user/directory contact.
Last Name	The last name of a user/directory contact.
Ext.	Extension number of a user/directory contact.
Type	Indicates the type of extension, including but not limited to the following: • User Extension • Local Voice Mail Extension • Distribution List • Account Code Extension • System Conference Extension • Auto-Attendant • Local Auto-Attendant
Site	The site where the extension is located.

Parameter	Definition
Trunk Group	Name of the trunk group associated with the extension number.
DID	Direct inward dialing (DID) number of the user/ directory contact.
Work	Work number of the user/directory contact. **Note**: This must not be the same as the extension number of the user/contact.
Home	Home number of the user/directory contact.
Fax	Fax number of the user/directory contact.
Cell	Cell number of the user/directory contact.
Pager	Pager number of the user/directory contact.
Company Name	Name of the company
Department Name	Name of the department

20.3 Creating a System Directory Contact

1. Launch Connect Director with administrative privileges.
2. In the navigation pane, click **Administration** > **Features** > **System Directory**.

Note:
The **System Directory** page that is displayed is split into the **List** pane (top) and the **Details** pane (bottom). The **List** pane displays all the contacts in the system directory, with parameters as described in System Directory Page Parameter Descriptions. The **Details** pane allows you to view the details for a selected contact.

3. Click **New** on the list pane, and type the required information on the details pane.

Note:
See the parameter descriptions in System Directory Page Parameter Descriptions above for entering the details. Note that external contact numbers entered in the **Home, Work, Fax, Cell** and **Pager** fields must include a country code (for example, +1 for the U.S.).

4. Click **Save**.

The information is saved in the directory and instantly updated in the list pane.

Note:
To create a copy of the non-Mitel entries in the System Directory, click **Copy**.

20.4 Exporting a System Directory Contact

To export a system directory contact, you must follow these steps:

1. Launch Connect Director with administrative privileges.
2. In the navigation pane, click **Administration** > **Features** > **System Directory**.

Note:

The **System Directory** page is displayed, which is split into the **List** pane (top) and the **Details** pane (bottom). The **List** pane displays all the contacts in the system directory, along with parameters as described in the table in the Viewing a System Directory Contact on page 667 section. The details pane allows you to view and edit the details for a selected contact.

3. Select the contact that you want to export into a CSV file, and click **Export**.

The information for the selected contact is downloaded as a CSV file to your local machine.

20.5 Importing a System Directory Contact

To import a system directory contact, you must follow these steps:

1. Launch Connect Director with administrative privileges.
2. In the navigation pane, click **Administration** > **Features** > **System Directory**.

Note:

The **System Directory** page is displayed, which is split into the **List** pane (top) and the **Details** pane (bottom). The **List** pane displays all the contacts in the system directory, along with parameters as described in the table in the Viewing a System Directory Contact on page 667 section. The details pane allows you to view and edit the details for a selected contact.

3. Select the contact that you want to import into a .xls file, and click **Import**.

The information for the selected contact is downloaded as a .xls file to your local machine.

Note:

- You can successfully import contacts only if the Type column is either “User Extension” or “Workgroup”, and the **Ext** and **Address ID** columns are blank.
- You cannot import the contact to a CSV format.

20.6 Deleting a System Directory Contact

1. Launch Connect Director with administrative privileges.
2. In the navigation pane, click **Administration** > **Features** > **System Directory**.

Note:
The **System Directory** page that is displayed is split into the **List** pane (top) and the **Details** pane (bottom). The **List** pane displays all the contacts in the system directory, with parameters as described in System Directory Page Parameter Descriptions. The **Details** pane allows you to view the details for a selected contact.

3. Select the contact that you want to delete, and click **Delete**.
4. You are prompted to confirm the deletion in the **Confirmation** dialog box. Do one of the following:

   - Click **OK** to confirm the deletion.
   - Click **Cancel** to abort the deletion process.

If you chose to delete the contact, the contact is no longer displayed in the **List** pane.

Session Initiation Protocol 21

This chapter contains the following sections:

This chapter describes how to configure Mitel's implementation of Session Initiation Protocol (SIP).

21.1 Overview

Mitel's implementation of SIP can apply to the following:

- SIP trunks
- SIP extensions
- Integration of Mitel with a unified messaging system from a third-party vendor

This chapter also contains technical information to help with planning for SIP on a MiVoice Connect system.

21.2 Introduction to SIP Profiles

A SIP profile is a set of parameters that supports interoperability between a Mitel SIP component and a component from another source or with a different configuration. The components to which SIP profiles apply are SIP trunk groups, SIP extensions, and SIP servers. The sections about these components describe the SIP profiles that apply to these functional areas.

Among SIP trunk profiles, an important distinction between profiles is whether the profile enables hairpinning of media streams through the switch. Without hairpinning, a Mitel SIP trunk supports only the call control tasks and not the media stream. In this scheme, the media stream flows directly between the end-points. (Therefore, switch resources are not needed for controlling media flows.) However, for SIP trunks to support the full set of telephony features in the current release, certain functions are possible only if the media stream flows through a switch. For media streams to flow through a switch, hairpinning must have been applied to the SIP trunk group by a SIP trunk profile that enables it.

Mitel provides some SIP profiles, and customers can create custom profiles by using an existing SIP profile as the basis of a new profile. Custom profiles are an advanced task, as further described in SIP Profiles for Interoperability on page 675.

21.2.1 Current and Legacy Support for SIP Functions

The MiVoice Connect system includes significant SIP trunking features on its half-width voice switches. (Other trunk types already supported these features.) With SIP trunks, most of this SIP functionality depends on one of the current SIP trunk profiles.

The current release includes generic and default, carrier-specific SIP trunk profiles. The introduction to these SIP profiles, including the list of switches that support the full set of SIP trunk functions, is in Configuring SIP Trunk Profiles on page 683, and their effects on individual SIP functions are described in applicable sections throughout this chapter. Customized profiles are also supported. However, customization and the detailed descriptions of SIP trunk profiles exist only in the SIP-related application notes on interoperability from Mitel. Mitel application notes are available for customers in the Mitel Innovation Network Partner Program.

We recommend that existing customers implement the higher trunking functionality on half-width switches by applying SIP trunk profiles, as described in this chapter. However, we also support two legacy SIP profiles for customers that upgrade. Some customers might have no interest in the full feature set after upgrading to Release 13 or later. For example, a customer might have a remote office that uses only the most basic telephony.

When an existing customer upgrades to the current Mitel release while the SystemTrunk or the ATTBVOIP SIP trunk profile is in use, the SIP trunk profile remains in use on the trunk group but with the string “_DEPRECATED” appended to the profile name. Therefore, if profiles SystemTrunk and ATTBVOIP were in use at the time of the upgrade, these profiles remain in use but appear in Connect Director to SystemTrunk_DEPRECATED and ATTBVOIP_DEPRECATED.

Note:

New installations of the current Mitel release do not contain legacy SIP trunk profiles. Only customers who have applied SIP trunk profiles previously and then upgrade to the current Mitel release retain the legacy SIP trunk profiles.

Customers wanting to retain legacy configurations need to be aware that, for a specific trunk group, they cannot mix old functions with the new versions of these functions. (Trunk groups cannot mix old and new SIP trunk profiles.)

In this chapter, wherever a difference exists between the current release and the legacy version, the feature section describes the new capability and the limitation of the legacy

version. Where a new function is independent of the new SIP profiles, the new capability is described without reference to either to legacy or to new status.

21.2.2 SIP Profiles for Interoperability

Although this chapter outlines SIP trunk profiles, SIP extension profiles, and the SIP server profile and how to apply them, SIP profiles are an advanced topic. The chapter provides basic information for most administrators to apply a profile, but in-depth details for every profile parameter are beyond this document's scope. These details exist in the application notes for interoperability. Application notes are available through the Mitel Innovation Network Partner Program. For detailed information on SIP profiles, search the notes available through the Mitel Innovation Network Partner Program at:https://www.mitel.com/developer/mitel-solutions-alliance/tech-connect

For information about the benefits of being a Mitel technology partner or to become a technology partner, go to: https://www.mitel.com/developer/mitel-solutions-alliance/tech-connect

21.3 Operational Behaviors of Mitel SIP Trunks

This section contains details about the behavior of SIP on Mitel trunks. Some subsections point out specific functions and features that are supported in the current release but not in the legacy configurations that some customers might keep. These details can be very relevant to your choices for the configuration of SIP trunk groups. However, if you are already familiar with Mitel's implementation of SIP on trunks in your system and just want the task descriptions for configuring SIP trunks, you can proceed to Configuring SIP Trunks on a Voice Switch on page 679.

21.3.1 Resource Allocation on a Switch

The use of SIP can involve tradeoffs in the allotment of switch resources. Port tradeoff is unavoidable when the switch provides media hairpinning.

For example, one analog switch port supports up to five SIP trunks. Therefore, if one to five SIP trunks is configured on an analog switch port, one less Time Division Multiplexing (TDM) port is available for analog, SGT1, and so on.

For SIP Trunk Media Proxy—the switch-level enable for using hairpinning through a SIP profile in a trunk group—the half-width switches do either of the following:

- Dedicate all their resources to serving as a media proxy.
- Support port-specific configuration for making tradeoffs between SIP trunks, SIP proxy ports, or IP phones that use either SIP or media gateway control protocol (MGCP).

The configuration steps in this chapter illustrate these capabilities.

Note:

Be aware that if a site's headquarters, DVS, or voicemail model switch is using file-based music on hold (MOH) and a G.729 call comes in on a SIP Trunk on a ST-generation switch that has media proxy ports, the file-based MOH will not play to the external party because the call is hairpinned. By default, ST-generation switches that have media proxy ports are hardcoded for always-on hairpinning.

This file-based MOH scenario is similar when a call comes in using G.729 on SG-generation switches that have media proxy ports for which hairpinning is configured to be on. Hairpinning is not always on by default on SG-generation switches.

21.3.2 Conferencing and SIP Trunks

When a SIP trunk participates in a conference call, the following behaviors can apply:

- If hairpinning is enabled on the SIP trunk(s) and no phones on the conference are SIP phones, the SIP Media Proxy Resources provide the ports for the conference so that no Make Me ports are involved. However, the following details apply:
  - A three-party conference can use SIP Media Proxy Resources instead of Make Me ports. However, four-party (up to eight-party) conferences always go to Make Me conference ports.
  - If even one SIP extension participates in the conference, the conference does not use any SIP Media Proxy Resources, so therefore, reserved Make Me ports must be available for the conference.
  - If most SIP Media Proxy Resources are in use at the time a user initiates a conference, such that an insufficient amount of these resources are available, the switch uses Make Me conference resources instead.
  - If the conference call includes at least one SIP extension, Make Me ports for conferences must be available on the initiating side of the conference call. A conference call consists of three to six terminating endpoints.
- Without the use of SIP Media Proxy Resources and the association of a SIP trunk profile to a trunk group, a minimum of four Make Me conference ports must be reserved—even for a three-way conference.

21.3.3 Dual Tone Multi-Frequency Support

In compliance with RFC 2833, switches send and receive DTMF out-of-band. Mitel complies with RFC 2833 for all codecs on SIP trunks. However, for a SIP trunk to support the Additional Phones feature and External Assignment, hairpinning is necessary

because DTMF is a requirement for supporting these functions. (The user enables these features in Connect client.)

21.3.4 Extension Assignment over SIP Trunks

SIP supports Extension Assignment regardless of the configuration of hairpinning although hairpinning does ensure support for DTMF. With hairpinning, the capabilities and configuration procedures for Extension Assignment are identical to Extension Assignment across other trunks. See Configuring Extension Assignment on page 549.

The following points need consideration if media streams are not hairpinned:

- The carrier or service provider must provide DTMF through SIP INFO messages.

Note:

The trunk group must have the SIP INFO Method for transmitting Dual Tone Multi-Frequency (DTMF) enabled. To enable this, select the **SIP info for G.711 DTMF** check box on the General tab of the Trunk Groups page. See Trunk Group Parameters on page 222 for more information.

- If the service provider does not provide DTMF through SIP INFO, Extension Assignment works only if the user's configuration in Connect client enables "Accept call by answering."
- The user cannot use keypad features during the call because they rely on DTMF.

Note:

According to RFC 2976, an INFO message carries application-level information along the SIP signaling path. The INFO method is not used to change the state of SIP calls or the parameters of the session that SIP initiates. The INFO message just carries optional application layer information generally related to the session.

21.3.5 General SIP Feature Considerations

This section describes various features or functions that Mitel SIP supports in the current release as well as functions that Mitel SIP does not support.

- In the current release, the following features are supported by SIP only if the trunk has a SIP trunk profile with hairpinning and the trunk is on a half-width switch or a virtual switch:
  - Silent Coach
  - Silent Monitor
  - Barge-In
  - Call recording
- Fax (and modem) redirection works only if the carrier or ITSP supports T.38. For details about T.38, see T.38 Support on Switches on page 187.
- The maximum number of music on hold (MOH) streams that a SIP-enabled switch can support varies with the switch model and the switch's configuration. Also, the allotment of resources for jack-based MOH includes streams for Backup Auto Attendant and transmission of ringback tones. The range of such streams across all the voice switch models is 14–60.

Note:

For SIP trunks to transport jack-based MOH, the **Jack-based music on hold** check box must be selected to enabled jack-based MOH for the SIP trunk switch. The MOH source is the SIP trunk switch, as follows: An external source for MOH plugs into the SIP trunk switch at the switch's MOH jack, and the switch places the stream on the trunk.

Jack-based MOH is not supported on virtual switches

- A SIP switch attempts to transmit MOH over G.711 U. (Switches supports G.711 A-law and U-law.) If the far end does not support G.711, the switch uses G.729.
- If Make Me conferences are planned, a minimum of four Make Me ports must be reserved. A three-way Make Me conference uses three Make Me ports, a four-way conference uses four ports, and so on up to the maximum of an eight-way conference. For each media stream, up to the maximum of eight-way conferencing, an additional Make Me conference port must be available.
- End-users can set up Make Me conference calls by using their Connect client or IP phone. SIP extensions require permissions and a minimum of four MakeMe ports to set up MakeMe conference call.
- A SIP trunk can be a member of a three-party conference but cannot initiate a three-way conference (unless the SIP device merges the media streams).
- Mitel SIP supports basic transfers (blind transfers) and attended transfers (consultative transfers).

21.3.6 Digit Translation Across SIP Trunks

Digit translation should be used when number plans overlap two systems that are tied by trunks. The translation tables can translate numbers for extensions, voice mail, auto-attendant, and so on. For a description of how to specify a digit translation table, see Creating Digit Translation Tables on page 47.

21.4 Configuring SIP Trunks on a Voice Switch

In general, configuring the SIP trunk and applying a SIP trunk profile involves the following:

Note:

You can perform tasks [1] and [2] in any order.

1. Reserving SIP trunk resources on a switch
2. Configuring SIP trunk profiles (if needed)
3. Creating a SIP trunk group (includes application of a SIP trunk profile)
4. Creating one or more SIP trunks in a trunk group
5. (Optional) Configure users for trunk group access through membership in a user-group

The sections that follow provide the detailed descriptions of these tasks.

21.4.1 Reserving Switch Resources for SIP

This section describes the preliminary task of reserving port resources for SIP trunks.

Voice Switches provide two SIP proxy port sources: Built-in capacity and port assignment. Definitions of these two sources follow.

- **Built-in capacity:** The half-width switches, such as the Voice Switch 50, provide IP phone, SIP trunk, and SIP proxy resources that are independent of port switches. The number of resources varies with each switch model. Each resource unit supports one IP phone, one SIP trunk, or five SIP proxy ports.

Note:

To allocate the Built-in resource for SIP proxy ports, type the number of IP Phone and SIP Trunk resources in their respective data entry fields. The remaining resources are available to serve as SIP proxy ports.

- **Port resources:** A switch port can be configured to support 100 SIP proxy ports.
- **IP Phone ports:** Each SIP extension consumes 1 IP phone port.

Routing the media streams through the switch consumes a large amount of the switch's resources. A large portion of the resources are reserved when *SIP Trunk Media Proxy* is enabled to support hairpinning. SIP Trunk Media Proxy pertains to the ports that the switch can use for hairpinned media streams. Hairpinning and its prerequisite enable described in this section apply only to the half-width switches listed in this section and in Supporting Switches on page 684.

Note:

- If an existing customer is satisfied with the features and performance supported by the SIP configuration before an upgrade to the current Mitel release, enabling SIP Trunk Media Proxy and applying a SIP trunk profile with hairpinning enabled is not necessary. These functions are necessary only if the customer wants the features listed in General SIP Feature Considerations on page 677.
- Enabling hairpinning is applicable only to SG-generation switches. ST-generation switches that have media proxy ports are configured to have always-on hairpinning.

This section illustrates the similarities and the differences between two schemes for reserving SIP Trunk Media Proxy, based on switch model. In these two schemes:

- Regardless of whether SIP Media Proxy resources are reserved for ports, the switch must have at least five SIP trunks reserved.
- On the ST100DA, ST1D, 220T1, 220T1A, 220E1, T1k, and E1k, all of the switch's trunk resources are reserved for SIP Trunk Media Proxy through one check-box enable. When SIP Trunk Media Proxy is enabled, the Built-in capacity fields remain active, but the drop-down lists for physical port configuration are deactivated.

  When SIP Trunk Media Proxy is enabled on the all-or-none users of this resource, the built-in capacity increases from 70 to 100 on the 220T1A and 220E1.

Note:

Once the SIP Trunk Media Proxy check box is selected, no configurable Make-Me conference capability exists on the switch.

- On the ST2D, all of the trunk resources for each span on the switch are reserved for SIP Trunk Media Proxy through one check-box enable for each span. Resources can be reserved for SIP Trunk Media Proxy on one or both spans. When SIP Trunk Media Proxy is enabled for a span, the drop-down lists for physical port configuration are deactivated for that span.

Note:

If one span is dedicated to SIP trunks, the second span can be configured for SGE1/SGT1 ISDN PRI trunks.

- Reserve individual ports for SIP Trunk Media Proxy by way of a drop-down list. Applicable switches are the Voice Switch models ST50A, ST100A, 90, 90V, 90BRI, 90BRIV, 50, 50V, 50BRI, 50BRIV, and 30BRI and 30. The Small Business Edition (SBE) models also have the drop-down list for individual ports.

21.4.1.1 Reserving Resources on the 220T1

Reserving the port resources on a Voice Switch 220T1 if hairpinning is to be used:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the switch to reserve port resources on in the **List** pane.
4. In the **Details** pane, click the **Switch** tab.

   This example uses the 220T1 to illustrate the necessary enable when the use of hairpinning is expected.
5. Select the **Assign digital ports as 20 SIP Trunks with Media Proxies** check box.

Note:
After you enable this parameter, all port-level reservations are disabled. For information about applying a SIP trunk profile, see Configuring SIP Trunk Profiles on page 683.

6. Click **Save**.

21.4.1.2 Reserving Resources on the 50V

Using the Voice Switch 50V as an example, this section describes how to reserve built-in SIP trunk resources and reserve resources at the port-level. You can reserve SIP Media Proxy resources for individual ports on the Voice Switch 50V and other half-width switches.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the name of the switch to reserve port resources on in the **List** pane.
4. In the **Details** pane, click the **Switch** tab.

   This example uses the 50V to illustrate the necessary enable when the use of hairpinning is expected.
5. For each port that you want to reserve for SIP Medial Proxy, do the following:

   a. In the **Port Type** column, select **SIP Trunk with Media Proxy**.
   b. Enter the desired values in the remaining columns.
6. Click **Save**.

After the SIP resources are reserved, you must create SIP trunk group and SIP trunk.

21.4.2 Creating a SIP Trunk Group

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page opens.
3. Click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new trunk group.

4. In the **Trunk type** list, select **SIP**.
5. Review the remaining parameters on all of the tabs in the details pane, and specify values as appropriate.

Note:
For complete information about creating a trunk group, see Adding or Editing a Trunk Group on page 221.

6. Click **Save**.

21.4.3 Creating a SIP Trunk

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunks**. The **Trunks** page opens.
3. Click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new trunk.

4. In the **Trunk group** list, select the SIP trunk group to assign the trunk to.
5. Review the remaining parameters and specify values as appropriate.

Note:
For complete information about creating a trunk, see Adding or Editing an Individual Trunk on page 255.

6. Click **Save**.

21.4.4 Configuring SIP Trunk Profiles

A SIP trunk profile is an advanced facility that provides SIP trunks with the following:

- Support for features that work only if the media stream passes through a switch. This capability becomes possible when hairpinning is enabled in the profile and the profile is applied to the trunk group.

Note:
For ST-generation switches with media proxy, hairpinning is always on. These switches support only a single G.729 stream per physical port. If a SIP trunk call on a ST-generation switch is hairpinned using G.729 codec on the external leg of the call, the other connected endpoint, which is the internal leg of the call, must have additional codecs outside of G.729, such as G711 or other supported codecs.

- The flexibility to interoperate in certain environments or with very specific configurations from third-party services or equipment providers.

Whether provided by Mitel or created by a customer, a SIP trunk profile exists independently of the trunks and the system administrator assigns profiles to a SIP trunk group.

Whether for a new Mitel installation or after an upgrade, customers who want to use all the features that SIP trunks can support must apply a profile with hairpinning enabled. The exceptions are customers who are satisfied with features that do not involve media streams traversing the switch. For a list of features that use hairpinning, see General SIP Feature Considerations on page 677.

21.4.4.1 Supporting Switches

The switches that support hairpinning of media streams are listed in the table below.

Table 162: Models of Voice Switches that Forward Media Streams

ST50A	ST1D
ST100A, ST100DA	ST2D
30, 30BRI	T1k, E1k
50, 50V	220T1
90, 90V, 90BRI, 90BRIV	220T1A, 220E1

Note:

Hairpinning is also supported on Virtual SIP Trunk Switches.

21.4.4.2 Viewing SIP Trunk Profiles

Mitel provides a set of default SIP profiles. For details about the SIP profiles provided by Mitel, see SIP Trunk Profiles Provided by Mitel on page 686. Knowledgeable users can also create custom profiles based on a profile provided by Mitel or any existing SIP trunk profile; however, users must refer to Mitel's application notes on interoperability for guidance.

You can view a list of all SIP profiles on the SIP Trunk Profiles page.

Note:

SIP trunk profiles that are in use at the time of a system upgrade are retained after the upgrade. These profiles are renamed by appending the string "_DEPRECATED" to the name of the profile. Users can disable a deprecated profile that survived the upgrade process and apply a new profile from the current Mitel release.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **SIP Profiles**. The **SIP Profiles** page opens.

Note:
For descriptions of the columns on the SIP Trunk Profiles page, see the following table.

Table 163: SIP Trunk Profiles Page: List Pane

Column Name	Description
Name	Name of the SIP trunk profile.

Column Name	Description
Enabled	Indicates whether or not the SIP profile is enabled. Only enabled profiles can be applied to a trunk group.

21.4.4.2.1 SIP Trunk Profiles Provided by Mitel

The SIP trunk profiles provided by Mitel in the current release are listed in the following table

Table 164: SIP Trunk Profile Provided by Mitel

Profile Name	Parameters	Notes
Default Tie Trunk	OptionsPing=0 OptionsPeriod=60 StripVideoCodec=0 DontFwdRefer=0 SendMacIn911CallSetup=1 HistoryInfo=0 EnableP-AssertedIdentity=0 AddG729AnnexB_NO=0 Hairpin=0 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0 **Note**: For ST-generation switches with media proxy, Hairpin=1.	This is the default profile used for connecting a Mitel PBX to another Mitel PBX or to a PBX system from another manufacturer. • Hairpinning is disabled except as noted. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is disabled; therefore, this profile supports G.729 Annex B.

Profile Name	Parameters	Notes
AT&T	OptionsPing=1 OptionsPeriod=60 StripVideoCode=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=;2H OverwriteFromUser=0	This profile is used for a typical SIP trunk that connects with an AT&T central office. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.

Profile Name	Parameters	Notes
CenturyLink	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0	This profile is used for a typical SIP trunk that connects with a Century Link (formerly Qwest Communications) central office. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.

Profile Name	Parameters	Notes
Verizon	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=0 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0	This profile is used for a typical SIP trunk that connects to a Verizon central office. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.

Profile Name	Parameters	Notes
Default ITSP	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0	This is a generic profile that can be used for a typical SIP trunk that connects with a central office. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.

Profile Name	Parameters	Notes
Century Link (formerly Qwest)	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 1CodecAnswer=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0	This profile is used for a typical SIP trunk that connects with a Century Link (formerly Qwest Communications) central office. • Hairpinning is enabled. • Response with a single preferred codec, rather than a list of codecs, on call establishment is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.

Profile Name	Parameters	Notes
Default Sky ITSP	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0 SRTP=0	This is a generic profile that can be used for a typical Sky SIP trunk that connects with an Internet Telephony Service Provider (ITSP). • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.
Mobility Router	DontFwdREFER=0 SendMacIn911CallSetup=1 IgnoreEarlyMedia=1	This is a generic profile that can be used for a typical mobility SIP trunk that connects with the Mobility Router (SMR). • MAC address transmission by a SIP extension is enabled when emergency number is dialed.

Profile Name	Parameters	Notes
Sky-Connect	Hairpin=1 Register=1 RegisterUser=UserID DontFwdRefer=1 UseSIPS=1 Port=5061 SRTP=1 EnableAlwaysOnHairpin=1 RegisterExpiration=3600 OptionsPing=1 OptionsPeriod=60	This is a generic profile that can be used for a typical Sky Connect SIP trunk that connects with Mitel Sky Connect. • Hairpinning is enabled. • Secure signaling is enabled. • Encoded media is enabled. • Port 5061 is assigned to encrypted SIP (SIP-TLS).

Profile Name	Parameters	Notes
ShoreTel SIP	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion EnableP-AssertedIdentity=1 AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterUser=BTN RegisterExpiration=3600 CustomRules=0 OverwriteFromUser=0	This is a generic profile that can be used for a typical SIP trunk that connects with Mitel SIP Trunking Service. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B.

Profile Name	Parameters	Notes
Default Intrado	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterExpiration=3600 CustomRules=0 RayBaumEnabled=1 RayBaumVendor=INTRADO RayBaumVendorOrgID=None	This profile is used for a typical SIP trunk that connects with Intrado vendor for handling emergency calls for US sites. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when an emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B. **Note**: The following parameters are applicable for US customers as part of RAY BAUM: • The RayBaumEnabled parameter indicates whether RAY BAUM is enabled. The values that you can specify for this parameter are **0** or **1**. • The RayBaumVendor parameter indicates the Ray Baum vendor name. The values you can specify for this parameter are **None**, **REDSKY**, or **INTRADO**. • The RayBaumVendorOrgID parameter indicates the RAY BAUM vendor organization ID.

Profile Name	Parameters	Notes
Default Intrado (Continued)	RBIntradoExtMapSBCPublicAddr = (Public IP address) RayBaumDefaultCallback = (Callback number)	• If the SBCPublicIP parameter is set in the SIP profile, it means that the Extension Bind feature is enabled in MiVoice Connect. The SIP profile name for SBCPublicIP is RBIntradoExtMapSBCPublicAddr. • The DefExt parameter is the default extension, which is the extension number of the receptionist or a common service location through which all users of PBX can be accessed or assisted. The SIP profile name for DefExt is RayBaumDefaultCallback.

Profile Name	Parameters	Notes
Default RedSky	OptionsPing=1 OptionsPeriod=60 StripVideoCodec=1 DontFwdRefer=1 SendMacIn911CallSetup=1 HistoryInfo=diversion AddG729AnnexB_NO=1 Hairpin=1 Register=0 RegisterExpiration=3600 CustomRules=0 RayBaumEnabled=1 RayBaumVendor=REDSKY RayBaumVendorOrgID=None	This profile is used for a typical SIP trunk that connects with RedSky vendor for handling emergency calls for US sites. • Hairpinning is enabled. • MAC address transmission by a SIP extension is enabled when an emergency number is dialed. • Absence of support for G.729 Annex B is enabled; therefore, this profile does not support G.729 Annex B. **Note**: The following parameters are applicable for US customers as part of RAY BAUM: • The RayBaumEnabled parameter indicates whether RAY BAUM is enabled. The values that you can specify for this parameter are **0** or **1**. • The RayBaumVendor parameter indicates the RAY BAUM vendor name. The values you can specify for this parameter are **None**, **REDSKY**, or **INTRADO**. • The RayBaumVendorOrgID parameter indicates the Ray Baum vendor organization ID.

Note:
If US customers want to use RAY BAUM without RedSky or Intrado, then you must add the RayBaumEnabled=1 profile parameter to their SIP trunk profile.

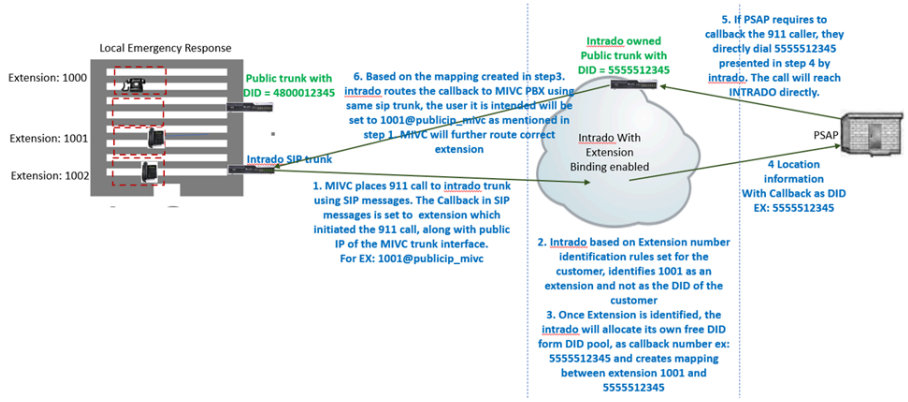
21.4.4.2.2 Extension Binding Feature

The Extension Binding feature is an optional feature for binding an Intrado-owned DID to an emergency caller for use by a PSAP if an emergency call were to be dropped. The PSAP would call the Intrado DID, which Intrado will route back to MiVoice Connect. Due to this, the callback will reach the device that dialed 911 using MiVoice Connect routing.

It is important for the customer to select the extension identification rules to be followed by Intrado that meet the requirements of the customer. This must be communicated to the Intrado team while setting up the account.

With Intrado's Extension Bind feature, MiVoice Connect provides the extension number as the callback number. After identifying this as the MiVoice Connect extension number and not a DID, Intrado provides an Intrado-owned DID to the PSAP. If an emergency callback is required, the PSAP will call Intrado's DID, which they would route back to the subscriber (extension) using the SIP trunk to Ingate. Ingate will forward it to the MiVoice Connect trunks and then on to the actual extension.

Figure 20: Intrado Extension Bind Flow



Note:

- If the SBCPublicIP parameter is set in the SIP profile, it means that the Extension Bind feature is enabled in MiVoice Connect. The SIP profile name for SBCPublicIP is RBIntradoExtMapSBCPublicAddr.
- The DefExt parameter is the default extension which is the extension number of the receptionist or a common service location through which all users of PBX can be accessed or assisted. The SIP profile name for DefExt is RayBaumDefaultCallback.
- Without the Extension Bind feature, Intrado will expect the Contact header (which identifies a user/callback destination) to be a 10-digit DID number (US), and an emergency callback will come back to MiVoice Connect through the public PSTN.
- Without Intrado's Extension Bind feature, MiVoice Connect provides CPN/DID for all users/devices that can make 911 emergency calls and the PSAP will call back MiVoice Connect directly through the public PSTN.

With the Intrado Extension Binding feature, the callback number can be either of the following:

- A MiVoice Connect extension number
- A publicly reachable MiVoice Connect DID number. The DID number in US will be a 10-digit number.

If the Extension Binding feature is enabled and the callback number sent by MiVoice Connect is the extension number, then Intrado will provide its own DID number as the callback number to PSAP. When PSAP uses the callback, it routes the call using Intrado SIP trunk (SIP messaging).

How Intrado identifies the callback for the incoming call is based on the rules that are configured at Intrado for the account. The rules can be one of the following:

- Treat all numbers as the extension number (no chance for publicly reachable MiVoice Connect DID number).
- Treat all numbers other than 10-digit numbers as extension numbers.
- Treat all numbers up to X digits as extension numbers.

Note:

Based on the existing extension number length, the customer can select one of the rules mentioned above.

For US customers, treating all numbers other than 10-digit numbers as extension numbers is more suitable. However, if a PBX has a 10-digit extension number plan, then it causes a conflict and the extension binding will not work. In this situation, the customers can either increase the extension plan in MiVoice Connect or opt to treat all numbers as extension numbers.

Note:
The extension number in MiVoice Connect includes the extension prefix and the extension number.

Based on this rule selection, Intrado decides whether or not to apply extension binding for a call. If the callback number that Intrado derives is not the MiVoice Connect extension, it will not apply the extension bind mechanism to the call, and the number present in the MiVoice Connect header will be transparently sent to PSAP as callback.

For more information about the Intrado Extension Binding feature, see the *Intrado Extension Binding* section in the *MiVoice Connect RAY BAUM'S General Overview and Solution Deployment Guide for Intrado*.

21.4.4.3 Adding or Editing a SIP Trunk Profile

The parameters for the selected SIP profile are configured on the SIP Profiles page. This page is opened from the SIP Trunk Profile List by adding or editing a SIP profile. All parameter fields can be edited for User Defined profiles.

Note:

The predefined profiles provided by Mitel cannot be edited or deleted. However, the profiles can be enabled or disabled.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **SIP Profiles**. The **SIP Trunk Profiles** page opens.
3. Do one of the following:

   - To edit an existing profile, click the name of the trunk group in the **List** pane.
   - To create a copy of an existing profile, click **Copy**.
   - To create a new profile, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing profile.

4. Review the parameters and specify values as appropriate. For descriptions of the profile parameters, see SIP Trunk Profiles Page: General Tab.
5. Click **Save**.

Table 165: SIP Trunk Profiles Page: General Tab

Column Name	Description
Name	Specifies the name of the SIP trunk profile.
Enable	Select this check box to enable the SIP profile. Only enabled profiles can be applied to a trunk group.
System parameters	Specifies the device characteristics and default settings.
Custom parameters	Specifies any additional device settings or overrides of the defaults listed in the System parameters field. **Note**: Documenting all the custom parameters is beyond the scope of this document. To see all the supported custom parameters for SIP profiles, refer to the third-party API documentation for SIP trunks. (Consult the Mitel Technology Partner Program).

21.5 Setting Up 3rd-Party SIP Phones and ATAs

This section begins with introductory information on the resources required to support third-party SIP phones in a Mitel network and then describes the configuration steps for setting up SIP proxy services to support SIP extensions. A SIP device is typically a phone or an analog telephone adapter (ATA) that can serve as a Mitel extension if the device complies with RFC 3261. The *MiVoice Connect Planning and Installation Guide* provides important guidance for selecting a source of third-party SIP phone.

Note:

Because of variations and ongoing development in phones from third-party vendors, customers might have to test phone models under consideration for interoperability with the MiVoice Connect system.

21.5.1 Network Elements

This section describes the system and network components that the administrator specifies to enable SIP endpoints to communicate. In a MiVoice Connect system, SIP endpoints typically are phones. If you are very familiar with these components, you can proceed to the configuration steps for Connect Director in Configuring SIP Extensions on page 711.

In general, the resources that a system uses to support SIP extensions are:

- IP phone resources for SIP extensions: Each SIP extension must point to a SIP proxy server.
- SIP proxy resources: A SIP proxy server is a Voice Switch that you configure to provide the necessary support for SIP extensions. A Mitel network can have one primary SIP proxy server that is operational and a backup server.

Implementing SIP extensions involves the following components:

- In general, resources on a Voice Switch can be allocated to trunks, analog extensions, SIP proxy media, or IP phones (which can be SIP endpoints). Two approaches are available for allocating SIP resources: one approach is a switch-level reservation of built-in resources (in the Built-in part of the switch configuration page), and the other approach is called the trade-off method. The trade-off method reallocates resources at the port-level. Both of these approaches are available on the same switch configuration page.

For reallocating resources on each port, the resource trade-offs are as follows:

- One reallocated trunk resource supports 20 SIP endpoints.
- One reallocated analog extension supports 100 SIP endpoints.
- One reallocated IP phone resource supports 20 SIP endpoints.

- In particular, a SIP proxy server (also called a registrar server) is a Voice Switch switch that facilitates communication between SIP endpoints, as follows:
  - A proxy server forwards requests from a SIP endpoint to another SIP endpoint or another server (when the other server actually processes the request).
  - Within a Mitel network, proxy server functionality is built into half-width and full-width switches. You can designate up to two proxy switches per site: one switch is assigned as the primary proxy server, and the other switch acts as the back-up proxy server in case the primary fails.
  - A Virtual IP Address is an IP address for the voice switch that you configure to be the SIP proxy server for the site. This IP address must be static. It applies to both the primary (operational) and back-up SIP proxy server. (The Virtual IP Address moves to the backup proxy server if the primary proxy server fails).

Note:

If the site does not have a back-up SIP proxy server, you do not need to specify an IP address for the Virtual IP Address. In this case, only the name of the one proxy server is needed.

The page for specifying the Virtual IP Address is **Administration** > **System** > **Sites**.

21.5.2 Supporting SIP Devices

In the current release, the IP8000 is the only SIP phone that Mitel provides. All other SIP phones that can operate in a Mitel network would come from other manufacturers. The *MiVoice Connect Planning and Installation Guide* provides important guidance for selecting a third-party SIP phone.

21.5.2.1 User Configuration of SIP Phones

A substantial variety exists among the third-party vendors' approach to phone registration. Some phones have an on-phone set-up dialog, others require a web-browser, and at least one vendor's ATA is known to require SNMP. The approach can vary from phone to phone, and many manufacturers support configuration by way of a centralized server.

When registration is available through the phone's interface, the end-user configures the SIP extension in response to prompts that appear on the phone. The user presses phone buttons to enter the requested data at each prompt.

Users must have received a SIP password from the system administrator before starting the configuration tasks. To configure SIP, the user enters the following:

- The Mitel username
- SIP password
- SIP proxy address (the Virtual IP Address, configured in Connect Director on the Sites page; **Administration** > **System** > **Sites**)

The MiVoice Connect system recognizes the extension, the DID number, or the Client Username. Client Username is the best choice. For information on Client Username (or simply User ID), see Configuring a User Account on page 488.

The phone sends a SIP REGISTER request to the SIP proxy server. For a new registration, the server's response can take a few seconds.

Note:

Changing the IP address of a SIP device can result in that device being listed twice on the Telephones page in Connect Director. In this case, the most recent registration takes precedence.

If many SIP phones register simultaneously, a significant delay might result while completing SIP phone registration. Distributing SIP phones to multiple switches and multiple sites could help overall with SIP registration.

21.5.2.2 SIP Profile Support for SIP Extensions

SIP device models can support different feature sets on third-party phones. These feature sets can relate to, for example, call control capabilities, codec compatibility, and provisioning procedures. SIP extension profiles are specific for particular SIP device models, as described in Creating a SIP Extension Profile on page 714.

21.5.2.3 Extension Assignment

The Extension Assignment feature lets a user temporarily assign his or her primary phone to another device. Consequently, the other device temporarily functions as an assigned phone.

The user can assign the primary extension to a Mitel phone or the user's personal phone. For example, if a user wants to use a personal cellphone for the Mitel extension while moving around a Mitel site or off-site, that user activates Extension Assignment from the cellphone.

The user configures one or two phone numbers for Extension Assignment in the Connect client Options window to point to the primary phone. Thereafter, whenever the user

enables Extension Assignment capability in the Options window, he or she can place or receive calls on the assigned phone.

During an Extension Assignment session, if the user's primary phone is an IP phone, it goes into anonymous mode during the session. Although Extension Assignment is available for SIP phones and regular IP phones, the display on these two phone types behaves differently during an Extension Assignment session. On a regular IP phone, the phone's display shows the word "Anonymous" during the session. However, because SIP supports only the regular phone display, a SIP phone in the anonymous state still displays the standard information and gives no indication of being anonymous.

When ready to end the Extension Assignment session, the user can disable Extension Assignment from Connect client or the assigned phone.

Note:

The user must complete the REGISTER process for the primary SIP phone before activating Extension Assignment. (In contrast, for a regular phone, an end-user must use voicemail to manage Extension Assignment).

A user has a phone on his or her desk: The user registers a SIP Softphone or Wi-Fi phone that temporarily becomes the assigned extension.

21.5.3 User Features

This section describes the user features supported by SIP extensions.

21.5.3.1 Call Dialing and Initiation

SIP extensions support the following call initiation features:

1. **Make Call:** Calls can be made from a SIP phone or from Connect client.
2. **On-hook dialing:** On-hook dialing is supported from Connect client.
3. **Intercom:** SIP extension users initiate Intercom calls to an extension by pressing:

   - *** 1 5 extension number**

Note:

On an SIP extension, an Intercom call arrives like a regular call.

4. **Redial and Speed dial:** Redial and Speed dial initiated from SIP extensions through Connect client operate similar to on-hook dialing.

Note:

Redial and Speed dial methods differ for each SIP device model. Feature keys on a specific model of a SIP device can be programmed to support speed dial.

5. **E911:** Calls to emergency numbers from a SIP extension (or regular phone) send an emergency identification number or CESID number with the call. For a description of the extent of Mitel's support for emergency calls, see Configuring a System for Emergency Calls on page 983.

   Unregistered SIP phones cannot place 911 calls.
6. **Dial plans and extension lengths:** When the SIP call manager receives an incomplete number or an illegally formed number from a SIP device, the system terminates the call after it transmits a "That extension is not valid" message to the caller.
7. **Night bell:** SIP extensions can pick up the night bell by pressing star code ***14**.

21.5.3.2 Call Routing

Call routing operations provide options for answering or routing incoming calls. SIP extensions support the following call routing options:

- **Answer call:** SIP extensions can answer calls only from the phone.

  Offering calls can be redirected to Voice Mail, an Auto-Attendant, or another extension through Connect client.
- **Hang-up:** SIP extensions can hang up calls from the phone or from Connect client.
- **Ring No Answer (RNA):** The number of rings that trigger a No Answer response is specified in the Availability States parameters for each user. When the No Answer condition is triggered, the SIP call manager redirects the call to the RNA destination as specified by Connect Director.

- **Busy:** When the user call stack is larger than the phone call stack, and the SIP phone rejects overflow calls with SIP response 486 Busy, the switch can redirect the call to the busy destination as specified in Connect Director.
- **Forward Always:** SIP extensions support Forward Always. When this parameter is set, all calls will be forwarded to the destination specified in Connect Director.
- **Call waiting:** The specific call waiting implementation differs for each SIP phone model. SIP extensions support call waiting to one or multiple simultaneously-offered calls for the SIP devices that support this feature.
- **Call rejection:** If the SIP phone rejects the call with ***603 Decline*** response code, the switch fails the call and plays the reorder tone to the caller.
- **Call redirect:** If the SIP phone returns a ***3xx*** response code, the switch redirects the call to the user's RNA destination. If the RNA destination is not configured, the reorder tone is played.
- **Find Me:** SIP extensions support FindMe and Voice Mail Notification.

21.5.3.3 Caller ID

Caller ID is the caller information transmitted to the other party during a voice call.

- **Caller ID presentation:** SIP extensions can display caller name and number.
- **Caller ID blocking:** SIP extensions support caller ID blocking and private extensions.
- **Caller ID for Workgroup and Hunt Group agents:** The system sends the original caller information while the phone rings. After the recipient answers the call, the system continues to display the original caller name and number.

21.5.3.4 Call Control

Users manage active voice calls through call control operations. Mitel SIP extensions support the following call controls:

- **Hold:** Call hold and unhold are performed on the phone. Implementation of the reminder ring for held calls differs among SIP phone models.
- **Basic transfer:** SIP extensions support blind transfers that use REFER messages. Transfers that use re-INVITE are not supported.
- **Consultative transfer:** SIP extensions support consultative transfers that use REFER. Transfers that use re-INVITE are not supported.
- **Park from SIP phone:** Calls from SIP extensions are parked when the user selects a different line and then presses the following sequence of keys: ***11 number**.
- **Unpark on SIP phone:** SIP phone users pick up a parked call by pressing *12 and then the extension number, for example: ***** **1 2 2508**. (On a SIP phone, taking the handset off-hook is not sufficient to resume a parked call.)
- **Pickup:** SIP phone users pick up a call by pressing ***13**, followed by the number.
- **Unpark:** SIP phone users unpark a parked call by pressing ***12** and then the number.

- **Conference Calls:** Three-party conference calls initiated from the phone use the phone's resident multipoint control unit (MCU).

  - A three-party conference call initiated from Connect client uses Make Me conferencing.
  - Make Me conferencing is used when a SIP phone joins a conference call.
  - Four to eight-party conference calls are supported using Make Me conferencing. Conferences must be initiated through Connect client.
- **Simultaneous ringing:** Multiple SIP extensions can be configured to ring simultaneously in response to a call. A user enables the Additional Phones feature and External Assignment in the Connect client Tools > Options window.
- **Call recording:** A SIP extension user can record calls that traverse a SIP trunk if the user has permission. Call recording is enabled through the user's Class of Service. The user initiates call recording in Connect client.
- **Voicemail:** SIP extensions reach voice mail by pressing **#** on the phone or by pressing the Connect client VM button.
- **MWI:** SIP extensions support Message Warning Indicator by using NOTIFY or SUBSCRIBE/NOTIFY on phone models that support MWI. MWI is configurable through SIP phone profiles.
- **Agents:** SIP extensions are available for Workgroup and Hunt Group agents.
- **Bridged call appearance:** SIP extensions do not support Bridged Call Appearances.
- **DTMF:** SIP Extensions support DTMF tones as specified by RFC 2833.
- **Huntgroup busy out:** SIP extensions can busy out huntgroups by pressing ***18**, followed by the hunt group number.

21.5.3.5 General Feature Limitations

Mitel does not support the following special call features on SIP extensions:

- **Silent Monitor:** SIP extensions cannot initiate or be the recipient of this operation.
- **Silent Coach:** SIP extensions cannot initiate or be the recipient of this operation.

  Barge In: SIP extensions cannot initiate or be the recipient of this operation.
- **Whisper Page:** SIP extensions cannot initiate or be the recipient of this operation.

21.5.4 System Features

SIP extensions support the following system features:

- **Account codes:** Users on SIP extension can be forced to use account codes for external calls.
- **Bandwidth allocation:** Mitel allocates bandwidth for SIP voice calls.

- **Backup Auto Attendant (BAA):** The SIP call manager switch provides BAA to the SIP extension.
- **Supported Codecs:** Mitel default settings support the negotiation of supported codecs. For information about codecs, see Codec Negotiation and Bandwidth Management on page 438.
- **Fax redirection:** Fax calls to SIP extensions are redirected to the site's fax redirect number.
- **Music on Hold (MoH):** Mitel does not support jack-based MOH for SIP extensions; file-based MOH is supported for SIP extensions.
- **Extension Assignment – external devices:** A SIP extension user can be configured so that the Extension Assignment feature can be initiated from devices that are external to the MiVoice Connect system.
- **On-Net dialing:** SIP extensions can use on-net dialing.
- **PSTN failover:** If PSTN Failover is enabled at the time of a WAN disconnection, a user can still reach someone at another site by using the PSTN. For example, if the WAN connection between two Mitel sites is down and a user calls the other office and PSTN failover is enabled, the call traverses the PSTN (instead of failing).
- **Packetization period:** The default packetization period for all calls involving SIP extensions is 20 ms.
- **Video call:** The "Allow intersite video calls" setting in the Telephony Features Permissions allows or prevents video calls between Mitel sites for users with that Class of Service. For a video call to exist, all participating members must be members of a user group with a COS that enables intersite video. Each user must also have a supported camera model and have currents drivers for the camera and the video graphics card.

Note:

The MiVoice Connect system does not allocate bandwidth for video calls. Consequently, heavy traffic on the network can have an impact on video calls and even audio communication.

- **Country Call Progress Tones and Ring Tones:** SIP extensions provide call progress and ring tones for countries supported by Mitel.
- **Language support:** SIP extensions provide support for languages as required by the countries supported by Mitel.

21.5.5 User Assignment

This section briefly mentions the type of information that Mitel customers need for configuring third-party SIP phones. The operational variations and regular updates in the phones from individual manufacturers mean that Mitel cannot give specific directions for

phone models from third parties. However, several items are very commonly configured on a SIP phone to identify it, as follows:

- User ID - According to individual deployments, can be extension number, DID, or Client User ID.
- SIP password - Configured in Connect Director and can consist of the following characters: **!#$%&'()* +,-.0123456789:;=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_/ `abcdefghijklmnopqrstuvwxyz{|}~**

  The characters ? “ <> are not allowed by the system.
- IP address of the SIP proxy at the site.

21.5.6 Configuring SIP Extensions

This section describes the procedures for setting up SIP extensions.

21.5.6.1 Specifying the SIP Network Elements

The Sites page supplies the following SIP configuration tasks for a site:

- Defining the IP address for the SIP proxy server
- Designating the switches that serve as the site’s SIP proxy servers; the site can have a primary server and a secondary server

To configure the SIP network elements for a site:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page opens.
3. Click the name of the site to edit in the **List** pane.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the selected site.

4. Review the parameters at the bottom of the General tab and specify values as appropriate. For descriptions of the SIP Proxy parameters, see the following table.

Table 166: Sites Page: General Tab, SIP Proxy Parameters

Parameter	Description
Virtual IP address	Specifies the virtual IP address of the site's operational SIP proxy server (registrar server). This parameter is required when both Proxy switch 1 and Proxy switch 2 are configured. **Note**: The Virtual IP Address is independent of the switch that performs the server functions. It must be either outside the address range that a DHCP server manages or marked as reserved, and it must be on the same subnet as the regular IP address of the switch.
Proxy switch 1	Specifies the switch that performs the site's SIP server functions. The drop-down list displays all the switches at the site that are configured to support proxy functions. This parameter is required for SIP extensions.
Proxy switch 2	Specifies the switch that functions as the SIP proxy server when Proxy Switch 1 is not available. This parameter is optional but recommended.

21.5.6.1.1 Redundant Setups

In a redundant setup, the Virtual IP Address is used for configuring SIP extensions.

The system instantiates the Virtual IP Address on the switch specified as "Proxy Switch 1." If "Proxy Switch 1" fails, "Proxy Switch 2" activates the Virtual IP Address on its network interface. When the first proxy returns to service, it again uses the Virtual IP Address, and the back-up proxy releases the address.

21.5.6.1.2 Non-Redundant Setups

If no redundant SIP proxy server is implemented:

- The name of the voice switch is required.

- The Virtual IP Address box can be empty, but we recommend that a Virtual IP Address be assigned to ensure a smooth transition to redundancy in the future.
- The proxy switch IP address must be used when SIP extensions are configured.

21.5.6.2 Setting the SIP Call Controls

You can configure the SIP Call Control Options for the MiVoice Connect system on the Call Control Options page.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Features** > **Call Control** > **Options**. The **Call Control Options** page opens.
3. Review the parameters in the SIP area of the page, and specify values as appropriate.

Note:
For descriptions of the SIP call control options parameters, see Call Control Options Page: SIP Area.

4. Click **Save**.

Table 167: Call Control Options Page: SIP Area

Column Name	Description
Realm	Specifies the name of the protected area (realm) to which the SIP authentication parameters are applied. For digest authentication, each domain of this type defines a set of user names and passwords that the system uses for granting access.
Enable session timer	Select this check box to enable the session timer. The session timer controls the interval at which SIP devices transmit or receive a RE-INVITE or UPDATE method to refresh the current session.

Column Name	Description
Session interval	Specifies the interval, in seconds, at which keepalive heartbeats are broadcast. The heartbeat is sent out at the specified period and if no response is received, the session is dropped. See RFC 4028 for more information about this parameter. **Note**: The default of 1800 seconds usually is best for most Mitel installations.
Refresher	Specifies whether the session timer is applied to the caller or called party. Select one of the following options: • **None** - to specify no preference • **Caller (UAC)** - to specify the caller • **Caller (UAS)**- to specify the called party See *RFC 4028* for more information about this parameter. **Note**: The method is either RE-INVITE or UPDATE. The method is dynamically selected, based on the methods advertised by the supported header.

21.5.6.3 Creating a SIP Extension Profile

A SIP Phone Profile is a Mitel record that lists characteristics, properties, features, and settings for a specific SIP device. A Voice Switch uses SIP Phone Profiles to monitor and service the SIP devices connected to the system. Mitel provides predefined profiles and supports user-defined profiles.

- Predefined profiles support generic devices or devices for which a specific profile is not defined. Although predefined profiles cannot be deleted or modified, they can be deactivated or superseded by user defined profiles.
- User-defined profiles are created through Connect Director and specify settings for certain SIP device models.

21.5.6.3.1 Viewing SIP Phone Profiles

You can view a list of all pre-defined and user-created SIP Phone Profiles on the SIP Phone Profiles page in Connect Director.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **SIP Profiles**. The **SIP Phone Profiles** page opens.

Note:
For descriptions of the columns on the SIP Phone Profiles page, see the following table.

Table 168: SIP Phone Profiles Page: List Pane

Column Name	Description
Name	Name of the SIP phone profile.
User Agent	The expression Mitel uses to identify devices covered by the profile. Mitel compares this expression to the **User Agent** field in the header of SIP packets handled by the system.
Enabled	Indicates whether or not the SIP phone profile is enabled. Only enabled profiles are used when evaluating the characteristics of a device.
Priority	The priority of the SIP phone profile. This number indicates the order by which the profile is evaluated against the SIP packet header. The sequence of profile evaluation is from high to low.

Note:
The **User-Agent** field of successive profiles are compared to the **User-Agent** field of the SIP packet header until a match is found. The profile containing the matching **User-Agent** field is then used to specify device configuration settings.

21.5.6.3.2 Adding or Editing a SIP Phone Profile

Note:

The predefined profiles provided by Mitel cannot be edited or deleted. However, the profiles can be enabled or disabled.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **SIP Profiles**. The **SIP Phone Profiles** page opens.
3. Do one of the following:

   - To edit an existing profile, click the name of the profile in the **List** pane.
   - To create a copy of an existing profile, click **Copy**.
   - To create a profile group, click **New**.

   Note:
   The **General** tab in the **Details** pane displays parameters for the new or existing profile.

4. Review the parameters and specify values as appropriate.

   Note:
   For descriptions of the profile parameters, see the following table.

5. Click **Save**.

Table 169: SIP Phone Profiles Page: General Tab

Column Name	Description
Name	Specifies the name of the SIP phone profile.
User Agent	Specifies the expression Mitel uses to identify devices covered by the profile. Mitel compares this expression to the User Agent field in the header of SIP packets handled by the system.
Priority	Specifies the priority of the SIP phone profile. This number indicates the order by which the profile is evaluated against the SIP packet header. The sequence of profile evaluation is from high to low.
Enable	Select this check box to enable the SIP phone profile. Only enabled profiles are used when evaluating the characteristics of a device.
System parameters	Specifies the device characteristics and default settings.
Custom parameters	Specifies any additional device settings or overrides of the defaults listed in the System parameters field.

21.5.6.3.3 Custom Parameters

The custom parameters are additional device settings or overrides of the default settings listed in the **System Parameters** field. For a description of each available custom parameter, see the following table.

Table 170: SIP Phone Profiles: Custom Parameters

Custom Parameter	Description
OptionsPing	Set this parameter to **1** to enable the SIP device to process `SIP OPTIONS` commands. An `OPTION` command is sent to the SIP device as a keepalive message.

Custom Parameter	Description
SendEarlyMedia	Set this parameter to **1** if the SIP device is capable of receiving “early media.” Some BAA prompts are streamed as early media.
MWI	Set this parameter as follows: • Set to **none** if the SIP device does not support MWI. • Set to **subscribe** when the SIP device subscribes for message waiting service. • Set to **notify** when the SIP device can receive MWI notification without subscribing to the service.
1CodecAnswer	Set this parameter to 1 to set only one codec in Answer mode for Session Description Protocol (SDP).
StripVideoCodec	Set this parameter to 1 to have the Mitel user agent strip video codecs from SIP SDP.
AddGracePeriod	Set this parameter to add extra time to the expire time for SIP registrations.
Accept302=ext	Set this parameter to forward calls.
FakeDeclineAsRedirect	Set this parameter to 1 to treat the response code “603 decline from SIP endpoint” as a redirect to the call routing destination.

21.5.6.3.4 Setting an Extension Password

A user extension is enabled for SIP only when a value is assigned to the user’s SIP Password parameter. If no SIP password is assigned, the extension will not support SIP.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.

3. Do one of the following:

   - To edit an existing user, click the name of the user in the **List** pane.
   - To create a copy of an existing user, click **Copy**.
   - To create a new user, click **New**.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the new or existing user.

4. In the **SIP phone password** field, type a password for the SIP extension.
5. Enter the password again in the second field.
6. Click **Save**.

21.5.6.3.5 Viewing SIP Devices

All SIP devices on the Mitel network are listed on the Telephones page in Connect Director. SIP devices are deleted from this page when they are physically removed from the network.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Telephones**. The **Telephones** page is displayed.
3. Click the name of the SIP device you want to view details for in the **List** pane.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the SIP device.

21.6 Integrating Mitel SIP with Unified Messaging from Third-Party Vendors

Mitel software allows an organization to integrate an external, third-party unified messaging (UM) system with the MiVoice Connect system. Mitel also supports customer plans for deploying a separate voicemail or fax server within the Mitel environment. After setting up the Mitel solution, a customer can deploy a third-party solution (such as Microsoft Exchange) to play voicemail or send faxes (through a Mitel-supported UM fax server).

For more information on configuring Mitel-supported, third-party UM solutions, contact the Mitel Innovation Network Partner Program.

For general information, go to the following location: https://www.mitel.com/developer/mitel-solutions-alliance/tech-connect

Note:

A Unified Messaging SIP Link license is required for every Unified Messaging (SIP) server added in Connect Director. To add a server, the check box Allow External Voice Mail for Extension-Only User must be selected.

21.6.1 Considerations for Integrating with Third-party UM

Plans for integrating a Mitel network with a third-party UM system should include consideration of the following behaviors:

- After Mitel user accounts move to a third-party UM server, those users' existing voicemails are deleted from the MiVoice Connect system. Therefore, we recommend that you save existing voicemails before integrating with Mitel.
- Mitel does not actually integrate voicemail with Outlook even though you can enable Outlook integration in Connect client. This option enables Mitel partners or outside vendors to set up integration of voicemail with Outlook.
- The message waiting indicator (MWI) that signals a waiting voicemail message is not available for Connect client.
- The following voicemail features are not available to a user when Mitel is integrated with third-party UM systems:
  - Any Phone
  - Find-Me
  - Escalation Profiles
- Switching between Mitel and External SIP Unified Messaging voicemail results in the following conditions.
  - Loss of all existing Mitel messages (initial backup is recommended)
  - Users might need to re-create the Connect client rules to reflect the new voicemail number

Note:

An important behavior that relates to Connect client's Power Routing should be understood. The action is Forward Call to Voice Mail, and the circumstance when this behavior is relevant is when a Mitel customer changes the voicemail server to a SIP Unified Messaging (SIPUM) server. Before the migration to SIPUM, any rule that forwards calls to voice mail (or all rules if that is more convenient) should be disabled. If a rule whose action forwards calls to voice mail remains enabled during migration, the rule fails to migrate.

21.6.2 Configuring a Mitel SIP Unified Messaging Server

This section describes the steps for configuring a Mitel SIP UM server.

To integrate Mitel with a third-party UM system, the system administrator must do the following:

1. Configure a Mitel SIP server through Connect Director.
2. Set up and configure one of the supported third-party UM solutions.

Note:

Enable a Voice Switch to act as the SIP proxy for the site where you add the SIP UM Server.

21.6.2.1 Adding or Configuring a SIP Server

1. Launch Connect Director and log in as the administrator.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Integrated Servers** > **SIP Servers**. The **SIP Servers** page opens.
3. Do one of the following:

   - To edit an existing server, click the name of the server in the **List** pane.
   - To create a copy of an existing server, click **Copy**.
   - To create a new server, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing server.

4. Review the parameters at the bottom of the General tab and specify values as appropriate.

Note:
For descriptions of the SIP Proxy parameters, see SIP Servers Page: General Tab.

5. Click **Save**.

Table 171: SIP Servers Page: General Tab

Parameter	Description
Name	Specifies the SIP server name (usually that of a Microsoft Exchange).
Site	In the drop-down list, select the name of the site where the UM Server resides. Note that a pop-up message appears if the UM Server site changes.
Protocol	In the drop-down list, select the SIP transport protocol for the SIP UM server. For Microsoft TCP Microsoft Exchange server, select TCP.
Host (name/address/domain)	Specifies the IP address or fully qualified domain name of the server. **Note**: This must be an IP address or fully qualified domain name.
Override default port	The default port is 5060, but you can use this field to specify another port number.

Parameter	Description
Allow external voice mail for Extension-Only user	Select this check box to allow external voice mail for an extension only user. **Note**: The Mitel customer must have a license for Mitel External Unified Messaging SIP Link.
Allow fax redirect to this server	Select this check box to use the server as a Site Fax Server.
Extension	Specifies a unique extension for the SIP UM Server. This should be identical to the pilot number assigned on the SIP UM Server.
Assigned user group	In the drop-down list, select the user group to associate with the server. This user group is used to provide outbound trunk calling capability from the server. Assign a user group with outbound trunk access. On an Exchange server, this user group is used to make external calls for the following features: • MS Outlook play on phone feature for playing voice mail on an external number. • Call sender feature to call to an external user who left a voice mail.
SIP profile	In the drop-down list, select a SIP profile for the server. For an Exchange server, select Microsoft Exchange.

Parameter	Description
Digest authentication	In the drop-down list, select the type of calls for which to perform authentication.: • **None** - to disable authentication for inbound and outbound calls • **Inbound-Only** - to perform authentication of credentials for inbound calls only • **Outbound-Only** - to provide credentials for outbound calls when authentication is required by the call recipient • **All** - to perform authentication for inbound calls and provide credentials for outbound calls **Note**: The options available depend on what the SIP UM server supports. For MSE, select **None**.
Username	Specifies the user name for digest authentication. A Username is valid only with a customized SIP trunk profile that allows a user ID instead of the default billing telephone number (BTN) in the default profiles. **Note**: This information may be obtained from the SIP ITSP service provider.
Password	Specifies the password for digest authentication. **Note**: This information may be obtained from the SIP ITSP service provider.

21.6.2.2 Configuring a User Group with Access to SIP Servers

After you have created a SIP server, you must add or configure a user group with access to the server.

For complete information about configuring user groups, see Configuring User Groups on page 481.

1. Launch Connect Director and log in as the administrator.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page opens.
3. Do one of the following:

   - To edit an existing user group, click the name of the user group in the **List** pane.
   - To create a copy of an existing user group, click **Copy**.
   - To create a new user group, click **New**.

Note:
The **General** tab in the **Details** pane displays parameters for the new or existing user group.

4. In the **Voice mail interface mode** drop-down list, select **External Voice Mail, SIP**.
5. Click **Save**.

Note:
The Availability States destinations for this user group are set to the selected SIP server extension.

21.6.2.3 Configuring User Access to a SIP Server

Users have access to the facilities supported on a SIP server when they are members of a user group that has access to a SIP server. The key point for giving SIP server access to the user's voicemail and other messages is to add the user as a member of a user group that has that access. For information about configuring a user group with access to a SIP server, see Configuring a User Group with Access to SIP Servers on page 725.

For complete information about configuring users, see Configuring a User Account on page 488.

1. Launch Connect Director and log in as an administrator.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. Do one of the following:

   - To edit an existing user group, click the name of the user in the **List** pane.
   - To create a copy of an existing user, click **Copy**.
   - To create a new user, click **New**.

   Note:
   The **General** tab in the **Details** pane displays parameters for the new or existing user.

4. In the **License type** list, select **Extension-Only**.
5. In the **User group** list, select the user group to associate with the user.

   Note:
   You must select a user group with the voice mail interface mode set to External Voicemail, SIP. See Configuring a User Group with Access to SIP Servers on page 725 for information about setting the voice mail interface mode for a user group.

6. In the **Mailbox server** list, select a UM server.
7. Click **Save**.

Monitoring and Diagnosing 22

This chapter contains the following sections:

This chapter provides details about using the Diagnostics and Monitoring system available through Connect Director.

22.1 Overview

The Diagnostics and Monitoring system is a comprehensive set of tools that enables:

- Status, fault, and performance monitoring
- System capacity planning
- Voice quality monitoring
- Root cause analysis
- Troubleshooting

22.1.1 Architecture

The Diagnostics & Monitoring system is accessible through the Maintenance and Diagnostics menus in Connect Director and consists of the following components:

- Monitoring Service

- Monitoring Agents
- Monitoring Database
- Status Database

22.1.1.1 Monitoring Service

The Monitoring Service receives and processes data from the following sources:

- call quality reports from the Monitoring Agents
- status database (shoreware status)
- the CDR database (shorewaecdr)

To collect statistics, the Monitoring Service requires that switches, service appliances, and softswitches have an active network connection to the Headquarters server. If the network connection is not functioning, statistics are not reported. In addition, because metrics are not collected if the Monitoring Service is not running, any average calculations for a particular time period that includes time when the Monitoring Service was down will not be accurate.

22.1.1.2 Monitoring Agents

The Monitoring Agents are integrated services residing on switches, servers, and phones in the MiVoice Connect system. They collect call quality metrics and path trace information, summarize the data in one or more reports, and send the reports to the Monitoring Service at the end of each call. Any media streams without IP media do not send reports.

22.1.1.3 Monitoring Database

The Monitoring Database (shorewaremonitoring) is installed on the Headquarters server. It stores the raw data collected by the Monitoring Service.

For information about configuring the Monitoring Database, see Changing Settings for the Monitoring Database on page 730.

22.1.2 Requirements

The Diagnostics and Monitoring system has the following requirements:

- To collect call quality data, switches need active connections to phones and a call's duration needs to be at least 30 seconds.
- The Monitoring Service requires that the local time zone of the computer on which the Headquarters server is running be the same as the local time zone specified for the Headquarters server in Connect Director.

22.2 Managing the Monitoring Service and Database

To manage the Monitoring Service and the Monitoring Database, you can do the following tasks:

- Change the leadership of the Monitoring Service from Headquarters to a remote server
- Change the settings for the Monitoring Database

22.2.1 Changing the Leadership of the Monitoring Service

By default, the Monitoring Service is installed only on the Headquarters server, and this configuration should be adequate for most installations. However, if your system has more than 10,000 busy-hour call attempts (BHCA), then you should install an instance of the Monitoring Service on a remote server to reduce the processing load on the Headquarters server. Details are provided in the *MiVoice Connect Planning and Installation Guide*.

If you have installed a remote instance of the Monitoring Service, you would assign the Main Service role to the remote instance and the Event Collector role to the instance on the Headquarters server. (The remote server is never in the Event Collector role.) For details about the information displayed on the Monitoring Service list pane, refer the below table.

To change the leadership of the Monitoring Service instance from the Headquarters server to the remote server:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Configuration** > **Monitoring Service**. The **Monitoring Service** page is displayed.
3. In the **Monitoring Service** pane at the top of the page, select the row for the Headquarters server.
4. In the **Monitoring Service Instance** pane at the bottom of the page, in the **Role** drop-down list, select **Event Collector**.

Note:

- The ✎ indicates that the role has changed.
- To revert to the default settings, click **Reset**.

5. Click **Save**.

Table 172: Monitoring Service Page: List Pane

Column Name	Description
status indicator	The status of the Monitoring Service.
IP Address	The IP address of the server where the Monitoring Service is running.
Port	The port number that the Monitoring Service uses.
Role	Whether the Monitoring Service is in the Main Service role or the Event Collector role.
Build Number	The build number of the Monitoring Service.

Table 173: Monitoring Service Instance Details

Parameter	Description
IP Address	The IP address of the selected Monitoring Service.
Port	The port number the selected Monitoring Service instance uses.
Role	If you want to change the role of the Monitoring Service instance, select a new role from the drop-down list. A single instance of the Monitoring Service should have the Main Service role. If you have a Monitoring Service instance running on a remote server, it should have the Main Service role, and the Headquarters instance of the Monitoring Service should have the Event Collector role.

22.2.2 Changing Settings for the Monitoring Database

Though Mitel recommends that you use the default values for the settings related to purging and reclaiming space in the Monitoring Database, you can change the settings. These settings are described in the following table.

Table 174: Configuration Settings for the Monitoring Database

Name	Description
Call Quality data	The number of days to retain data related to call quality. The default is 31 days.
Alert data	The number of days to retain data related to alerts. The default is 3 days.
Event data	The number of days to retain data related to events. The default is 3 days.
5 Minute Aggregation data (# days)	The number of days to retain 5-minute aggregation data. The default is 2 days.
1 Hour Aggregation data (# days)	The number of days to retain 1-hour aggregation data. The default is 10 days.
Daily Aggregation data (# days)	The number of days to retain daily aggregation data. The default is 31 days.
Time of Day to Purge/ Reclaim	The time on a 24-hour clock to run the database purge audit process. This process deletes the expired data from the Monitoring Database according to the settings specified in the configuration settings and reclaims the space in the database. Specify a time during non-peak hours for your system. The default is 1 a.m.

To change settings for the Monitoring Database:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Configuration** > **Monitoring Database**. The **Monitoring Database Settings** page is displayed.
3. If you want to change the default values, use each drop-down list box to select a value for a particular field.

Note:

- The icon indicates values that you have changed.
- To revert to the default settings, click **Reset**.

4. To save the settings you selected, click **Save**.

22.3 Navigating the Pages in the Maintenance Menu

This section describes the key components and capabilities of the pages available through the Maintenance menu.

22.3.1 Refreshing the View

The **Dashboard**, **Topology**, and **Status** pages in the Maintenance menu automatically refresh every 30 seconds. To stop automatically refreshing a page, click the **Stop Refreshing** button at the top right corner of the page. If you want to resume refreshing a page, click the **Resume Refreshing** button.

The **Alerts and Call Quality** pages do not automatically refresh. To get real-time status, you can refresh those pages by clicking the **Refresh** button at the top right corner of the page.

22.3.2 Zooming In and Out

In charts such as those on the Dashboard or on the detail panes of the Status pages, you can zoom in or out using either of the following methods:

- Click the and buttons at the top right of each chart.
- Click on the area in a chart where you want to zoom, and use the scroll wheel on your mouse to zoom in or out.

To scroll up or down within a chart, click and drag anywhere on the chart.

22.4 Viewing System Status with the Dashboard

The Dashboard displays real-time performance data up to the current minute, based on data collected by the Monitoring Service. By changing the time period, you can view current or historical performance information.

22.4.1 Selecting the Time Period

You can display monitoring metrics for the following pre-defined time periods:

- Last 1 Hour
- Last 12 Hours
- Last 24 Hours
- Last 7 Days
- Last 30 Days

The time frame you select depends on your purpose. If you want to monitor current system performance, select **Last 1 Hour** (the default) as the time period. If you want to do capacity planning, select **Last 30 Days** as the time period.

To select the time period:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance > Dashboard**. The **Dashboard** page is displayed.
3. Use the time chooser in the upper left corner to select a different time period in the drop-down list.

The data displayed in the Dashboard changes accordingly.

22.4.2 Call Volume

The Call Volume chart shows the total number of calls and the number of bad calls for the system during the specified time interval. In the bar graph, the green segment indicates the number of good calls and the red segment indicates the number of bad calls. A call's designation as good or bad is derived from the Mean Opinion Score (MOS). A MOS value above 3.6 indicates good call quality, and a MOS value below 3.0 indicates bad call quality.

22.4.2.1 Monitoring Call Volume

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**. The **Dashboard** page is launched.

3. In the Call Volume chart (upper left corner), hover over a bar on the graph to see the following details:

   - The green segment shows the total number of calls (good and bad) and the time range.
   - The red segment shows the number of bad calls, the percentage of total calls that were bad, and the time range.

22.4.2.2 Getting Detailed Information About Calls

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**. The **Dashboard** page is launched.
3. In the Call Volume chart (upper left corner), click a bar in the graph.

   The Call Quality page is launched, and the information it displays varies depending on whether you click a green or red segment of a bar:

   - If you click a green segment, the **Call Quality** page shows the following information:
     - Calls filtered by the time interval for the bar you clicked, with the most recent call during that interval listed first
     - Metrics for the most recent call (on the Details tab)
     - IP path for the most recent call (on the IP Path Trace tab)
   - If you click a red segment, the Call Quality page shows bad quality calls filtered by the time interval for the bar you clicked.

For more information about the information displayed on the Call Quality page, see Monitoring Call Quality on page 824.

22.4.3 Call Quality

The Call Quality chart shows the average and worst call quality during the selected time interval. Call quality is measured using the Mean Opinion Score (MOS) scale. A MOS value of 3.6 or higher is considered “toll quality.” A MOS value between 3 and 3.6, which is shown in the yellow area of the chart, indicates substandard but acceptable call quality. A MOS value below 3.0, which is shown in the red area of the chart, indicates poor call quality.

Note:
To collect call quality data, switches require active connections to phones and the call duration must be at least 30 seconds. For more details, see the Requirements on page 728 section.

For more information about factors that impact call quality, see Monitoring Call Quality on page 824.

22.4.3.1 Viewing High-Level Information about Call Quality

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**. The **Dashboard** page is displayed.
3. In the Call Quality chart (upper right corner), hover over a point on the graph to see the following details:
   - To see the average score for a particular time range, hover over a circle on the blue line.
   - To see the worst score for a particular time range, hover over a square on the purple line.

22.4.3.2 Viewing Details for an Average Quality Call or Worst Quality Call

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance > Dashboard**.

   The Dashboard page is displayed.

3. In the Call Quality chart (upper right corner), do one of the following:

   - To view the following details about an average quality call, click a circle on the blue line for the desired time frame:

     - Calls filtered by the time interval for the bar you clicked, with the most recent call during that interval listed first
     - Metrics for the most recent call (on the Details tab)
     - IP path for the most recent call (on the IP Path Trace tab)
   - To view the following details about the worst quality call, click a square on the purple line for the desired time frame:

     - The call with the lowest MOS score during the specified time frame
     - Metrics for this worst quality call (on the Details tab)
     - IP path for this worst quality call (on the IP Path Trace tab)

For more information about the information displayed on the Call Quality page, see Monitoring Call Quality on page 824.

22.4.4 Bandwidth Utilization

The Bandwidth Utilization chart shows the trend lines for the five sites that consumed the most intersite bandwidth for media streams for the selected time period. Site names and their associated colors are listed at the top of the chart, and the color of each trend line corresponds to a site's color. Of the sites with the highest bandwidth utilization, the site with the highest bandwidth utilization is on the left and the site with the lowest bandwidth utilization is on the right.

The information displayed in the Bandwidth Utilization chart could be useful for the following purposes:

- Capacity planning — Frequent bandwidth utilization peaks above 80 percent (in the chart's red zone) could indicate a need for increased WAN bandwidth. But occasional spikes of bandwidth utilization above 80 percent do not necessarily mean that you need to increase bandwidth.
- Troubleshooting — Rejected calls or poor audio quality could be the result of a critical shortage of intersite bandwidth.
- System provisioning — Reviewing bandwidth utilization and trunk group utilization together can provide information to help you better provision the system.

For more information about how bandwidth impacts your MiVoice Connect system, see the *Network Requirements and Preparation* section in the *MiVoice Connect Planning and Installation Guide*.

22.4.4.1 Viewing Highest Bandwidth Utilization

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance**> **Dashboard**. The **Dashboard** page opens.
3. In the Bandwidth Utilization chart (middle left), hover over a point on the graph to see the following details about a site's bandwidth:

   - Site name
   - Average bandwidth utilization for that site during the given time range
   - Maximum bandwidth utilization for that site during the given time range
   - Time range

22.4.4.2 Viewing Detailed Information for a Site

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance**> **Dashboard**. The **Dashboard** page opens.
3. In the Bandwidth Utilization chart (middle left), click on a point on a site's trend line.

Note:
The **Status and Maintenance** > **Sites** page is launched, and it displays detailed information about the selected site. For more information about the details displayed on the **Status and Maintenance** > **Sites** page, see Monitoring Site Status on page 758.

22.4.5 Highest Trunk Group Usage

The Highest Trunk Group Usage chart shows trend lines for the five busiest trunk groups. The percentage of total trunk ports used within the group is shown for the specified time interval. Trunk group names and their associated colors are listed at the top of the chart, and each trend line's color corresponds to a trunk group's color. Of the five busiest trunk groups, the trunk group with the highest usage is listed on the left and the trunk group with the lowest usage is listed on the right.

The information displayed in the Highest Trunk Group Usage chart could be useful for the following purposes:

- Troubleshooting — Failing calls could result when the call volume exceeds the trunk group capacity in your system.
- Capacity planning — Trunk group usage over 50 percent (in the chart's yellow zone) could indicate a need to increase trunk group capacity or WAN bandwidth. But occasional spikes of trunk group usage above 50 percent do not necessarily mean that you need to increase trunk group capacity.
- System provisioning — Reviewing trunk group utilization and bandwidth utilization together can provide information to help you better provision the system.

22.4.5.1 Viewing Trunk Groups with the Highest Usage

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**. The **Dashboard** page is displayed.
3. In the Highest Trunk Group Usage chart (middle right), hover over a point on the graph to see the following details about the trunk groups with the highest usage:

   - Trunk group name
   - Site name
   - Average simultaneous trunk port occupancy for that trunk group for the given time range
   - Maximum simultaneous trunk port occupancy for that trunk group for the given time range
   - Time range

22.4.5.2 Viewing Detailed Information for a Trunk Group

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**.The **Dashboard** page is displayed.
3. In the Highest Trunk Group Usage chart (middle right), click on a point on the usage trend line for a trunk group.

The Status and Maintenance > Trunk Groups page is launched, and it displays detailed information about the selected trunk group and time interval. For more information about the details displayed on the Status and Maintenance > Trunk Groups page, see Monitoring Trunk Group Status on page 810.

22.4.6 Highest Feature Usage

The Highest Feature Usage chart shows the trend line for the five switches with the highest total feature usage. These features include voice mail, conferences, group paging, hunt groups, bridged call appearance, and workgroups. Use of these features impacts CPU utilization on each switch that hosts these features, and heavy use of these features could impact system performance.

Switch names and their associated colors are shown at the top of the chart, and each trend line's color corresponds to a switch's color. At the top of the chart, the switches are listed from highest feature usage on the left to lowest feature usage on the right.

Feature usage counts reflect the number of active calls at the time TMS writes to the Monitoring Database, not the cumulative number of active calls between measurement intervals. For this reason, calls less than 30 seconds in duration might not be reflected in feature usage counts.

The information displayed in the Highest Feature Usage chart could be useful for the following purposes:

- Load balancing — High feature usage on a particular switch might indicate a need to move frequently used features to ports on different switches.
- Capacity planning — High feature usage on the switches in your MiVoice Connect system might indicate a need to add switch capacity to the system.

22.4.6.1 Viewing Highest Feature Usage

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance**> **Dashboard**. The **Dashboard** page opens.
3. In the Highest Feature Usage chart (lower left), hover over a point on the graph to see the following details about features with the highest usage:

   - Name of the site where the ports supporting the features are being used
   - Name of the switch on which the feature depends
   - Total number of ports used during the specified time range
   - Time range

22.4.6.2 Viewing Detailed Information for a Switch with Highest Feature Usage

1. Launch Connect Director.

2. In the navigation menu, click **Maintenance**> **Dashboard**. The **Dashboard** page opens.
3. In the Highest Average CPU Usage chart (lower right), click a point on a usage trend line for a switch or soft switch.

The Appliances page or the Servers page is launched, and it displays detailed information about the switch or softswitch with the highest average CPU usage during the selected time interval. For more information about the details displayed on the Appliances page, see Monitoring Appliance Status on page 766.

22.4.7 Highest Average CPU Usage

The Highest Average CPU Usage chart shows the trend line for the five switches or soft switches (servers) with the highest CPU usage by percentage. Switch or softswitch names and their associated colors are listed at the top of the chart, and each trend line's color corresponds to a switch's color. Of the five switches with the highest CPU usage, the switch with the highest average CPU usage is on the left and the switch with the lowest average CPU usage is on the right.

The information displayed in the Highest Average CPU Usage chart could be useful for the following purposes:

- Capacity planning — Frequent spikes in average CPU usage for a switch could indicate that the switch is overburdened.
- Troubleshooting — Average CPU usage above 60 percent could cause performance issues.
- Load balancing — High CPU usage on a particular switch or softswitch could indicate a need to add more switches or move frequently used features to ports on different switches.

22.4.7.1 Viewing Highest Average CPU Usage

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**. The **Dashboard** page opens.

3. In the Highest Average CPU Usage chart (lower right), hover over a point on the graph to see the following details about switches or softswitches (servers) with the highest average CPU usage:

   - Site name
   - Switch name
   - Average CPU usage during the specified time range
   - Maximum CPU usage during the specified time range
   - Average memory usage during the specified time range
   - Maximum memory usage during the specified time range
   - Time range

22.4.7.2 Viewing Detailed Info for Switch/Softswitch with Highest Average CPU Usage

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Dashboard**. The **Dashboard** page is displayed.
3. In the Highest Average CPU Usage chart (lower right), click a point on a usage trend line for a switch or soft switch.

The Appliances page or the Servers page is launched, and it displays detailed information about the switch or softswitch with the highest average CPU usage during the selected time interval. For more information about the details displayed on the Appliances page, see Monitoring Appliance Status on page 766. For more information about the details displayed on the Servers page, see Monitoring Server Status on page 788.

22.5 Viewing the Topology of Your System

The Topology feature displays the real-time status and connectivity for MiVoice Connect system components. You can view your system components in either of the following visual maps:

- The System view shows all configured sites, including all voice switches and servers for each site. This view provides a high-level overview of your system's configuration and status.
- The Site view shows all configured components (including servers, voice switches, service appliances, softswitches, voice mail switches, trunk groups, and phones) for a particular site.

In both views, the node icons are color coded, which allows you to see the current status of each site and component at a glance. Status for sites is aggregated to the most severe status based on the site's components. For example, if a switch at a site is down, the icon for the switch would be red and the icon for the site would be red, even if other switches at the site are green or yellow. The topology node icons and the status colors are described in the following table.

You can see the status of the connections or associations between nodes by clicking a particular node. The connections or associations are displayed based on the perspective of the node that you click. Therefore, if you click on each of the two nodes that are connected by a line, the line could indicate a different connectivity status based on which node is in focus.

The status of the connectivity between nodes is represented by a colored line or other indicator, as follows:

- A green line indicates that the nodes are connected.
- A dashed yellow line indicates that the connection between the nodes is functional but impaired or limited in some way.
- A dashed red line indicates that there is no communication between the nodes because of a software, hardware, or network issue for at least one of the nodes.
- A gray line indicates one of the following, depending on the nodes connected with it:
    - When DRS is enabled, a gray line connecting two sites indicates that calls can be routed between the sites, but protocol communication between the sites is not necessary.
    - In the System view, a gray line between the WAN node and nodes with gray site icons indicates that these sites have been defined in the system but currently have no hardware configured.
    - In the Site view, a gray line between voice switches and trunk groups or phones indicates which switch manages those trunk groups or phones.

Connectivity status is independent of device status. For example, a green switch icon means that the device is operating normally, but if you click the switch node icon you might see that it has a dashed red connectivity line to one or more switches, indicating that it cannot communicate with these switches.

When you click a site node, the site's connectivity to other sites is aggregated based on the connectivity status of the site's switches and servers. For example, if a site has a switch that is down (red) and a switch that is operating with some impairment (yellow), the line showing that site's connectivity to other sites is yellow, indicating some impairment.

When you click a switch or server node, the lines represent switch-to-switch, switch-to-server, or server-to-server connections, depending on the type of node you click. Connectivity between these components relies on one or more of the following Mitel proprietary protocols, which are described in the *MiVoice Connect Maintenance Guide*:

- Distributed Telephony Application Service (DTAS)
- Location Service Protocol (LSP)
- Network Call Control (NCC) Remote Procedure Call (RPC)

The communication protocol for these connections depends on whether Distributed Routing Service (DRS) is enabled or disabled, as follows:

- If DRS is enabled:
  - For switch-to-switch connections within the same site, the connectivity line represents a connection using LSP.
  - For switch-to-server connections, the connectivity line represents a connection using LSP. If the switch is managed by the server, the connectivity line also represents an NCC RPC connection.
  - For server-to-server connections, the connectivity line represents a connection using DTAS and LSP.
- If DRS is disabled:
  - For switch-to-switch connections, the connectivity line represents a connection using LSP.
  - For switch-to-server connections, the connectivity line represents a connection using LSP. If the switch is managed by the server, the connectivity line also represents NCC RPC connections.
  - For server-to-server connections, the connectivity line represents a connection using DTAS and LSP connections.

When more than one protocol is used, the color of the connectivity line represents the worst status of any active protocols.

Note:

Status and connection information displayed in the topology map could be up to two minutes old.

Table 175: System Topology Node Icons

Icon	Description
	Represents a site. The color of the icon changes based on status: • Green indicates that all switches and servers at the site are in service. • Yellow indicates that one or more switches or servers are impaired but not out of service. • Red indicates that one or more switches or servers are out of service. • Gray indicates that there is no hardware installed at the site.
	Represents a site with one or more servers on premise. The color of the icon changes based on status: • Green indicates that all switches and servers at the site are in service. • Yellow indicates that one or more switches or servers at the site are impaired but not out of service. • Red indicates that one or more switches or servers are out of service. • Gray indicates that the system does not have enough information to determine the status.
	Represents a voice switch. The color of the icon changes based on status: • Green indicates that the switch is in service. • Yellow indicates that the switch is impaired or FTP booted but not out of service. For example, if some trunk or phone ports on the switch are out of service, that switch's node icon would be yellow. • Red indicates that the switch is out of service. • Gray indicates that the system does not have enough information to determine the status.

Icon	Description
	Represents a server. The color of the icon changes based on status: • Green indicates that the server is operating normally. • Yellow indicates that the server is impaired but still functioning. • Red indicates that the server has a critical error state. • Gray indicates that the system does not have enough information to determine the status.
	Represents a trunk group. The color of the icon changes based on status: • Green indicates that the ratio of In Service trunks to Configured trunks is greater than 50 percent. • Yellow indicates that the ratio of In Service trunks to Configured trunks is between 20 and 50 percent. • Red indicates that the ratio of In Service trunks to Configured trunks is 20 percent or less. • Gray indicates that no trunks are configured in the trunk group.
	Represents a collection of phones. The number of phones is indicated under the node icon.
	Represents a wide area network (WAN)

22.5.1 Navigating the Topology Map

To easily focus on the components you want to see, you can adjust the topology map in a variety of ways, as described in this section.

22.5.1.1 Expanding and Collapsing Nodes

To focus on a particular node in the topology map, you select that node by clicking it. When the node is selected, it is highlighted with a blue circle. By right-clicking a selected node icon, you can access a pop-up menu with commands relevant to that type of node. For example, right-clicking the WAN node displays a menu that lets you expand or collapse all sites.

For sites that include hardware, you can click the site's node icon and then click on the node.

22.5.1.2 Refreshing the View

By default, the topology map automatically refreshes every 5 minutes. You can stop or resume automatic refreshing by clicking the **Stop Refreshing** button or the **Resume Refreshing** button at the top right corner of the page. You can refresh the view immediately by clicking the **Refresh** button.

22.5.1.3 Zooming in and out in the Topology Map

From any view in the topology map, you can use the mouse wheel to zoom in and out so that the size of the map increases or decreases.

22.5.1.4 Viewing IP Addresses for Servers and Switches

To view the IP address for a switch or server, hover over the node icon for that component.

22.5.1.5 Accessing a List of Sites

Click the **Show Sites** Menu button to display the **All Sites** list, which provides an expandable tree that shows a nested list of all configured sites, reflecting parent-child relationships for the sites. After clicking the top of the tree to expand the list, you can double-click any active site to see a topology map for that site. Each site in the list has a colored icon that corresponds to the site's status.

You can collapse the **All Sites** list by clicking at the top of the heading bar, and you can expand it by clicking. To reset the topology map to the high-level System view, click the "All Sites" entry in the **All Sites** list. To close the **All Sites** list, click the **Hide Sites Menu** button.

22.5.1.6 Repositioning Node Icons and All Sites List in Map View

To focus on a particular node within the topology map, you can adjust the view as follows:

- Click and drag any node icon to change its orientation in the topology map.
- Click any point in the background of the topology map and drag to reposition the map.

To reposition the **All Sites** list on the page, click and drag the expanded or minimized list to a different area on the page.

22.5.1.7 Expanding All Sites

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Topology**. The MiVoice Connect System view is displayed.
3. Click the **WAN** icon.

> **Note**:
>
> The WAN node is highlighted with a blue circle.

4. Right click the **WAN** icon and select **Expand All Sites**.

All sites, servers, and switches in the MiVoice Connect system and their logical connections are displayed.

22.5.2 Viewing System Topology

The nodes in the System view represent logical and physical MiVoice Connect system components: sites, servers, and switches.

> **Note**:
>
> The System view reflects logical connectivity. For this reason, the network icon labeled as a WAN might actually represent a LAN.

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Topology**.

   The high-level MiVoice Connect System view is displayed, showing sites configured in the system.
3. To see all configured components and associations, click the WAN node icon.

   The node is highlighted with a blue circle.

4. Right-click the highlighted WAN node icon, and select **Expand All Sites** from the pop-up menu.

   All sites, switches, and servers in the MiVoice Connect system are displayed.
5. Click any site, server, or switch to see the one-way connectivity for that component to other components in the system.

Note:

You can easily remove components from the topology view for a particular site by clicking the site's node icon and then clicking 

22.5.3 Viewing Site Topology

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Topology**.

Note:
The high-level Connect System view is displayed, showing sites configured in the system.

3. To see the topology for a site where hardware is installed, do one of the following:

   - Use the Sites Menu, as follows:

     a. Click **Show Sites Menu**. The All Sites list is displayed.
     b. Click  to expand the menu.
     c. In the **All Sites** list, double-click the site.

Note:
All servers, switches, trunk groups, and phone collections for the site are displayed.

- Use the pop-up command menu as follows:

  a. Click the node icon for that site.

  The site's node icon is highlighted with a blue circle.

  b. Right-click the highlighted site node icon, and select **Show Site Topology** from the pop-up menu.

Note:
All servers, switches, trunk groups, and phone collections for the site are displayed.

4. Click the icon for any server, switch, trunk group, or phone collection to see the one-way connectivity from that component to other components in the system.
5. To see details on any component, do the following:

   a. Click the component's icon.

   The component's node is highlighted with a blue circle.

   b. Right-click the highlighted node, and select one of the following commands from the pop-up menu:

   - For a server, select **Show Server Details**.
   - For a switch, select **Show Switch Details**.
   - For a trunk group, select **Show Trunk Group Details**.
   - For phones, do one of the following:
   - Select **Show Phone Details (This Site)**.
   - Select **Show Phone Details (This Switch)**. The status page for the selected component is displayed.

22.5.4 Viewing Site Connectivity

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Topology**. The Connect System view is displayed.

3. Click the node icon for a site.

The site's icon is highlighted with a blue circle, and the site's one-way connectivity to other components is displayed.

22.5.5 Viewing Server Connectivity

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Topology**. The Connect System view is displayed.
3. Expand a site by doing one of the following:
   - In the **All Sites** list, click a site.
   - In the topology map, click a site node and then click the plus icon on the site node.
   - In the topology map, click a site node and then right-click it and select **Show Site Topology** from the pop-up menu.
4. Click a server icon.

The server is highlighted with a blue circle, and one-way connectivity to other components is displayed.

22.5.6 Viewing Switch Connectivity

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Topology**. The Connect System view is displayed.
3. Expand a site by doing one of the following:
   - In the **All Sites** list, click a site.
   - In the topology map, select a site and click the plus icon on the site node.
4. Click a switch icon.

The switch is highlighted with a blue circle, and the switch's one-way connectivity to other components is displayed. The server that manages the switch is indicated by a small circle (switch management indicator) on the connection line.

22.6 Monitoring Switch Connectivity

The Connectivity page shows connectivity status for all MiVoice Connect voice switches and appliances configured in the system.

When Distributed Routing Service (DRS) is enabled, the switch connectivity table is organized by site. When DRS is disabled, status for all MiVoice Connect voice switches is shown.

In the connectivity grid, the following indicators provide information about a switch:

- Green with a check mark indicates that the switch is connected and communicating with other switches in the system.
- Yellow with a question mark indicates that the switch connectivity is unknown because it cannot communicate with TMS.
- Red with an “X” indicates that the switch has lost communications with the server.

22.7 Monitoring the Status of Mitel Components

The status pages available through the **Maintenance** menu provide a detailed view of real-time status, performance metrics, and call history for the following system components:

- System
- Sites
- Appliances
- Servers
- IP phones
- Trunk groups
- Voice mail
- Make Me Conferencing
- Audio/Web Conferencing
- IM
- Connect Sync

The status pages are divided into a top pane and a bottom pane. The top pane (the “list pane”) displays a list of components and their status, and the bottom pane (the “details pane”) displays detailed information about the specific component highlighted in the top pane. Where appropriate, the bottom pane also provides additional tabs for information such as detailed status, performance, and related calls.

When you click a particular type of status page in the navigation menu, by default the first item in the list pane is selected and that item’s detailed information is displayed in the details pane. You can select another item in the list pane and view its details in the details pane.

22.7.1 Monitoring System Status

The **Status and Maintenance** > **System** page provides a high-level summary of the components in your MiVoice Connect system. The page includes a list pane at the top and a bottom pane that shows the system's conferencing capacity.

22.7.1.1 Status and Maintenance > System List Pane

The Sites area on the left side of the list pane displays a list of sites in configuration-hierarchy order and provides high-level information about site status. The Servers and Appliances area on the right side of the list pane shows servers and appliances grouped according to the sites to which they belong.

On the **Status and Maintenance** > **System** page, you can click a site name to open the Status and Maintenance > Sites page or a server or appliance name to open the **Status and Maintenance** > **Servers** page. For more information, see Monitoring Site Status on page 758 and Monitoring Server Status on page 788.

Table 176: Columns in the Status and Maintenance > System List Pane

Column Name	Description
Sites	
site status indicator	High-level status of the site: • Green indicates that the site is in service and connected. • Yellow indicates a warning state at the site that does not affect the site's service. • Red indicates that the site is down or experiencing a severe service impact.
Site	The name of the site
TMS Comm	TMS connections within the site. The first number represents the available connections, and the second number represents the expected total number of connections.

Column Name	Description
Usage	The current switch and phone usage for the site. Possible values are: • Idle—No ports or IP phones are off-hook or in-use. • In Service—The configured ports or IP phones are ready for service. • In Use—At least one port or IP phone has an active call. • Ports Off-Hook—At least one port or IP phone is off-hook, but no ports are in use. • Unknown—The usage state is unknown, perhaps because communication between the server and the switch has been lost.
Service	The current service status for the site. More than one service state can be in effect for a site, but only the most severe service state is displayed until that state is resolved. Possible values are: • Unknown—The state of the switch is unknown. This is typically the case during an upgrade when the switch is disconnected from the system. • In Service—All system components are in service and functioning. • Firmware Update Available—The server has a new optional version of firmware available for voice switches. A voice switch in this state continues to run call control as well as access the voice services on the server. To propagate the patch to the voice switches, you must restart them. • Restart Pending—A Restart When Idle command was issued, but the restart did not occur because switch ports are still in use. • Upgrade In Progress—The voice switch is currently being upgraded with a new software version.

Column Name	Description
Service (continued)	• Platform Version Mismatch—The switch firmware version does not match the build version installed on the Headquarters server. • Booting From FTP—The voice switch did not boot from flash memory but booted from an FTP server, most likely on the server. You can correct this problem by rebooting the voice switch. If this does not correct the problem, contact Mitel Technical Support. • Port Out Of Service—One or more, but not all, trunk or phone ports are out of service on the voice switch. Ports or IP phones typically go out of service because either someone manually put them out of service or the call control software automatically put them out of service due to a signaling problem (for example, the dial tone was not received from the central office). • Hunt Group Out Of Service—All ports associated with a hunt group are out of service. • SIP Trunks out Of Service—All ports associated with a SIP trunk are out of service. • SIP Trunks Out Of Service Operational—All ports associated with a SIP trunk are out of service because of operational trouble, typically on the other side of the trunk connection. • SIP Trunks Out Of Service Administrative—All ports associated with a SIP trunk are out of service because an administrator has set them to an “out of service” state. • Ports Out Of Service Busy—All ports are out of service. • SoftPhones Out Of Service—All softphones are out of service for one or more switches in the system. • All Ports Out Of Service—All ports (trunk, softphone, analog phone, and IP phone) on a voice switch at the site are out of service.

Column Name	Description
Service (continued)	• Configuration Mismatch—A configuration mismatch has been detected between a switch and a server, between two servers, or between two switches. • Firmware Mismatch—The firmware on one or more phones does not match the build version installed on the Headquarters server. • D Channel Down—A PRI or BRI signaling channel (D channel) is out of service. • Fan Failure—A fan associated at least one switch has failed. • Temperature Failure—The temperature associated with a switch has exceeded the normal safe range. • Voltage Failure—The voltage associated with a switch has exceeded the normal safe range. • Firmware Update Failure—A firmware update was requested for a phone, but it failed. • Disk Failure—A disk associated with a switch or server has failed. • Lost Communication—The server lost communication with the voice switch. Note that the voice switch may be fully operational but the server cannot see the voice switch due to a networking issue. This also occurs when the voice switch is powered off.
Servers and Appliances	
status indicator	Status of the server or appliance
Server/Appliance	The name of the server or appliance
Type	The type of server or appliance

Column Name	Description
Status	The current status of the server or appliance. Possible values are: • Unknown—The status of the server or appliance is unknown. This typically occurs during upgrade or when the server is disconnected from the Headquarters server for an extended period of time. • In Service—The server or appliance is in service. • Software Upgrade Available—A new software version is available for the server or appliance. • Software Version Mismatch—The version of the server software does not match the Headquarters server, which could cause instability. • Database Version Mismatch—The schema version of the distributed database instance on the server does not match the version expected by the server. • SMTP Send Error—The SMTP server is having persistent trouble sending email. • Error Initialize TMS—The TMS instance on the server has encountered an error upon initialization. • Lost Database Connection—The connection to the Headquarters database or local distributed database has failed. • Lost TAPI—TAPI connectivity has failed. • Lost Communication—The connection to one or more switches has failed. • Unexpected Error—An unknown error has occurred, which indicates a critical problem.
Services	The status of the server's services. Possible values are: • Running • Not Running • Unknown
Disk Used	The percentage of the server's disk space in use

Column Name	Description
DB	The status of the server's local database, if it has one: • A green icon indicates that the server's local database is functioning normally. • A red icon indicates that the database is down or, if distributed database is enabled, is not synchronized with the database on the Headquarters server.

22.7.1.2 Status and Maintenance > System Bottom Pane

The bottom pane on the System status page summarizes system-wide audio/web conferencing capacity and provides a section that allows you to apply commands to servers, switches, and appliances. The following table shows the columns in the Conferencing pane.

Table 177: Columns in the Status and Maintenance > System Bottom Pane (Conferencing)

Column Name	Description
Total Conference Ports	The types of conferencing services available on the system
In-Use	The total number of audio and Web conference ports currently in use
Licensed Capacity	The number of audio and Web licenses on the system
System Capacity	The system's configured maximum capacity for simultaneous audio or Web conferences
Apply This Command to All Switches and Appliances	If you want to apply one of the following commands to all switches and appliances in the system, select the command from the drop-down and click **Apply**: • **Restart** • **Restart when idle** • **Reboot** • **Reboot when idle**

Column Name	Description
Apply this Command to All Servers	If you want to apply one of the following commands to all servers in the system, select the command from the drop-down list and click **Apply**: • **Publish Wallpapers** • **Publish Ringtones** • **Publish All**
Temporarily Disable IP Phone Failover Across Sites	For some maintenance tasks, such as system-wide maintenance, enable this option to temporarily disable IP phone failover. When this feature is enabled, spare switches also do not fail over throughout the system. Ensure that you deselect this option when the maintenance task is finished.

For information about how to use the maintenance commands at the bottom of the **Status and Maintenance** > **System** page, see the *MiVoice Connect Maintenance Guide*.

22.7.2 Monitoring Site Status

On the **Status and Maintenance** > **Sites** page, you can view a list of all sites configured in your MiVoice Connect system and see a summary of real-time status and performance information for each site. The page includes a list pane and a details pane with **Status**, **Performance**, and **Calls** tabs.

22.7.2.1 Status and Maintenance > Sites List Pane

The following table shows the columns in the list pane at the top of the **Sites** page.

Table 178: Columns in the Status and Maintenance > Sites List Pane

Column Name	Description
Command (two drop-down lists)	Select one of the following maintenance commands to perform on the switches at the selected site or sites: • **Reboot and Reset:** Manage how you reboot appliances or restart services. **RebootAppliance(s)** reboots/restarts the appliance or service immediately. Calls that the switches are servicing when this command is selected will be lost. For the following voice switches and service appliances, Reboot Appliance(s) performs an upgrade and reboot if a new software version is available: SG90V, SG50V, SG90BRIV, virtual phone switch, virtual trunk switch, SA100, SA400, and virtual service appliance. **Reboot Appliance(s) When Idle** stops and restarts all services on each switch or appliance at the selected site after the calls they are managing are completed. Calls that are active when these commands are selected are allowed to finish normally. For the following voice switches and service appliances, the **Reboot Appliance(s) When Idle** option performs an upgrade and reboot if a new software version is available: SG90V, SG50V, SG90BRIV, virtual phone switch, virtual trunk switch, SA100, SA400, and virtual service appliance. **Restart Mitel Services** restarts the appliance or service immediately. Calls that the switches are servicing when this command is selected will be lost.

Column Name	Description
Command (two drop-down lists) (continued)	**Restart Mitel Services When Idle** stops and restarts all services on each switch or appliance at the selected site after the calls they are managing are completed. Calls that are active when these commands are selected are allowed to finish normally. • **Download Software:** Manage the download of software to appliances or the Linux DVS. **Download to Linux DVS** downloads the ConnectApplianceInstall.iso file for the Linux DVS. **Download to Appliance(s)** downloads software to the switches that use the two-stage upgrade process. **Cancel Pending Download** stops the download of switch software for the switches that use the two-stage upgrade process. • **Update Software:** Manage the update process for appliances. **Update Appliance(s)** triggers the selected switches to upgrade to the downloaded version of the software and then reboot. **Update Appliance(s) When Idle** triggers the selected switches to upgrade to the downloaded software when the switches are idle and then to reboot when the upgrade is complete. For more information about the two-stage upgrade process for switches, see the *MiVoice Connect Maintenance Guide*.
command check box	Allows you to select one or more sites to apply maintenance commands to the switches at that site or sites

Column Name	Description
status indicator	High-level status of the site: • Green indicates that the site is in service and connected. • Yellow indicates a problem (a warning state) at the site that does not affect the site's service. • Red indicates that the site is down or experiencing a severe service impact.
Site	The name of the site
TMS Comm	The communication state of all switches at the site. The first number represents switches with which the Telephony Management Service (TMS) can currently communicate. The second number is the total number of switches at the site. For more information about TMS, see the *MiVoice Connect Maintenance Guide*.
Usage	The current switch and phone usage for the site. Possible values are: • Idle—No ports or IP phones are off-hook or in-use. • In Service—The configured ports or IP phones are ready for service. • In Use—At least one port or IP phone has an active call. • Ports Off-Hook—At least one port or IP phone is off-hook, but no ports are in use. • Unknown—The usage state is unknown, perhaps because communication between the server and the switch has been lost.

Column Name	Description
Service	The current service status for the site. Possible values are: • Unknown—The state of the switch is unknown. This is typically the case during an upgrade when the switch is disconnected from the system. • In Service—All system components are in service and functioning. • Firmware Update Available—The server has a new optional version of software available for voice switches. A voice switch in this state continues to run call control as well as access the voice services on the server. To propagate the patch to the voice switches, you must restart them. • Restart Pending—A Restart When Idle command was issued, but the restart did not occur because switch ports are still in use. • Upgrade In Progress—The voice switch is currently being upgraded with a new software version. • Version Mismatch—The switch software version does not match the build version installed on the Headquarters server. • Booting From FTP—The voice switch did not boot from flash memory but booted from an FTP server, most likely on the server. You can correct this problem by rebooting the voice switch. If this does not correct the problem, contact Mitel Technical Support. • Port Out Of Service—One or more, but not all, trunk or phone ports are out of service on the voice switch. Ports or IP phones typically go out of service because either someone manually put them out of service or the call control software automatically put them out of service due to a signaling problem (for example, the dial tone was not received from the central office).

Column Name	Description
Service (continued)	• Hunt Group Out Of Service—All ports associated with a hunt group are out of service. • SIP Trunks Out Of Service—All ports associated with a SIP trunk are out of service. • SIP Trunks Out Of Service Operational—All ports associated with a SIP trunk are out of service because of operational trouble, typically on the other side of the trunk connection. • SIP Trunks Out Of Service Administrative—All ports associated with a SIP trunk are out of service because an administrator has set them to an “out of service” state. • Ports Out Of Service Busy—All ports are out of service. • SoftPhones Out Of Service—All softphones are out of service for one or more switches in the system. • All Ports Out Of Service—All ports (trunk, softphone, analog phone, and IP phone) on a voice switch at the site are out of service. • Configuration Mismatch—A configuration mismatch has been detected between a switch and a server, between two servers, or between two switches. • Firmware Mismatch—The software on one or more phones does not match the build version installed on the Headquarters server. • D Channel Down—A PRI or BRI signaling channel (D channel) is out of service. • Fan Failure—A fan associated at least one switch has failed. • Temperature Failure—The temperature associated with a switch has exceeded the normal safe range. • Voltage Failure—The voltage associated with a switch has exceeded the normal safe range.

Column Name	Description
Service (continued)	• Firmware Update Failure—A software update was requested for a phone, but it failed. • Disk Failure—A disk associated with a switch or server has failed. • Lost Communication—The server lost communication with the voice switch. Note that the voice switch may be fully operational but the server cannot see the voice switch due to a networking issue. This also occurs when the voice switch is powered off.
Download Status	The download status of the firmware for the switch or appliance.
SIP Trunks	The first number represents the SIP trunks in use (total SIP trunks configured in the database for all switches at each site), and the second number represents the SIP trunk capacity count (the sum of each switch's built-in and configured SIP port capacity).
IP Phones	The first number represents IP phones in use (the total number of IP phone ports configured in the database), and the second number represents IP phone capacity (the sum of all switches' built-in and configured IP phone ports capacity).
Bandwidth	The first number represents active bandwidth, and the second number represents admission bandwidth.
Staged Build	The firmware build that has been downloaded to a second partition on the switch or appliance but that has not yet been installed on the switch or ap pliance (using the Update Firmware command).

22.7.2.2 Status and Maintenance > Sites Details Pane

The details pane at the bottom of the page includes Status, Performance, and Calls tabs.

22.7.2.2.1 Status Tab

For the site selected in the details pane, the Status tab displays:

- A list of the site's softswitches, voice switches, voicemail-enabled switches, and service appliances on the left side of the pane

- A list of servers (including Headquarters, voicemail-enabled switches, and servers/appliances) on the right side of the pane

For details about the columns included in the lists, see the *Columns in the Status and Maintenance > Appliances List Pane* table in the *Status and Maintenance > Appliances List Pane* section.

To see details about a particular switch or server:

- On the **Status** tab, click the name of the switch or server/appliance that you want more information about.

The status page for that switch or server/appliance is displayed.

22.7.2.2.2 Performance Tab

The Performance tab includes the following charts:

- The Trunk Group Usage chart shows the five trunk groups with the highest usage on the selected site.
- The Bandwidth Usage chart shows the bandwidth usage trend for the site for the selected time period.

22.7.2.2.3 Calls Tab

The **Calls** tab displays a list of the 10 most recent calls, by default, associated with the selected site. For details about the fields on the **Calls** tab, see Columns on the Call Tab Page.

Table 179: Columns on the Call Tab Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect sys tem
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the p hone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured
Ext/Port	The extension number at the source site associated with the endpoint inv olved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.

Column Name	Description
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint in volved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

To see details for a particular call:

- On the **Calls** tab, click a call stream.

The **Call Quality** page, which shows details for the selected call, is displayed.

22.7.3 Monitoring Appliance Status

On the **Status and Maintenance** > **Appliances** page, you can see a list of all switches configured in the system, as well as real-time status and summary statistics for each switch.

22.7.3.1 Status and Maintenance > Appliances List Pane

The following table shows the columns in the list pane at the top of the Appliances page.

Table 180: Columns in the Status and Maintenance > Appliances List Pane

Column Name	Description
Command	Allows selection of one or more appliances to apply one of the following maintenance commands, which are available from the drop-down list. Not all commands can be applied to all switch types. • **Reboot and Reset:** Manage the reboot of appliances. **Reboot Appliance(s)**immediately stops all services and reboots each switch. Calls that the switches are servicing when this command is selected are lost. For the following voice switches and service appliances, this option performs an upgrade and reboot if a new software version is available: SG90V, SG50V, SG90BRIV, virtual phone switch, virtual trunk switch, SA100, SA400, and virtual service appliance. **Reboot Appliance(s) When Idle stops** all services and reboot each switch after the calls that it is managing are completed. Calls that are active when this command is selected are allowed to finish normally. For the following voice switches and service appliances, this option performs an upgrade and reboot if a new software version is available: SG90V, SG50V, SG90BRIV, virtual phone switch, virtual trunk switch, SA100, SA400, and virtual service appliance. **Restart Mitel Services** immediately stops all services and reboots appliance(s). Calls that the switches are servicing when this command is selected are lost. For the following voice switches and service appliances, this option performs an upgrade and reboot if a new firmware version is available: SG90V, SG50V, SG90BRIV, virtual phone switch, virtual trunk switch, SA100, SA400, and virtual service appliance. **Restart Mitel Services When Idle** stops and restarts all services on each switch or appliance at the selected site after the calls they are managing are completed. Calls that are active when these commands are selected are allowed to finish normally. **Reboot Phones** immediately reboots the selected phone(s). This operation interrupts calls. **Reboot Phones When Idle** reboots the selected phone(s) after calls are completed

Column Name	Description
Command (continued)	• **In/Out of Service:** Manage services on appliances. **Put Appliance(s) In service** puts all ports on the switch in service. Ports already in service with active calls are not affected. **Put Appliance(s) Out of Service.** places all ports on the voice switch out of service. Active calls are dropped. This command is a forceful way to remove traffic from a voice switch before you replace the switch **Put Appliance(s) Out of Service When Idle** puts all idle ports out of service, and remaining ports are also put out of service when they go idle. This command is a graceful way to remove traffic from a voice switch before you replace it. • **Failback from Spare:** Manage failback on appliances. **Failback Spare** clears the parameters assigned to the system for failover and returns the switch to the spare-switch state • **Update Software:** Manage updates on appliances. **Update Appliance** triggers a reboot of the switch, which launches an upgrade of the switch software to a new software version that has already been downloaded to the switch. For complete details on the two-stage upgrade process, see the *MiVoice Connect Maintenance Guide*. **Update Appliance(s) When Idle** waits until the switch is idle before triggering a reboot of the switch, which launches an upgrade of the switch software to a new software version that has already been downloaded to the switch. For complete details on the two-stage upgrade process, see the *MiVoice Connect Maintenance Guide*. **Force Appliance(s) Update** launches an upgrade of the current active partition with software from `<drive>:\inetpub \ftproot\tsb`. Be aware that this command immediately disrupts switch operations.

Column Name	Description
Command (continued)	• **Download Software:** Manage software downloads on appliances. **Download Phone Software to Linux DVS** pushes a phone software image to a Linux distributed voice server (Linux DVS). • **Troubleshooting:** Manage troubleshooting on Voice Switches. **Start USB Logging and Reboot** turns on logging to a USB device for the selected switch or switches for diagnostic purposes. After you apply this command, you must immediately reboot the selected switches for the command to take effect. **Stop USB Logging and Reboot** turns off logging to a USB device for the selected switch or switches. After you apply this command, you must immediately reboot the selected switches for the command to take effect. Archive Switch Logs creates an archive copy of the logs for voice switches. The logs are uploaded to the configured FTP location (<drive>:\inetpub\ftproot\Logs).
Command check box	Allows you to select one or more switches to which to apply the selected command. **Note**: The **Command** check box is not applicable for Ingate. If you try to select this option for InGate, an error message stating that the operation is not applicable for InGate is displayed.

Column Name	Description
Status Indicator	High-level status of the site: • Green indicates that the switch is in service and connected. • Yellow indicates a warning state for the switch that does not affect the switch's service. • Red indicates that the switch is down or experiencing a severe service impact. • Grey indicates that the status of the appliance is unknown. **Note**: This status is applicable only for Ingate.
Appliance	The switch or appliance name.
Type	Switch type abbreviation. For a complete list of switch types, see the *Voice Switches* appendix in the *MiVoice Connect Planning and Installation Guide*.
Spare	The list of available spare switches.
Site	Name of the site associated with the switch.
IP	The IP address of the switch or appliance.
MAC	The MAC address of the switch or appliance.
Comms	TMS connections within the site. Displayed as X/Y where X is the available connections and Y is the expected total number of connections. **Note**: For InGate, the value of X is zero (0).

Column Name	Description
Usage	The usage state of the switch: • Idle—No ports or IP phones are off-hook or in-use. • In Service—The configured ports or IP phones are ready for service. • In Use—At least one port or IP phone has an active call. • Ports Off-Hook—At least one port or IP phone is off-hook, but no ports are in use. • Unknown—The usage state is unknown, perhaps because communication between the server and the switch has been lost.

Column Name	Description
Service	The current service status for the switch. Possible values are: • Unknown—The state of the switch is unknown. This is typically the case during an upgrade when the switch is disconnected from the system. • In Service—All system components are in service and functioning. • Firmware Update Available—The server has a new optional version of software available for voice switches. A voice switch in this state continues to run call control as well as access the voice services on the server. To propagate the patch to the voice switches, you must restart them. • Restart Pending—A Restart When Idle command was issued, but the restart did not occur because switch ports are still in use. • Upgrade In Progress—The voice switch is currently being upgraded with a new software version. • Platform Version Mismatch—The switch software version does not match the build version installed on the Headquarters server. • Booting From FTP—The voice switch did not boot from flash memory but booted from an FTP server, most likely on the server. You can correct this problem by rebooting the voice switch. If this does not correct the problem, contact Mitel Technical Support. • Port Out Of Service—One or more, but not all, trunk or phone ports are out of service on the voice switch. Ports or IP phones typically go out of service because either someone manually put them out of service or the call control software automatically put them out of service due to a signaling problem (for example, the dial tone was not received from the central office). • Hunt Group Out Of Service—All ports associated with a hunt group are out of service. • SIP Trunks Out Of Service—All ports associated with a SIP trunk are out of service. • SIP Trunks Out Of Service Operational—All ports associated with a SIP trunk are out of service because of operational trouble, typically on the other side of the trunk connection.

Column Name	Description
Service (continued)	• SIP Trunks Out Of Service Administrative—All ports associated with a SIP trunk are out of service because an administrator has set them to an **out of service** state. • Ports Out Of Service Busy—All ports are out of service. • SoftPhones Out Of Service—All softphones are out of service for one or more switches in the system. • All Ports Out Of Service—All ports (trunk, softphone, analog phone, and IP phone) on a voice switch at the site are out of service. • Configuration Mismatch—A configuration mismatch has been detected between a switch and a server, between two servers, or between two switches. • Firmware Mismatch—The software on one or more phones does not match the build version installed on the Headquarters server. • D Channel Down—A PRI or BRI signaling channel (D channel) is out of service. • Fan Failure—A fan associated at least one switch has failed. • Temperature Failure—The temperature associated with a switch has exceeded the normal safe range. • Voltage Failure—The voltage associated with a switch has exceeded the normal safe range. • Firmware Update Failure—A software update was requested for a phone, but it failed. • Disk Failure—A disk associated with a switch or server has failed. • Lost Communication—The server lost communication with the voice switch. **Note**: The voice switch may be fully operational but the server cannot see the voice switch due to a networking issue. This also occurs when the voice switch is powered off.
Download Status	The download status of the firmware for the switch or appliance.
Phone Image Down load	For distributed voice servers, the download status of a phone firmware image.

Column Name	Description
Phones	The first number represents IP phones in use (the total number of IP phone ports configured in the database), and the second number represents IP phone capacity (the sum of all switches' built-in and configured IP phone ports capacity). For a virtual phone switch, a red number indicates that the number of IP phones in use exceeds the provisioned capacity.
SIP Trunks	The first number represents the SIP trunks in use (total SIP trunks configured in the database for all switches at each site), and the second number represents the SIP trunk capacity count (the sum of each switch's built-in and configured SIP port capacity). For a virtual trunk switch, a red number indicates that the number of SIP trunks in use exceeds the provisioned capacity.
Conf	The first number represents conferences in use, and the second number represents conference capacity. For a virtual phone switch, a red number indicates that the number of active conferences exceeds the provisioned capacity.
BCA	The number of bridged call appearances (BCAs) configured for the switch.
HG	The number of hunt groups configured for the switch.
Role	Specifies whether the switch is operating as a primary switch or a failed-over spare swi tch.
Active Build	The active firmware build running on the switch or appliance.
Staged Build	The firmware build that has been downloaded to a second partition on the switch or appli ance but that has not yet been installed on the switch or appliance (using the Update Fi rmware command).

22.7.3.2 Status and Maintenance > Appliances Details Pane

The details pane at the bottom of the **Status and Maintenance** > **Appliances** page includes the **Status**, **Performance**, and **Calls** tabs.

Note:
By default, **Performance** and **Calls** tabs are disabled for Ingate. However, the values in the **Status** tab will appear as blank for Ingate.

22.7.3.2.1 Status Tab

The **Status** tab on the **Status and Maintenance** > **Appliances** page lets you monitor details for each switch. The details displayed depend on the type of switch or appliance selected. All fields displayed on the Status tab, regardless of switch or appliance type, are described in the following table.

Note:

If you select a softswitch in the list pane, the details pane does not include a Status tab.

Table 181: Fields in the Appliances Details Pane (Status Tab)

Area	Field	Description
Ports	status indicator	Status of the port: • Green indicates that the port is in service. • Yellow indicates a problem (a warning state) for the port. • Red indicates that the port is down.
	Port	The port number
	Description	The full name of the port or the trunk name
	Usage	The usage state of the port. The following values are possible: • Unknown—The state is unknown, likely because communication between the server and the switch has been lost. • In Use—The port has at least one active call. • Off Hook—The port is off-hook and has no active calls.

Area	Field	Description
Ports (continued)	Service	The service state of the port. The following values are possible: • In Service—The port is in service. • Out of Service—The port is out of service. On telephone ports, outbound calls are not possible because no dial tone is available. Also, the system does not offer inbound calls to the user. On trunk ports, outbound calls do not seize the trunk, and inbound calls are not answered. On trunk ports, outbound calls do not seize the trunk, and inbound calls are not answered. On loop start trunks, calls seize the trunk to emulate a busy condition to the central office. • Out of Service (operational)—The port is out of service due to a manual “put out of service” command. For trunks, the switch automatically attempts to seize the trunk on a periodic basis. When successful, the trunk is automatically put back in service.
Ports (applies to service appliances)	Conference Ports	Type of conference port
Ports (applies to service appliances) (continued)	Active Conferences (In Use)	The number of audio or web conferences that are currently active For a virtual service appliance, a red number in this field indicates that the number of active conferences exceeds the provisioned capacity.

Area	Field	Description
	Ports (In Use)	The number of ports used for audio or web conferences For a virtual service appliance, a red number in this field indicates that the number of ports in use exceeds the provisioned capacity.
	Ports (Free)	The number of dedicated conference ports available but not currently being used for audio or web conferences
	Percent (Free)	The percentage of dedicated conference ports that are currently available
Channels	command check box	Allows selection of one or more channels to apply maintenance commands (Reset, Put in service, Put out of service, Put out of service when idle)
	status indicator	Status of the port: • Green indicates that the port is in service. • Yellow indicates a problem (a warning state) for the port. • Red indicates that the port is down.
	Port	The port number
	Description	The full name of the port

Area	Field	Description
Channels (continued)	Usage	The usage state of the port. The following values are possible: • Unknown: The state is unknown, likely because communication between the server and the switch has been lost. • In Use: The port has at least one active call. • Off Hook: The port is off-hook and has no active calls.
	Service	The service state of the port. The following values are possible: • In Service: The port is in service. • Out of Service: The port is out of service. On telephone ports, outbound calls are not possible because no dial tone is available. Also, the system does not offer inbound calls to the user. On trunk ports, outbound calls do not seize the trunk, and inbound calls are not answered. On loop start trunks, calls seize the trunk to emulate a busy condition to the central office. • Out of Service (operational): The port is out of service due to a manual “put out of service” command. For trunks, the switch automatically attempts to seize the trunk on a periodic basis. When successful, the trunk is automatically put back in service.

Area	Field	Description
Hardware	Fan	Provides status for the switch's fan. Possible values are as follows: • OK • Slow • Failed • Unknown
	Temperature	Provides status about the temperature of the switch. Possible values are as follows: • OK • Yellow Alarm • Red Alarm • Unknown
	Voltages	Provides status for the switch's talk battery and ring voltages. Possible values are as follows: • OK • Failed • Unknown
Link Status	D-Channel	For a PRI, displays the status of the D-Channel. Possible values are as follows: • Down • In Service • Out of Service • Unknown
	Line Coding	Displays the status of the line coding for the switch. Possible values are as follows: • OK • Bipolar Violations • Loss of Signal • Unknown

Area	Field	Description
Link Status (continued)	Framing	Displays the status of the framing for the switch. Possible values are as follows: • OK • Yellow Alarm • Bit Error • Out of Frame • Unknown
	Loopback	Displays the status of loopback for the switch. Possible values are as follows: • Off • On • Unknown You can apply a loopback command (Off, Line, PayLoad) by selecting a command from the drop-down list.
	Span	Using the check box, provides the option to apply the following commands: • Reset • Put in service • Put out of service when idle
Link Error Summary	Error Free Seconds	The number of error-free seconds that occurred in the last 15 minutes and 24 hours.
	Errored Seconds	The number of errored seconds that occurred in the last 15 minutes and 24 hours.
	Severely Errored Seconds	The number of severely errored seconds that occurred in the last 15 minutes and 24 hours.

Area	Field	Description
Link Error Summary (continued)	Unavailable Seconds	The number of seconds the server was not available.
	Out of Frame	The number of times the link has been out of frame in the past 15 minutes and 24 hours.
USB Storage	USB device logging status	The current status of logging to a USB device connected to the switch. (Rebooting this switch is required before logging actually begins.) Possible values are as follows: • Logging ongoing • Logging stopped • USB device is not present
	USB device total storage	The total amount of storage space available on the USB device.
	USB device free storage	The total amount of free storage space available on the USB device.
Details	Last Boot Time	The last time the switch booted
	Boot Source	The source of the last time the switch booted. Possible values: • Flash • FTP boot • unknown boot source
	Connect Time	The most recent time that the server reestablished a connection with the switch
	Boot ROM Version	The boot ROM version number

Area	Field	Description
	Firmware Version	The version number of the firmware the switch is running
Details (continued)	Platform Version	The version number of the platform for the virtual service appliance
	CPU Board Version	The version number of the switch's CPU board
	CPU Board FPGA Version	The version number of the switch's CPU board field-programmable gate array
	CPU Usage	The current CPU utilization (by percentage) for the switch
	Memory Usage	The current memory utilization (by percentage) for the switch
	Active Calls	The number of calls currently in progress on the switch
	Number of CPU Cores	The number of CPU cores configured for the virtual machine hosting the virtual switch
	CPU Speed (MHz)	The CPU speed of the virtual machine that hosts the virtual switch
	Memory Configured (MB)	The amount of memory configured on the virtual machine that hosts the virtual switch
	Disk Total (GB)	The total disk space capacity of the virtual machine that hosts the virtual service appliance
	Link Status	The status of the connection

Area	Field	Description
	Active Interface	The name of the active network interface card
	Time Server	The IP address of the time server
Hunt Groups	Status Indicator	Indicates the status of the hunt group: • Green indicates that the hunt group is operating normally. • Yellow indicates that the hunt group is out of service. • Red indicates that the hunt group is not functional.
	Extension	The extension number for the hunt group
	Description	The name of the hunt group
	Usage	The current usage state of the hunt group. Possible value are: • Idle • Normal
	Service	The current service state of the hunt group. Possible values are: • Normal • Out of Service (Operational) • Out of Service (Administrative)

Area	Field	Description
IP Phones	status indicator	High-level status for the IP phones configured on the switch: • Green indicates that all phones on the voice switch are in service. • Yellow indicates that the Firmware Status of at least one phone on the voice switch is “Firmware Version Mismatch”. • Red indicates that at least one phone is out of service.
	IP Phones Maintenance link	Click this link to go to the IP Phones status page.
	Phones	The number of IP phones configured on the switch and the current IP phone capacity for the switch
	Usage	The current usage state of the IP phones. Possible values are: • Idle • Normal
	Service	The current service state of the IP phones. Possible values are: • In Service • Out of Service (Operational)
SIP Trunks	command check box	Allows selection of one or more trunks to which to apply maintenance commands (Reset, Put in service, Put out of service, Put out of service when idle), as specified in the Command field at the top of the pane

Area	Field	Description
SIP Trunks	status indicator	Indicates the status of the trunk group based on the percentage of In Service trunks divided by the ports within the trunk group: • Green indicates that the ratio of In Service trunks to Configured trunks is greater than 50 percent. • Yellow indicates that the ratio of In Service trunks to Configured trunks is between 20 and 50 percent. • Red indicates that the ratio of In Service trunks to Configured trunks is 20 percent or less. • Blank indicates that no trunks are configured for this trunk group.
	Name	The name of the SIP trunk
	Trunks	The name of the SIP trunk group. Click the link to open the Trunk Group Status page for the trunk group.
	Usage	The current usage state of the SIP trunks. Possible values are: • Idle • Normal
	Service	The current service state of the trunk group. Possible values are: • In Service • Out of Service • Unknown

Area	Field	Description
Span x (Disabled or Enabled)	Category	Possible values: • Layer 1 • Layer 2 • Loopback • Span
	Status	Possible values: • Active • Off
	Command	Use the command drop-down lists to turn Loopback on or off and to apply various commands to the Span.
Link Performance	Category	For a BRI, provides performance details for each Span for the past 15 minutes and the past 24 hours for the following categories: Link Active Rx/Tx Frames Rx/Tx Errors Warnings
	Status	The status of the link and the number of frames, errors, and warnings
	Command	The number of commands executed on the link
Failover Status	Failover Status	For a spare switch, indicates whether the switch has failed over
	Current Site	The spare switch's current site

Area	Field	Description
	Home Site	The spare switch's home site

22.7.3.2.2 Performance Tab

The Performance tab includes the following charts:

- The Feature Usage chart shows the maximum and average number of calls related to specific features during the specified time interval. The features included in the chart are voicemail, Hunt Groups, Workgroups, BCA, and Paging Groups. Each feature is displayed separately so that you can see the extent to which each feature has been used for a given time interval.

Note:

Feature usage counts reflect the number of active calls at the time TMS writes to the Monitoring Database, not the cumulative number of active calls between measurement intervals. For this reason, calls less than 30 seconds in duration might not be reflected in feature usage counts.

- The Platform Resources chart shows the CPU and memory usage trend for the selected switch for the selected time period.

Because high feature usage can lead to an increase in CPU and memory usage, the information in these charts might be correlated.

22.7.3.2.3 Calls Tab

The **Calls** tab displays a list of the 10 most recent calls, by default, associated with the selected switch. For details about the fields on the **Calls** tab, see Columns on the Call Tab Page.

To see details for a particular call:

- On the Calls tab, click a call stream.

The **Call Quality** page, which shows details for the selected call, is displayed.

Table 182: Columns on the Call Tab Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect sys tem
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the p hone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured
Ext/Port	The extension number at the source site associated with the endpoint inv olved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint in volved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

22.7.4 Monitoring Server Status

From the **Status and Maintenance** > **Servers** page, you can view a list of all servers and appliances configured in the system, as well as the real-time status and summary statistics for each server and appliance.

22.7.4.1 Status and Maintenance > Servers List Pane

The following table shows the columns in the list pane at the top of the **Servers** page.

Table 183: Columns in the Status and Maintenance > Servers List Pane

Column Name	Description
status indicator	Shows the status of the server: • Green indicates that the server is operating normally. • Yellow indicates that the server is in a warning state but still functioning. • Red indicates that the server is in an error state.
Server/Appliance	The name of the server
IP	The IP address of the server
Type	The device type of the server or appliance
Spare	The list of available spare switches.
Site	The name of the site where the server resides

Column Name	Description
Status	The status of the server. Possible values are: • Unknown—The status of the server or appliance is unknown. This typically occurs during upgrade or when the server is disconnected from the Headquarters server for an extended period of time. • In Service—The server or appliance is in service. • Software Upgrade Available—A new software version is available for the server or appliance. • Software Version Mismatch—The version of the server software does not match the Headquarters server, which could cause instability. • Database Version Mismatch—The schema version of the distributed database instance on the server does not match the version expected by the server. • SMTP Send Error—The SMTP server is having persistent trouble sending email. • Error Initialize TMS—The TMS instance on the server has encountered an error upon initialization. • Lost Database Connection—The connection to the Headquarters database or local distributed database has failed. • Lost TAPI—TAPI connectivity has failed. • Lost Communication—The connection to one or more switches has failed. • Unexpected Error—An unknown error has occurred, which indicates a critical problem.
Services	The running state of the server's services. Possible values are: • Running • Not Running • Unknown

Column Name	Description
DB	The status of the server's local database if it has one: • A green icon indicates that the server's local database is functioning normally. • A red icon indicates that the database is down or, if distributed database is enabled, is not synchronized with the Headquarters database.
Disk Used	The percentage of the server's disk space in use

22.7.4.2 Status and Maintenance > Servers Details Pane

The details pane provides more status information about the selected server, including database information, services running on the servers, and a list of calls associated with the selected server. The details pane includes Status and Calls tabs.

22.7.4.2.1 Status Tab

The Status tab displays different information based on the server type you select in the list pane. The fields for the various types of servers are described in the following tables:

- The table below describes the fields on the Status tab for a Headquarters server.
- The table below describes the fields on the Status tab for a Distributed Voice Server.
- Service appliances include only an Application Service Status area on the Status tab, which lists services relevant to service appliances.

Table 184: Fields in the Status and Maintenance > Servers Details Pane (Status Tab) for a Headquarters Server

Field	Description
Create Database Snapshot button	Provides a means to create a snapshot of the primary database
Status	Shows status of TAPI and SMTP Send, as follows: • TAPI status can be OK or Lost TAPI. • SMTP Send status can be OK or Failed.

Field	Description
Database	Provides the following status information for the primary database: • status indicator • Master State • Master Log File Name • Master Log Position
Application Service Status	Provides a list of services running on the server and their status, and allows you to apply commands to these services. For more information about these services, see Mitel Services.

Table 185: Fields in the Status and Maintenance > Servers Details Pane (Status Tab) for a Distributed Voice Server

Field	Description
Resync Database command button	Provides a means to resynchronize the remote database with the primary database on the Headquarters server. For more information, see Creating a Database Snapshot and Resynchronizing Databases on page 799.
Status	Shows status of TAPI and SMTP Send, as follows: • TAPI status can be OK or Lost TAPI. • SMTP Send status can be OK or Failed.

Field	Description
Local Database	If Distributed Database is configured, provides the following details about the local copy of the database: • colored status indicators • Replication State • Slave IO Thread • Slave SQL Thread • Master Log File Name • Read Master Log Position • Exec Master Log Position • Pending Local Updates • Estimated Seconds Behind Master • Last Error
Database Connection	Shows the status of the connection to the Headquarters database
Application Service Status	Provides a list of services running on the server and their status, and allows you to apply commands to these services. For more information about these services, see Mitel Services.

The Application Service Status area, which is included on the Status tab for Headquarters servers, Distributed Voice Servers, and service appliances, provides current status for the Mitel services, which are listed in the following table. For service appliances, the Application Service Status area lists only the services that are relevant to the service appliance.

Table 186: Mitel Services

Name	Description	Details
ShoreTel Monitoring Service	ShoreTel Monitoring Service	This service enables the monitoring processes necessary for the Diagnostics & Monitoring system.

Name	Description	Details
ShoreTel-AuthenticatorService	ShoreTel Authenticator Service	This service authenticates user names and passwords and passes a “ticket” to the ShoreTel Bootstrapper Service.
ShoreTel-BootstrapperService	ShoreTel Bootstrapper Service	This service uses the “ticket” from the ShoreTel Authenticator Service to enable a user to access a URL for a particular service.
ShoreTel-CDR	ShoreTel Call Accounting	This service records call accounting information, workgroup and call queueing data, agent activity, and media streams in call detail records (CDRs).
ShoreTel-ConnectSync	ShoreTel Connect Sync Service	This service enables interactions between MiVoice Connect and Mitel MiCloud Connect systems.
ShoreTel-CSISSVC	ShoreTel CSIS Server	This service manages communications between the server and Mitel clients.
ShoreTel-CSISVMSVC	ShoreTel CSIS VM Server	This service provides notification for clients and voicemail.
ShoreTel-DBUpdateSvc	ShoreTel Database Update	This service accepts database updates from remote computers.

Name	Description	Details
ShoreTel-Director	Connect Director	This service provides diagnostics and monitoring capabilities for MiVoice Connect system components.
ShoreTel-DirectorProxy	Connect Director Proxy	This service is a web server and a reverse proxy for the ShoreTel-Director service.
ShoreTel-DRS	ShoreTel Distributed Routing Service	This service allows the MiVoice Connect system to scale beyond 100 switches.
ShoreTel-EventSvc	ShoreTel Event Service	This service distributes events to Mitel applications and services.
ShoreTel-EventWatch	ShoreTel Event Watch Server	This service monitors the event log and delivers email notifications on certain events.
ShoreTel-IPDS	ShoreTel Client Application Service	This service manages client interaction for desktop, web, and device clients.
ShoreTel_KeyNotifier	ShoreTel_KeyNotifier	This service pushes the authentication keys into the web socket server (ShoreTel-WSS) so that it can complete authentication of its clients.

Name	Description	Details
ShoreTel-MailServ	ShoreTel Voice Mail Message Server	This service provides user mailbox capabilities, AMIS features, and system auto-attendant menus. It also manages the voicemail message store.
ShoreTel-MYSQLCDR	ShoreTel-MYSQLCDR	This service is a database process related to the Call Accounting Database.
ShoreTel-MYSQLConfig	ShoreTel-MYSQLConfig	This service is a database process related to the configuration database for Connect Director.
ShoreTel-MYSQLMonitor	ShoreTel-MYSQLMonitor	This service is a database process related to the monitoring database for the Diagnostics & Monitoring system.
ShoreTel-Notify	ShoreTel Notification Server	This service notifies Mitel application services of changes to the Mitel configuration.
ShoreTel-PortMgr	ShoreTel Voice Mail Port Manager	This service is part of the Mitel voicemail system and acts as the platform for voicemail operations. It provides user mailbox capabilities, AMIS features, and system auto-attendant menus.

Name	Description	Details
ShoreTel-Portmap	ShoreTel Port Mapper	This service manages the registration ports for ONCD RPC applications. It initiates RPC communication connections between TMS and switches.
ShoreTel-RemoteLogSvc	ShoreTel Remote Logging	This service accepts logging from remote computers.
ShoreTel-RPCAP	ShoreTel Remote Packet Capture Service	This service runs remote packet capture operations for diagnostic purposes on Mitel devices. **Note**: Mitel recommends that you do not use this feature on a busy SG-generation switch. Running remote packet capture on an SG-generation switch that has 5 or more active trunk calls can cause the switch to crash.
ShoreTel-SAMS	ShoreTel-SAMS	This service provides support for Connect Director.

Name	Description	Details
ShoreTel-SoftSwitch	ShoreTel Software Telephony Switch	This service hosts call endpoints for voicemail, workgroups, route points, and other interactive voice response extensions. Additionally, it hosts virtual users on the Headquarters softswitch.
ShoreTel-SysMgrSvc	ShoreTel System Management Service	This service provides registration and other functions for IP phones.
ShoreTel-TMS	ShoreTel Telephony Management Server	This service provides the telephony platform for Mitel applications and services.
ShoreTel-TransportSvc	ShoreTel Transport Server	This service provides transport services for Mitel applications and services.
ShoreTel-VmEmSync	ShoreTel Voice Mail Synchronizer	This service provides voicemail and email synchronization.
ShoreTel-WebFrameworkSvc	ShoreTel Web Framework Server	This service provides support for the Connect Web client and Client Application Server.
ShoreTel-WGSvc	ShoreTel Workgroup Server	This service manages workgroups and queues.
ShoreTel-WSS	ShoreTel Web Socket Server	This is the web socket server implementation that manages call control signaling for the Connect client softphone.

Name	Description	Details
ShoreTel-Zin	ShoreTel Database Management Service	This service manages and updates the MiVoice Connect database.

22.7.4.2.2 Starting or Stopping a Service

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Status and Maintenance** > **Servers**. The **Servers** page is displayed.
3. In the **List** pane at the top, click the Headquarters server.

Note:
The details for the Headquarters server are displayed on the **Status** tab.

4. On the **Status** tab, scroll to the **Application Service Status** area, and in the **Command** drop-down list select **Start** or **Stop**.
5. Select the check box of the service or services you want to start or stop.
6. Click **Apply**.
7. In the confirmation dialog box, click **OK**.

22.7.4.2.3 Creating a Database Snapshot and Resynchronizing Databases

You can determine if you need to create a database snapshot by determining how far out of synchronization the remote database is from the Headquarters database. To determine the database synchronization status, compare the master log file name and the master log file position for the Headquarters database (available in the **Database** section of the **Status** tab for the Headquarters server) with the details for the remote database (available in the **Local Database** section of the **Status** tab for the remote server). You can synchronize the two database systems. The synchronization point is the last snapshot performed on the primary database.

To create a database snapshot:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Status and Maintenance** > **Servers**. The **Servers** page is displayed.

3. In the **List** pane at the top, click the Headquarters server.

> **Note**:
> The details for the Headquarters server are displayed on the **Status** tab.

4. Click **Create Database Snapshot**.
5. In the confirmation dialog box, click **OK**.

To resynchronize a remote database with the Headquarters database:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Status and Maintenance** > **Servers**. The **Servers** page is displayed.
3. In the **List** pane at the top, click the remote server.

> **Note**:
> The details for the remote server are displayed on the **Status** tab.

4. Click **Resync Database**.
5. In the confirmation dialog box, click **OK**.

22.7.4.2.4 Calls Tab

The **Calls** tab displays a list of the 10 most recent calls, by default, for the selected server. For details about the fields on the **Calls** tab, see Columns on the Call Tab Page.

Table 187: Columns on the Call Tab Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect sys tem
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the p hone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured

Column Name	Description
Ext/Port	The extension number at the source site associated with the endpoint inv olved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint in volved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

22.7.5 Monitoring IP Phone Status

The **Status and Maintenance** > **IP Phones** page allows you to view a list of all IP phones configured in the system, along with status information and call details for each. The page includes a list pane at the top and a details pane at the bottom.

22.7.5.1 Status and Maintenance > IP Phones List Pane

The list pane displays a list of all IP phones currently available in the system and lets you view current status information for any phone listed. The following table shows the columns in the list pane on the IP Phones page.

You can use the filtering capability to quickly find a particular phone. For details on filtering, see Filtering Information on page 20.

Table 188: Columns in the Status and Maintenance > IP Phones List Pane

Column Name	Description
Command	Allows selection of one or more phones to apply one of the following maintenance commands, which are available from the drop-down list. Not all commands can be applied to all phone types: • **Reboot:** Select this option to immediately reboot the selected phone. This operation interrupts calls. • **Download Firmware:** Select this option to download the firmware to the phone's inactive partition. This option applies to 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones. • **Update Firmware:** Manage updating firmware on the phone. **Update Phone:** Select this option to immediately update the firmware on the phone. This operation interrupts any in-progress calls. **Update Phone When Idle:** Select this option to update the firmware on the phone when the phone is idle. Calls that are active when this command is selected are allowed to finish normally. • **In/Out Service:** Manage phone service. **Put Phone in Service:** Select this option to put a phone in service **Put Out of Service:** Select this option to immediately remove a phone from service. This operation interrupts calls. **Put Out of Service When Idle:** Select this option to remove a phone from service only when the phone is idle. Calls that are active when this command is selected are allowed to finish normally. • **Troubleshooting:** Select this option to diagnose issues with the phone.
	Upload phone logs: Select this optio to upload the phone logs and crash

Column Name	Description
command check box	Allows selection of one or more phones for application of maintenance commands
status indicator	The current status of the phone: • Green indicates that the phone is in service. • Yellow indicates that the firmware version is not up to date. • Red indicates that the phone is not in service.
Name	The configured name of the IP phone. By default, this is the MAC address of the phone.
Site	The name of the site where the phone resides
Switch	The name of the switch that manages the phone
User	The name of the user who is assigned to the phone
Ext	The extension assigned to the phone
Model	The phone model
IP	The IP address of the phone

Column Name	Description
Firmware Status	The current firmware status of the phone: • **Up to Date** indicates that the phone's current firmware version is greater than or equal to the minimum firmware version required for the phone. • **Update Available** indicates that the phone is running an acceptable firmware version, but a more recent firmware version is available for download. In other words, the phone is running a firmware version above or equal to the minimum version, but less than the recommended version. • **Firmware Version Mismatch** indicates that the phone's current firmware version is less than the minimum firmware version required for the phone.

Column Name	Description
Firmware Status (continued)	• **PBX Mismatch** indicates that the current PBX version is not compatible with the phone's current firmware version. • **Download Pending** indicates that all download resources are busy and the phone is waiting for a resource to become available before initiating the download. • **Download In Progress** indicates that a firmware download is currently in progress on the phone. • **Download Ready** indicates that a firmware download on the phone was successful. • **Download Failed** indicates that a firmware download on the phone failed. • **Update In Progress** indicates that an update is in progress. • **Reboot Failed** indicates that the reboot of the phone was not successful. • **Unknown** indicates that the phone firmware status cannot be determined. This could be because the phone cannot be reached over the network or the switch the phone is assigned to is disconnected from the server.
Service	The current service status for the phone. Possible values are: • **In Service**—The phone is registered with the system and functioning properly. • **Out Of Service (Operational)**—The phone is not registered with the system and is in an "out of service" state.

Column Name	Description
Usage	The current usage state for the phone. Possible values are: • **Idle**—The phone is not off-hook or in use. • **In Service**—The phone is ready for service. • **In Use**—The phone has an active call. • **Off-Hook**—The phone is off-hook. • **Unknown**—The usage state is unknown, perhaps because communication between the server and the switch has been lost.
Active Build	The firmware version that the phone is currently running
Staged Build	The firmware version that has been successfully staged to the alternate partition (applies only to IP400-Series phones)
MAC	The MAC address of the phone
RAST	Indicates whether or not the phone is connected to the MiVoice Connect phone system using RAST. • **True** - the phone is connected using RAST • **False** - the phone is not connected using RAST
Download Status	Indicates the download status of the requested firmware version.
Button Box	The number of button boxes attached to the phone

Column Name	Description
Hardware Version	The hardware version of the phone

22.7.5.2 Status and Maintenance > IP Phones Details Pane

The **Details** pane provides more information about the selected phone. The **Details** pane includes **Button Box Information**, **Calls**, and **Events** tabs that provide details about any attached button boxes, calls for the phone, and events relevant to the phone.

22.7.5.2.1 Button Box Information Tab

The **Button Box Information** tab provides the following details about any BB424 button boxes and M695 Programmable Key Module (PKM) attached to the IP phone selected in the list pane The fields displayed on the Button Box Information tab are described in the following table.

Table 189: Columns on the Status and Maintenance > IP Phones Details Pane (Button Box Information Tab)

Column Name	Description
Button Box MAC Address	The MAC address of the BB424 device. **Note**: This field is blank for M695 PKM.
Button Box Model	The model number of the button box.
Button Box Hardware Revision	The hardware revision level of the button box.
Button Box Firmware Revision	The firmware revision level of the button box.

22.7.5.2.2 Calls Tab

The **Calls** tab provides a detailed view of call information for the selected IP phone. The phone extension and user name are displayed in either the Source or Destination endpoint column. For details about the fields on the **Calls** tab, see Columns on the Call Tab Page.

Table 190: Columns on the Call Tab Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect sys tem
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the p hone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured
Ext/Port	The extension number at the source site associated with the endpoint inv olved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint in volved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

22.7.5.2.3 Events Tab

The **Events** tab provides a list of events relevant to the phone. The fields displayed on the **Events** tab are described in the following table.

Table 191: Columns on the Status and Maintenance > IP Phones Details Pane (Events Tab)

Column Name	Description
Severity	One of the following severity levels: • Error (Red) • Warning (Yellow) • Informational
Events	The event text
Time Created	The time the event was reported.

22.7.5.2.4 Overrides Tab

The **Overrides** tab allows you to view and change current automatic phone firmware upgrade settings for the selected phone. The displayed values are derived from the parameters specified on the **Overrides** tab of the **Phone Download Settings** page, but you can modify them. The following table describes the parameters you can set for this feature.

Table 192: Table 181: Fields on the Status and Maintenance > IP Phones Details Pane (Overrides Tab)

Field Name	Description
Override	Use the drop-down list to enable or disable the phone firmware version override option.
Phone Model	The phone model of the selected phone
Hardware Version	The hardware version of the selected phone
MAC Address	The MAC address of the selected phone
Firmware Version	Select the desired firmware version from the drop-down list.

Field Name	Description
Use recommended	Enable this option if you want to use the recommended phone firmware version.

22.7.6 Monitoring Trunk Group Status

The **Status and Maintenance** > **Trunk Groups** page allows you to view a list of all trunk groups configured in the system, along with status information, performance information, and call details for each. The page includes a list pane at the top and a details pane at the bottom.

22.7.6.1 Status and Maintenance > Trunk Groups List Pane

The **List** pane displays a list of all trunk groups configured in the system and allows you to view current status information for any trunk group listed. The following table shows the columns in the list pane on the **Trunk Groups** page.

Table 193: Columns in the Status and Maintenance > Trunk Groups List Pane

Column Name	Description
status indicator	Indicates the status of the trunk group based on the percentage of In Service trunks divided by the ports within the trunk group: • Green indicates that the ratio of In Service trunks to Configured trunks is greater than 50 percent. • Yellow indicates that the ratio of In Service trunks to Configured trunks is between 20 and 50 percent. • Red indicates that the ratio of In Service trunks to Configured trunks is 20 percent or less. • Blank indicates that no trunks are configured for this trunk group.
Name	The name of the trunk group
Type	The type of trunk group

Column Name	Description
Site	The name of the site in which the trunk group is configured
Trunks In Use	The first number represents the number of trunks/ports that are currently in use, and the second number represents the total number of configured trunks.
Trunks In Service	The first number represents the number of trunks/ports that are in service, and the second number represents the total number of configured trunks.

22.7.6.2 Status and Maintenance > Trunk Groups Details Pane

The **Details** pane provides more status information about the selected trunk group. The **Details** pane includes **Status**, **Performance**, and **Calls** tabs that provide real time status details for the trunks/ports in the trunk group, trending information, and recent calls for the trunk group.

22.7.6.2.1 Status Tab

The **Status** tab displays detailed information about the trunk group selected in the list pane. The fields displayed on the **Status** tab are described in the following table.

Table 194: Columns on the Status and Maintenance > Trunk Groups Details Pane (Status Tab)

Column Name	Description
command check box	Allows selection of one or more trunks to which to apply maintenance commands (Reset, Put in service, Put out of service, Put out of service when idle), as specified in the Command field at the top of the pane
status indicator	The service status for the trunk/port: • Green indicates that the trunk/port is in service. • Red indicates that the trunk/port is out of service.

Column Name	Description
Name	The configured name for the port
Type	The trunk group type
Site	The name of the site where the trunk group is configured
Switch	The name of the switch on which the port is configured
Port/Channel	The port number on the switch for the trunk group
Usage	The current usage state of the trunks. Possible values are: • Idle • Normal
Service	The current service state of the trunk group. Possible values are: • In Service • Out of Service • Unknown

22.7.6.2.2 Performance Tab

The **Performance** tab includes the following charts:

- The Trunks Occupancy chart shows how many trunks out of the total configured trunks were used on average (and at the peak) for each point within the selected time interval. The information this chart provides can be helpful in planning for trunk allocation.
- The Call Volume chart shows call volume, including the number of good calls, the number of bad calls, and the intersite calls for the selected trunk group.

22.7.6.2.3 Calls Tab

The **Calls** tab on the **Trunk Group Details** pane lists the 10 most recent calls, by default, for the selected trunk group. For all calls, the selected trunk group appears in either the Source or Destination User/TG column.

For details about the fields on the Calls tab, see Columns on the Call Tab Page.

Table 195: Columns on the Call Tab Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect sys tem
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the p hone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured
Ext/Port	The extension number at the source site associated with the endpoint inv olved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint in volved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

22.7.7 Monitoring Voice Mail Status

The **Status and Maintenance** > **Voice Mail** page provides status and call history information for voice mail servers and voice mailboxes configured in the MiVoice Connect system.

22.7.7.1 List Pane

The **List** pane displays a list of all voice mail servers configured in the system and lets you view current status information for any voice mail server listed. The following table shows the columns in the list pane on the **Voice Mail** page.

Table 196: Columns in the Status and Maintenance > Voice Mail List Pane

Column Name	Description
status indicator	Shows the status of the voice mail server: • Green indicates that the server is operating normally. • Yellow indicates that the server is impaired but still functioning. • Red indicates that the server is in an error state. **Note**: After you add a voice mail appliance for the first time, its status will appear in red indicating an error. To change the status, you must configure at least one mailbox on that appliance.
Voice Mail Server	The name of the voice mail server
IP Address	The IP address assigned to the voice mail server
Site	The name of the site where the voice mail server resides
Mailboxes	The number of voice mailboxes on the server.
Messages	The total number of messages stored in the voice mailboxes on the server
Space Used (MB)	The disk space used for voice messages, user name recordings, auto-attendant prompts, logs, and other data
Free Space (MB)	The amount of disk space available on the server: • Green indicates more than 50% free space. • Yellow indicates 25–50% free space. • Red indicates less than 25% free space.

Column Name	Description
Last Successful Backup	The time stamp for the most recent time the data on the voice mail server was backed up

22.7.7.2 Status and Maintenance > Voice Mail Details Pane

The **Details** pane provides more status information about the selected voice mail server. The **Details** pane includes **Performance** and **Calls** tabs that provide real time status details for the voice mail server.

22.7.7.2.1 Performance Tab

The **Performance** tab provides details for the selected voice mail server, including mailboxes and disk usage.

The Mailboxes Summary area shows the number of mailboxes and the number of messages on the selected server.

The Disk Summary area shows the free space and the total space as well as the space used for the following components:

- users
- recorded names
- auto-attendant prompts
- music-on-hold files
- logs and other data

The **Details** section on the **Performance** tab provides information about all the mailboxes assigned on the selected voice mail server. The fields are described in the following table .

Table 197: Columns in the Status and Maintenance > Voice Mail Servers Details Pane (Performance Tab)

Column Name	Description
status indicator	Shows the status of the voice mailbox: • Blank indicates that voice mailbox is within acceptable limits. • Yellow indicates that the voice mailbox is reaching capacity. • Red indicates that the voice mailbox is full.

Column Name	Description
First Name	The first name of the voice mailbox owner.
Last Name	The last name of the voice mailbox owner
Mailbox	The extension of the mailbox
User Group	The user group to which the mailbox owner is assigned
Number of Messages	
Total	The number of messages in the mailbox
Unheard	The number of messages that are marked as unheard
Deleted	The number of messages that have been deleted
Allowed	The capacity of the mailbox
Saved/Unheard (Days)	
Oldest	The age, in days, of the oldest message that is marked unheard.
Allowed	The age, in days, when messages marked as unheard are removed from the server
Heard (Days)	
Oldest	The age, in days, of the oldest message that is marked heard
Allowed	The age, in days, when messages marked as heard are removed from the server

Column Name	Description
Space Used (KB)	The disk space required to store contents of the specified mailbox. This includes space required for messages that are deleted but not purged.

22.7.7.2.2 Calls Tab

The **Calls** tab displays a list of voice mail calls associated with the selected voice mail server. For details about the columns on the Calls tab, see Columns on the Call Tab Page.

Table 198: Columns on the Call Tab Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect sys tem
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the p hone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured
Ext/Port	The extension number at the source site associated with the endpoint inv olved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint in volved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

22.7.8 Monitoring Make Me Conferencing Status

The **Status and Maintenance** > **Make Me Conferencing** page provides a list of switches focused only on the conferencing-related statistics. The details pane on this page provides a list of conference calls placed on the selected switch.

22.7.8.1 Status and Maintenance > Make Me Conferencing List Pane

The **Make Me Conferencing List** pane includes the columns shown in the following table.

Table 199: Make Me Conferencing List Pane

Column Name	Description
Switch	The name of the switch
Site	The site where the switch resides
Type	The type of the switch
IP Address	The IP address of the switch
In Use	
Active Calls	The number of currently active calls
Ports	The number of ports currently in use
Free	
Ports	The number of configured ports that are currently available
Percent	Ratio of free conference ports to total conference ports as a percentage

22.7.8.2 Status and Maintenance > Make Me Conferencing Details Pane

The **Make Me Conferencing Details** pane includes a **Calls** tab that displays a list of conference calls associated with the selected switch. For details about the columns on the **Calls** tab, see Columns on the Call Quality Page.

22.7.9 Monitoring Audio/Web Conferencing Status

The **Status and Maintenance** > **Audio/Web Conferencing** page provides a list of Mitel service appliances and related statistics.

22.7.9.1 Status and Maintenance > Audio/Web Conferencing List Pane

The **Audio/Web Conferencing List** pane provides a list of service appliances and usage details that are helpful for capacity monitoring and planning. The following table describes the columns included in the **Audio/Web Conferencing List** pane.

Table 200: Columns in the Audio/Web Conference List Pane

Column Name	Description
status indicator	Shows the status of the service appliance: • Green indicates that the service appliance is in service and connected. • Yellow indicates a problem (a warning state) in the service appliance that does not affect the service appliance's status. • Red indicates that the service appliance is down or experiencing a severe service impact.
Name	The name of the service appliance
Site	The name of the site where the service appliance resides
Audio Ports	
Peak	The peak number of audio ports used during the last 24 hours
Current	The number of audio ports currently in use
Web Ports	

Column Name	Description
Peak	The peak number of web ports used during the last 24 hours
Current	The number of web ports currently in use
Disk Used (GB)	
Used	Total disk space currently in use
Capacity	Total disk space available on the service appliance
Conferences	
Total	The number of registered conferences
Active	The number of conferences currently in progress
Requests per Hour	The number of conference requests made per hour
Last Successful Backup	The timestamp of the last backup of the service appliance database

22.7.9.2 Status and Maintenance > Audio/Web Conferencing Details Pane

The **Details** pane includes a **Calls** tab that provides a list of audio and web conferences placed on the selected service appliance. For details about the columns on the **Calls** tab, see Columns on the Call Quality Page.

22.7.10 Monitoring IM Status

The **Status and Maintenance** > **IM** page provides a list of service appliances that support an IM service instance and some related statistics for that instance.

22.7.10.1 Status and Maintenance > IM List Pane

The **IM List** pane includes the columns described in the following table.

Table 201: Columns in the Status and Maintenance > IM Page's List Pane

Column Name	Description
check box	Allows selection of one or more service appliances for stopping and starting the appliance
status indicator	Shows the status of the service appliance: • Green indicates that the service appliance is in service and connected. • Yellow indicates a problem (a warning state) in the service appliance that does not affect the service appliance's status. • Red indicates that the service appliance is down or experiencing a severe service impact.
Name	The name of the service appliance that is providing IM services
Site	The site where the service appliance is installed
Users	
Total	The total number of users registered on the site
Active	The number of users who are currently logged in to IM on the service appliance
Sessions	
Peak	The peak number of IM sessions during the last 24 hours
Current	The number of current active sessions

22.8 Monitoring Alerts

Alerts provide a mechanism for notifying you of possible issues within the MiVoice Connect system. The alerts can identify issues at a variety of levels, such as in the overall system, within a site, or in an individual component such as a switch.

The Alerts tool accessible in the Maintenance menu includes the following types of alerts:

- Event Correlation Alerts

  Many MiVoice Connect system components use the Windows Event Log to report status updates, inconsistencies, misbehavior, and critical system issues. The Monitoring Service captures all events logged by these components and attempts to find any correlations involving system issues. The Monitoring Service raises the appropriate alert and attaches all associated events.
- Composite Alerts

  The Monitoring Service identifies when several common issues occur within a physical or logical range. For example, if alerts are raised for a number of problematic switches within the same site, it would create an alert for that site that references the individual alerts as the cause.
- Threshold Alerts

  The Monitoring Service analyzes metrics from call quality reports as well as periodic status reports for the system and its components and compares these metrics to thresholds that indicate when an alert is necessary. The Monitoring Service continues to monitor when these metrics fall below the threshold limits and determines when the alerts can be safely cleared.

Note:

Because a small set of events for Distributed Voice Servers are not captured in the Maintenance component of Connect Director, some alerts are missing or get stuck. Status pages correctly reflect the current state of a local or remote server.

Table 202: Columns on the Alerts Page

Column Name	Description
Check box	Used with the **Command** drop-down list box to designate which alert records should be cleared

Column Name	Description
Severity	The severity level of the alert: • Blank—Information •  —Warning •  —Critical
Time Created	The time that the alert was generated
Last Updated	The date and time when the alert was created or cleared
Category	The category of the alert. See the *Mitel Connect Maintenance Guide* for more information.
Site	If the alert involves a switch, the name of the site where the switch resides
Switch	If the alert involves a switch, the name of the switch
Trunk Group	If the alert involves a trunk group, the name of the trunk group
State	The state of the alert. Possible values are Active or Cleared.
Description	The description of the alert

22.8.1 Clearing Alerts

You can clear an alert, which marks the alert as cleared. Cleared alerts are not deleted; they remain in the system so that they are available for investigative purposes and to provide historical perspective for troubleshooting and other analysis.

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Alerts**. The **Alerts** page is displayed.
3. In the **Command** drop-down list, select **Clear**.

4. In the **List** pane at the top, select the check box for the alert you want to clear.
5. Click **Apply**.
6. In the confirmation dialog, click **OK**.

22.9 Monitoring Call Quality

The **Call Quality** page enables easy troubleshooting of problems related to call and network quality by providing access to records of every media stream that occurs in the MiVoice Connect system. The call quality metrics are derived from monitoring IP network impairments such as packet loss and delay.

22.9.1 Aspects of Call Quality

Call Quality is evaluated based on thresholds for packet loss, delay/latency, and jitter.

22.9.1.1 Packet Loss

Packet loss refers to the percentage of media packets lost over the duration of a media session. You can view the following metrics related to packet loss in the **Maintenance** menu in Connect Director:

- Average packet loss, which is the ratio of lost packets to total packets over the entire call
- Maximum packet loss, which is the highest ratio of lost packets measured in any 10-second interval

Calculation of packet loss is performed per RFC 3550 using RTP header sequence numbers.

The causes of packet loss include queue drops, corrupted packets dropped in transit, and jitter buffer drops due to late arrival.

22.9.1.2 Delay/Latency

Delay or latency refers to the amount of time it takes for speech to exit the speaker’s mouth and reach the listener’s ear. Latency sounds like an echo or a two-way radio.

The causes of delay or latency include network congestion, route flapping, extremely long routes between endpoints, and satellite hops.

22.9.1.3 Jitter

Jitter, also known as Per Packet Delay Variation (PPDV), is the measure of the variability over time of the latency across a network. VoIP endpoints require media packets to be received in a steady stream at a consistent rate, or audio quality quickly degrades, which users hear as clicks or pops.

Applications that run on standard operating systems could inject jitter from the sending or receiving side due to process scheduling delays (timing drift). Network congestion can also cause jitter.

To address problems with jitter, use a dynamic jitter buffer and configure Quality of Service settings to reduce the impact of network congestion.

22.9.2 Call Quality Page

The **Call Quality** page has two panes:

- The **List** pane at the top provides a list of call streams (the media stream from the source to the destination endpoint).
- The **Details** pane at the bottom has multiple tabs that show metrics and configuration data for both media streams involved in the call, along with both path traces.

Note:

The **Call Quality** page does not automatically refresh, but you can refresh the page by clicking the **Refresh** option.

22.9.2.1 Call Quality List Pane

The **Call Quality List** pane includes the columns described in the following table .

Table 203: Columns on the Call Quality Page

Column Name	Description
Call Quality Indicator	A green, yellow, or red bubble that represents the voice quality for the media stream. This rating includes MOS and jitter.

Column Name	Description
Call ID	A unique identifier for the call that is assigned by the MiVoice Connect system
Start Time	The time that the media stream originated
End Time	The time that the media stream ended
Dest Site	The name of the destination site
Switch	For a phone, the name of the switch at the destination site with which the phone is registered. For a trunk, the name of the switch at the source site on which the trunk is configured
Ext/Port	The extension number at the source site associated with the endpoint involved in the call
User/TG	The name of the user or trunk group at the source site that is involved in the call.
Source Site	The name of the destination site with which the endpoint is associated
Switch	For a phone, the name of the switch at the source site with which the phone is registered. For a trunk, the name of the switch at the destination site on which the trunk is configured.
Ext/Port	The extension number at the destination site associated with the endpoint involved in the call
User/TG	The name of the user or trunk group at the destination site that is involved in the call.

Note:

For calls longer than 60 minutes, statistics are collected for only the most recent 60 minutes of the call.

22.9.2.2 Call Quality Details Pane

The **Call Quality Details** pane includes the **Details** tab and the **IP Path Trace** tab. The information provided is from the perspective of the receiver of each stream in the two-way path.

Note:

The **Details** pane does not show all media streams involved in conference calls that include multiple parties.

22.9.2.2.1 Details Tab

The information on the **Details** tab is displayed in separate columns for Endpoint A and Endpoint B. The rows in the table provide the collected values for the configuration and metric information from the individual media stream record. The values displayed are described in the following table.

Table 204: Fields on the Call Quality Details Tab

Field Name	Description
User/TG	The name of the user or trunk group
Ext/Port	The system extension or port for the endpoint, if known
Site	The name of the site at which the endpoint is configured
Switch	The name of the switch with which this endpoint is registered,

Field Name	Description
IP Address	The IP address of the phone or switch
MAC Address	The MAC address of the phone **Note**: If there is no MAC address provided for a given call detail, then this field is populated with **NA**.
Start Time	The start time for the stream
End Time	The end time for the stream
Codec	The audio codec and sample rate used in the stream If more than one codec is used for a call, only the last codec used for the call is displayed.
MOS	The stream's MOS, which the Monitoring Service calculates based on the IP metrics according to ITU-T G.107
Loss (max/avg,%)	The average and maximum packet loss percentage
Jitter (max/avg, ms)	The inter-arrival jitter, maximum and average, measured for the stream in microseconds
Delay (max/avg, ms)	The maximum and average round-trip delay in microseconds

22.9.2.2.2 IP Path Trace Tab

The **IP Path Trace** tab provides a graphical representation of the paths (“hops”) between the two endpoints in the selected call stream. The nodes show the IP addresses traversed in the path and the maximum delay in microseconds at each node.

22.9.2.3 Viewing High-Level Call Quality

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Call Quality**.

The **Call Quality** page launches, displaying the following information:

- The 10 most recent stream records, sorted by End Time.
- On the **Details** tab, details for the most recent media stream.

22.9.2.4 Viewing Call Quality Details for a Particular Call

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Call Quality**. The **Call Quality** page launches.
3. To select a particular media stream, click on a row in the list pane at the top of the page.
4. Choose one of the following:
   - To see metrics for the selected media stream, review the details on the **Details** tab.
   - To see the IP path for the selected media stream, click the **IP Path Trace** tab.

The path from A to B and B to A is displayed.

22.9.2.5 Finding All Recent Calls for a Site

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Call Quality**. The **Call Quality** page launches.
3. Click  on the bottom left corner of the **Call Quality List** pane.

Note:
Text boxes are added under each column heading in the Call Quality list pane.

4. Click in the text box under the **Source Site** column heading, and enter the site name for which you want to find all recent calls.
5. Click → to apply the filter.

The list is filtered to include only streams where the source site matches the site name that you entered in the text box.

22.9.2.6 Finding Calls for a Particular User and Time Range

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Call Quality**. The **Call Quality** page launches.
3. Click ⌕ on the bottom left corner of the **Call Quality List** pane.

   Text boxes are added under each column heading in the **Call Quality List** pane so that you can enter a filter.
4. Click in the text box under the User/TG column heading in the Source area, and enter the user name for which you want to find all recent calls.
5. Click in the text box under the **Start Time** column heading, and select a date from the calendar and a time (hour and minute), and click **Done**.
6. Click → to apply the filter.

The list is filtered to include only streams where the source endpoint user matches the entered user and that started during the specified time range.

22.9.2.7 Sorting Calls Using the Call Quality Indicator

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Call Quality**. The **Call Quality** page launches.
3. Click ⇕ in the column heading for the call quality status indicator.

The list is sorted from worst call quality to best call quality.

22.10 Viewing Events in the System

The **Events** page lists each event recorded in the system. Fields on the Events page are described in the following table.

Table 205: Columns on the Events Page

Column	Description
Time Created	The time the event was reported
Log Name	One of the following log names, where messages are recorded: • Application • System
Event ID	The event identifier number.
Server	The name of the server for which the event was reported.
Source	The system
Task Category	The category of the event
Severity	One of the following values: • Error. Errors require your immediate attention. • Warning. Warnings alert you to potential errors. • Informational. Informational messages provide the status of a service, switch, or port.
Description	Details about the event.

22.11 Using Event Filters

Event filters specify the criteria that trigger the MiVoice Connect system to send email notifications after an event has been reported. The **Event Filters List** page displays a list of the event filters that you have created. Details are provided in the following table.

Table 206: Event Filters Page: List Pane

Column	Description
Source	One of the following values: • **ShoreWare** indicates that the filter includes Mitel events. • **Services** indicates that the filter includes non-Mitel services. • **Other** indicates an event source other than a Mitel event or a non-Mitel service.
Category	The specific category of event based on the source of the event.
Event ID	A particular event ID number or **Any** if any event ID is included in the filter.
Type	One of the following event types: • **All** event levels. • **Error** indicates only Error-level events. • **Warning** indicates only Warning-level events. • **Information** indicates only Information-level events.
Server	The server the event filter applies to.
Email	The email address of the system administrator or technical support specialist who should receive email messages about events in the MiVoice Connect system.

22.11.1 Creating and Editing Event Filters

1. Launch Connect Director.
2. In the navigation pane, click **Maintenance** > **Event Filters**. The **Event Filters** page is displayed.
3. Do one of the following:
   - To create a new filter, click **New**.
   - To edit an existing filter, click the filter's name in the **Event Filters** list.
4. Edit or specify values for the parameters as described in The table below.
5. To save the event filter, click **Save**.

Table 207: Event Notification Edit Pane

Parameter	Description
Server	From the drop-down list, select the server the filter should run on.
Source	Select one of the following: • To filter for Mitel events, select **ShoreWare** and choose a source from the drop-down list. Selecting Any includes events for all Mitel categories. • To filter for any non-Mitel service, select **Services** and choose a source from the drop-down list. • To filter for a different source, select **Other** and type the source name.
Category	To enter a category name, select the first radio button and type the category name in the data-entry field. Otherwise, select **Any**.
Event ID	To specify a particular event ID in the filter, select the first radio button and specify the event ID in the data-entry field. To include any event ID that matches the criteria of the filter, select **Any**.
Type	Select the type of event to include in the event filter.

Parameter	Description
Email	Specify the email address of the system administrator or support specialist who should be notified when events matching the criteria in the filter are generated.

22.12 Monitoring Hybrid Services Status

Detailed information about MiVoice Connect HYBRID services is provided in articles on the Mitel Support website. Search for **HYBRID** to locate these articles.

22.13 Diagnosing Switch or Phone Problems through RPC

Through the Remote Packet Capture (RPC) tool, the MiVoice Connect system provides the capability to capture network protocol information for certain switches and phones. The packet trace information is captured in .pcap format, which can be viewed with Wireshark or another network protocol analysis tool. Typically, you would need to capture network protocol information only when Mitel Technical Support directs you to do so for problem diagnosis.

The following limitations apply for remote packet capture operations:

- Only the switches and phones on which remote packet capture is supported are listed on the Remote Packet Capture page.
- A switch or phone can be part of only one capture session at a time.
- You can capture packet information for up to 25 devices simultaneously. If you select more than 25 devices when you initiate a capture operation, the system notifies you that some capture operations will not begin immediately. If you proceed, some of the capture operations are put into a pending state.
- The maximum size of a capture file is 70 MB. When the maximum file size is reached, the capture session stops.
- The total maximum disk usage allowed for capture files is 4 GB. If this limit is reached, the system notifies you to delete capture files to clear space before you can initiate more capture sessions.
- A capture session can run for a maximum of 120 minutes. The capture operation stops running when it reaches this limit.

Note:

- If the network on which you are running a packet capture has high resource usage or environmental issues, then when you run a packet capture, connected phones might go out of service because of switches resetting. If this issue occurs, rather than using the Remote Packet Capture tool in Connect Director, capture packets through a port mirror on the data switch to the switch.
- In Connect Director, remote packet capture for 6900-Series phones fails. To fix this issue, you must collect the remote packet capture data from the phone and upload it to the respective server.
- The remote packet capture upload from Teleworker phone to HQ server through FTP or HTTPS does not work. To fix this issue, you must upload the pcap to the local FTP/TFTP server.

22.13.1 Remote Packet Capture List Pane

The **Remote Packet Capture** list pane provides a list of phones and switches for which you can run a remote packet capture. The following table describes the information displayed in the **Remote Packet Capture List** pane.

Table 208: Columns on the Remote Packet Capture List Pane

Column Name	Description
check box	Allows selection of one or more phones or switches to start or stop the packet capture operation.
Device Type	The type of device (phones or switches).
IP Address	The IP address of the switch or phone
MAC Address	The MAC address of the switch or phone
Device Name	The name of the device or the MAC address of the phone
Submitted By User	The name of the user who submitted the packet capture command

Column Name	Description
Last Logged Start Date	The starting date and time of the most recent capture process for this component
Protocols	The protocols selected when the packet capture process was initiated. The following protocols are included for switches: • BWMGR*—Bandwidth Manager Protocol • DRS*—Distributed Routing Service • LSP*—Location Service Protocol • NCC*—Network Call Control • ISDN (PRI/BRI)—Integrated Services Digital Network • SIP + TLS—Session Initiation Protocol with Transport Layer Security • SHORESIP*—Mitel's version of Session Initiation Protocol • MGCP—Media Gateway Control Protocol The following protocols are included for phones: • CAS* + TLS—Client Application Server with Transport Layer Security • SM* + TLS—Session Manager with Transport Layer Security • SIP + TLS—Session Initiation Protocol with Transport Layer Security • ARP—Address Resolution Protocol • RARP—Reverse Address Resolution Protocol • DNS—Domain Name Server • ICMP—Internet Control Message Protocol • RTP/SRTP/RTCP—Real-time Transport Protocol, Secure Real-Time Protocol, Real Time Conferencing Protocol When you run a capture against switches and phones, the protocols are limited to the protocols common to both types of devices. *Mitel proprietary protocol

Column Name	Description
Bytes Written	The number of bytes captured
Duration	The configured duration of the packet capture operation in minutes
Logging Status	The status of the packet capture operation. Possible values are: • No capture is running • Request Pending: This status displays very briefly after the command has been applied. • Session Processing: This status displays briefly as the capture service establishes a channel with the targeted phone or switch. • Session Running: This status displays while packets are captured and transferred. • Client Failed • Complete **Note**: You cannot stop a capture session when the Logging Status is “Session Processing.” You must wait and stop the capture session when the status is “Session Running.” To force a status update, click **Refresh**.

22.13.2 Starting Remote Packet Capture

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Remote Packet Capture**.

Note:

The **Remote Packet Capture** page launches, showing the list of eligible switches and phones in the top pane.

3. Optionally, to filter the list of phones and switches, do the following:

   a. Click  .

   Note:

   The filter list boxes are displayed under column headings.

   b. Enter text in one or more filter text boxes for the columns you want to use as a filter.

   c. Click  .

   Note:

   A subset of the list matching your filter is displayed.

4. To designate the phones and/or switches for which you want to capture packets, select the check box for one or more phones or switches.
5. In the **Command** drop-down list, select **Start** and then click **Apply**.

Note:

- A dialog box that allows you to choose settings for the log capture is displayed.
- If you select both switches and phones, the list of protocols that you can specify is limited to protocols common to switches and phones.

6. Enter the number of minutes in the **Capture Duration** field.
7. If you want to capture only SIP + TLS and SHORESIP protocols on one or more switches for an indefinite period of time, select the **Ignore the duration for the SIP and SHORESIP protocols for switches** check box. In this case, the value entered in

the **Capture Duration** field is ignored and the capture runs until one of the following events occurs:

- You stop the capture.
- The Headquarters server is rebooted.
- The switch is rebooted.

8. Do one of the following:

   - To capture log information for all protocols listed, select the **Capture every protocol** check box.
   - To select specific protocols, clear the **Capture every protocol** check box and select the check boxes for the protocols you want to capture.

9. To submit the packet capture request, click **Save**.

Note:

A message notifying you that the capture request was submitted successfully is displayed.

10. Click **OK**. The packet capture begins.

22.13.3 Stopping Remote Packet Capture

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Remote Packet Capture**. The **Remote Packet Capture** page launches. The **List** pane at the top lists switches and IP phones.
3. Optionally, to filter the list of phones and switches, do the following:

   a. Click  .

Note:
The filter text boxes are displayed under the column headings in the **List** pane.

   b. Enter text in one or more filter text boxes for the columns you want to use as a filter.

Note:
To filter for capture sessions that are currently running, enter **Session Running** in the text box under the **Logging Status** column heading.

c. Click → .

Note:
A subset of the list matching your filter is displayed.

4. To designate the phones or switches for which you want to stop capturing packets, select the check box for one or more switches or phones in the list.
5. In the **Command** drop-down list, select **Stop** and then click **Apply**. A confirmation dialog box is displayed.
6. Click **OK**.

22.13.4 Viewing Remote Packet Capture Log Files

You can view a list of remote packet capture log files (.pcap files) in the **All Previous Log Files** > **Captured Phone Logs** and the **All Previous Log Files** > **Captured Switch Logs** pane at the bottom of the **Remote Packet Capture** page. The columns in the **Captured Phone Logs** and the **Captured Switch Logs** pane are described in Columns in the All Previous Log Files > Captured Phone Logs pane and Columns in the All Previous Log Files > Captured Switch Logs pane respectively.

Table 209: Columns in the All Previous Log Files > Captured Phone Logs pane

Column Name	Description
Check box	Allows you to select one or more log files to which to apply commands.
Device Type	The type of phone device.
IP Address	The IP address of the phone device.
MAC Address	The MAC address of the phone device.

Column Name	Description
Device Name	The name of the phone device.
Submitted By User	The name of the user who submitted the capture request.
Last Logged Start Date	The date and time that the capture process started.
Protocols	The names of the protocols selected for the capture process.
Bytes Written	The number of bytes in the capture log.
File	The name of the log file generated in the capture session.

Table 210: Columns in the All Previous Log Files > Captured Switch Logs pane

Column Name	Description
Check box	Allows you to select one or more log files to which to apply commands.
Device Type	The type of switch device.
IP Address	The IP address of the switch device.
MAC Address	The MAC address of the switch device.
Device Name	The name of the switch device.
Submitted By User	The name of the user who submitted the capture request.
Last Logged Start Date	The date and time that the capture process started.

Column Name	Description
Protocols	The names of the protocols selected for the capture process.
Bytes Written	The number of bytes in the capture log.
File	The name of the log file generated in the capture session.

To open a capture file:

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Remote Packet Capture**.The **Remote Packet Capture** page opens.
3. In the **All Previous Log Files** > **Captured Phone Logs** and the **All Previous Log Files** > **Captured Switch Logs** pane, which shows the list of available capture files, locate the capture session whose log file you want to view.
4. Open a log file using one of the following methods:

   - In the **File** column, click the log file you want to open.
   - In the **File** column, right-click the log file you want to open and select **Open** or another option from the pop-up menu.

Note:
This step assumes that you have a network protocol analysis tool (such as Wireshark) installed that allows you to open .pcap files.

5. Review the capture log file.
6. Save the file in a new destination if desired.

22.13.5 Deleting Remote Packet Capture Log Files

To delete the remote capture log files:

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Remote Packet Capture**. The **Remote Packet Capture** page opens.

3. In the **All Previous Log Files** > **Captured Phone Logs** or the **All Previous Log Files** > **Captured Switch Logs** pane, which shows the list of available capture files, select the check box for one or more log files that you want to delete.
4. In the **Command** drop-down list, select **Delete Files** and then click **Apply**. A confirmation dialog box opens.
5. Click **OK** to delete the remote capture log files.

22.14 Testing Trunks

Through the Diagnostics and Monitoring system, you can test the trunks in your system. The Trunk Test tool allows you to monitor real-time activity on a trunk.

The **Trunk Test** page includes the trunk list pane at the top and a **Logs** tab for the selected trunk at the bottom. On this page, you can make or drop calls, view the properties of selected trunks, place trunks in service, and remove them from service. You can use the advanced filter to narrow the list of trunks to see only what you're interested in monitoring, and you can download the log messages for a selected trunk.

22.14.1 Trunk Test List Pane

The **Trunk Test List** pane provides a list of trunks in your MiVoice Connect system. The following table describes the information displayed in the **Trunk Test List** pane.

Table 211: Columns on the Trunk Test List Pane

Column Name	Description
command buttons	The following command buttons are available to perform actions against the selected trunk or trunks: • Make Call: Make a call using the selected trunk. • Drop Call: Drop the call that is currently established on the selected trunk. • Put in Service: Put the selected trunks in service. • Put Out of Service: Put the selected trunks out of service.
check box	Allows selection of one or more trunks to perform various actions such as making or dropping a call or putting a trunk in service or out of service.

Column Name	Description
Trunk	The name of the trunk
Type	The type of trunk: • Analog Loop Start • PRI • SIP
Trunk Group	The name of the trunk group
Switch	The switch on which the trunk is configured
Site	The site for which the trunk is configured
Hook	The hook status for the trunk

Column Name	Description
Trunk State	The current state of the trunk. Possible values are as follows: • Null – No status is available. • Trunk Phone Other – A state other than one listed here has been received. • On-Hook – The trunk is idle. • Trunk Phone Ringing – The far end device is ringing. • Off-Hook – The trunk has gone off-hook. Typically, the system next signals the trunk by sending dialtone to indicate the system is ready to receive digits. • Proceeding – Dialing has completed, and the call is proceeding through the switch or telephone network. This state occurs after dialing is complete and before the call reaches the dialed party, as indicated by ringback, busy, or answer. • Internal Dialtone – The call is receiving a dial tone from the switch, which means that the switch is ready to receive a dialed number. This is an internal dial tone, as within a PBX. • External Dialtone – The call is receiving a dial tone from the switch, which means that the switch is ready to receive a dialed number. This is an external (public network) dial tone. • Trunk Phone Dialing – The originator is dialing digits on the call. The dialed digits are collected by the switch. • Trunk Phone Established – A call has been established. • Trunk Phone Reorder – A special information tone that precedes a reorder announcement (equipment irregularity category) is occurring. This state is also reported when the telephone is kept off-hook too long.

Column Name	Description
Trunk State (continued)	• Trunk Phone Intercept – A tone advising the caller that the called number cannot be reached for reasons other than "subscriber busy" or "congestion" is occurring. • Trunk Phone Busy – The call is receiving a busy tone. A busy tone indicates that the call cannot be completed either because a circuit (trunk) or the remote party's station are in use. • Trunk Phone Ringback – The station to be called has been reached, and the destination's switch is generating a ring tone back to the originator. A ringback means that the destination address is being alerted to the call. • Trunk Ringback – The station to be called has been reached, and the destination's switch is generating a ring tone back to the originator. A ringback means that the destination is being alerted to the call. • Trunk Busy – The call is receiving a busy tone. A busy tone indicates that the call cannot be completed either because a circuit (trunk) or the remote party's station are in use. • Trunk Intercept – A tone advising the caller that the called number cannot be reached for reasons other than a circuit (trunk) or the remote party's station are in use. • Trunk Reorder – This special information tone precedes a reorder announcement (equipment irregularity category). Also reported when the telephone is kept off-hook too long. • Out-Of-Service – The trunk is out of service and is not able to send or receive calls.
Call State	The current state of the call
Caller ID	The caller IDs of both the originating and receiving ends of the call established on the trunk

Column Name	Description
Admin State	The administrative state of the trunk. Possible values are as follows: • Null – No status • In-Service – The trunk has been provisioned. • Out-of-Service (Operational) – The trunk is out of service; perhaps the remote destination is not reachable. • Out-of-Service (Administrative) – An administrator has taken the trunk out of service. • Not Acquired – • Out-of-Service (Busy Out) – The trunk is currently being used by a call.

22.14.2 Using the Advanced Filter

You can use the advanced filter to narrow the list of trunks by any combination of site, switch, trunk group, and trunk.

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Trunk Test**.The **Trunk Test** page is displayed.
3. Click to show the filter.
4. Click to show the advanced filter settings.

   The **Advanced Filter** is displayed.
5. Use the drop-down lists to specify the advanced filter criteria.
6. Click **Apply Filter**.

   The **List** pane shows the filtered list of trunks.
7. To clear the filter, click .

22.14.3 Making a Test Call to Monitor a Trunk

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Trunk Test**. The **Trunk Test** page is displayed.

3. In the list pane, which shows the list of trunks in the system, select the check box for the trunk you want to test.
4. Click **Make Call**. A pop-up window is displayed.
5. In the pop-up window, enter numbers in the following fields:
   - The access code (for SIP trunks)
   - The dial-from extension
   - The destination number
6. Click **Make Call**.

> **Note**:
> The call is initiated, and detailed log messages are shown in the **Logs** tab.

7. To drop the call, with the trunk still selected, click **Drop Call**.

22.14.4 Downloading Logs

You can download the trunk logs displayed in the Logs tab of the **Trunk Test** page. This allows you to save the logs before clearing them.

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Trunk Test**. The **Trunk Test** page is displayed.
3. Perform an action, such as a test call, to see the logs. or choose to capture some logs gathered previously.
4. Click **Download**. A `.txt` file that contains the log messages is generated and downloaded.

22.14.5 Clearing Logs

You can clear the trunk logs displayed in the Logs tab of the **Trunk Test** page. Clearing the logs also removes the logs from the database.

1. Launch Connect Director.
2. In the navigation menu, click **Diagnostics** > **Trunk Test**. The **Trunk Test** page is displayed.
3. In the **List** pane, which shows the list of trunks in the system, select the check box for the trunk whose logs you want to clear.
4. Click **Clear**.

Note:
The **Logs** tab for the selected trunk is cleared.

22.15 Updating Phone Firmware for 400-Series and 6900-Series IP Phones

Through the Diagnostics and Monitoring system, you can control how phone firmware for IP400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones is updated.

For example, you can automatically maintain all 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones at the recommended firmware level, or you can override the automatic updates if you want to select a different firmware version or disable automatic update for certain phone models or for specific phones.

To accomplish this, you define global settings for 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phone firmware updates and specify any overrides to the default settings.

Note:
The 400-Series and 6900-Series (6910, 6920, 6930, and 6940) IP phones use different firmware versions.

22.15.1 Specifying Global Settings for 400-Series and 6900-Series IP Phone Updates

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Configuration** > **Phone Firmware Update** > **Global Settings**.

Note:

The **Phone Firmware Update** page opens showing the global update settings.

3. Specify default settings, and optionally, specify settings that apply during the defined maintenance window.

Note:

For details about the parameters, see the table below.

4. Click **Save**.

Table 212: Phone Firmware Update Global Settings Page

Parameter	Description
Enable global automatic phone firmware update	Select this option if you want 400-Series and 6900-Series (6910, 6920, 6930, and 6940) IP phones to be automatically updated to the recommended firmware version.
Default (on-hours) settings	The configured default settings apply during on-hours or outside the maintenance window.
Simultaneous server download limit	Specify the maximum number of simultaneous downloads allowed from the server to phones.
Allow peer to peer phones update	Select this option if you want phones to have the capability to download firmware from other phones at the site. When a group of phones at a site is selected for firmware download and the server is remote, to minimize bandwidth utilization some phones automatically download firmware from other phones at the site.

Parameter	Description
Use different settings during maintenance window	Select this option if you want the phone firmware updates to adhere to different settings during the specified maintenance window. These settings override the default settings only during the specified maintenance time window, based on the local time zone for each site. **Note**: The time settings to update global automatic firmware is 24-hour format.
Maintenance Window	Specify the start and stop time for the maintenance window when the modified settings for phone automatic upgrades should be in effect.
Simultaneous server download limit	Specify the maximum number of simultaneous downloads allowed from the server to phones during the maintenance window.
Allow peer to peer phones update	Select this option if during the maintenance window you want phones to have the capability to download firmware from other phones at the site. When a group of phones at a site is selected for firmware download and the server is remote, to minimize bandwidth utilization some phones automatically download firmware from other phones at the site.

Parameter	Description
Use legacy protocol	Select this option only if the phones fail to update because they are running an outdated build. This option specifies to use SSH (the legacy protocol) rather than SIP to send commands to phones.
Recommended Firmware Versions	Lists the currently recommended firmware versions for the 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phone models.

22.15.2 Creating or Editing Overrides to the Phone Firmware Update Settings

You can create an override for a phone model or for a specific phone on the **Phone Firmware Update** page. If you want to create an override for a specific phone, you can also specify the override parameters by selecting the phone on the **Overrides** tab of the **Status and Maintenance** > **IP Phones** page.

Note:
Overrides is applicable to 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phones only.

To create an override on the **Phone Firmware Update** page:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Configuration** > **Phone Firmware Update** > **Overrides**.

Note:
The **Phone Firmware Update** page showing override settings is displayed. For details about the parameters on the details pane, see Phone Firmware Update Overrides Page.

3. Do one of the following:
   - To edit the details for an existing override, click the name of the override in the list pane and edit the parameters in the **Details** pane.
   - To create a new override definition, click **New** and specify the parameters in the **Details** pane.
4. Click **Save**.

To create an override for a specific phone:

1. Launch Connect Director.
2. In the navigation menu, click **Maintenance** > **Status and Maintenance** > **IP Phones**. The **IP Phones Status** page is displayed.
3. In the list pane, click the name of the 400-Series and 6900-Series (6910, 6920, 6930, and 6940) phone for which you want to define a firmware update override.

> **Note**:
> The details for that phone are displayed in the **Details** pane.

4. Click the **Overrides** tab.
5. On the **Overrides** tab, specify the parameters for the override.

> **Note**:
>
> For details about the override parameters, see the table below

6. Click **Save**.

Table 213: Phone Firmware Update Overrides Page

Parameter	Description
Override	Specify the override action from the following options: • **Disable Automatic Update:** Phone firmware upgrades will not happen automatically for any phone that has this override. Upgrades for these phones can be triggered only by selecting a command on the Status > IP Phones page. • **Override Firmware Version:** Select this override if you want to specify a firmware version other than the recommended version.
Phone Model	Select the phone or group of phones that the override should apply to.
Hardware Version	Select the hardware version that the override should apply to
MAC Address	Specify the MAC address of the individual phone for which you want to disable the automatic upgrade or override the firmware version.
Firmware Version	From the drop-down list, select the firmware version that should be downloaded to the specified phone.
Use recommended	Enable this option if you want to use the recommended firmware for the specified phone.

System Backup and Restore 23

This chapter contains the following sections:

This chapter describes the procedures for backing up and restoring system files. The tools for performing these tasks are scripts and, optionally, batch files.

23.1 Overview

A system administrator can use the default scripts that we provide or use the default scripts to create new scripts. Also, the system administrator can back up and restore all files or selected files.

When following the descriptions in this chapter, readers need to understand that two types of interfaces can apply to the topics of back up and restore. The choice of interface depends on the task that the system administrator is doing:

- To search for and modify scripts or other components, the system administrator uses Windows Explorer and, when necessary, a text editor for modifying a script.
- To initiate a backup or restore, the administrator uses the server's command prompt.

- To cache an RSA key for each Voice Switch and Service Appliance, the administrator uses the server's command prompt.

23.2 Introduction to Backup and Restore

We recommend that customers regularly back up the files on the Headquarters server, Distributed Voice servers (DVS), Voicemail Switches, and Service Appliances. Customers can use the backed-up files to restore existing devices or add the files to hardware that replaces other hardware (such as defective components). We provide scripts to back up or restore these Mitel devices. Customers can modify these scripts.

Note:
The person who runs a script must have Administrator privileges and enter a username and password when the system prompts for these credentials.

The system copies the script file to a directory on the Headquarters and DVS servers when the system administrator installs the server software.

By design, the backup and restore scripts support a server. Therefore, by default, the script backs up and restores only the server on which the script exists. However, with the correct configuration, the script can also back up and restore any voicemail switch or service appliance in the network. Furthermore, the system can use a batch file to initiate system-wide backup or restore. A Mitel installation includes default batch files in the folder that contains the backup and restore scripts. System administrators can use programs such as Microsoft Scheduler to configure automatic backups.

The following table shows the files that the system can back up.

Table 214: List of Backed-up Files

Headquarters Server	Distributed Voicemail Server	Voicemail Model Switch	Service Appliance 100 and 400
\inetpub\ftproot \Program Files (x86)\Shoreline Communications \ShoreWare Server \MySQLConfig \MySQL Server \my.ini \Program Files (x86)\Shoreline Communications \ShoreWare Server \MySQLCDR \MySQL Server \my.ini \Shoreline Data\Call Records 2 \Shoreline Data \CrashDumps \Shoreline Data \data \Shoreline Data \Database \Shoreline Data \IMAAData	/Shoreline Data /MessageFiles /Prompts /SoftSwitch /Templates /Logs /Vms	/cf cfg.dat ShoreTel.cfg	certs db_files IM Library Recordings SharedLibrary

Headquarters Server	Distributed Voicemail Server	Voicemail Model Switch	Service Appliance 100 and 400
\Shoreline Data\IMArchives \Shoreline Data\Install History \Shoreline Data\keystore \Shoreline Data\Logs \Shoreline Data\MCM \Shoreline Data\MessageFiles \Shoreline Data\Prompts \Shoreline Data\Scripts \Shoreline Data\SoftSwitch \Shoreline Data\Temp \Shoreline Data\Templates \ShorelineData\UserData \Shoreline Data\Vms \Shoreline Data\wss			

23.2.1 Estimated Backup and Restore Times

The duration of a backup or restore operation depends on many factors. For example, the amount of information to back up or restore, the configuration, and the environment

affect the duration. This section provides approximate durations for backing up or restoring different parts in the MiVoice Connect system.

The following two system loads illustrate approximate times for a Mitel backup:

- Clean System—no voicemail or Call Data Records (CDRs) and no service appliance
  - Total – 379 secs
  - VM – 2 secs
  - CDR– 35 secs
- Loaded System (VM: 100 messages/13.5 MB; CDR: 500,000 calls)
  - Total – 508 secs
  - Backup VM – 21 secs
  - Backup CDR – 104 secs

The following is an estimate of the time to restore Server files:

- Clean System
  - Total – 416 secs
  - VM – 3 secs
  - CDR – 32 secs
- Loaded System (VM: 100 messages/13.5 MB – CDR for 500,000 calls)
  - Total – 525 secs
  - VM – 22 secs
  - CDR – 98 secs

Note:

While running Anti-virus scan, if you perform a backup on Configuration (shoreware) or CDR (shorewarecdr) database, the backup process fails.

23.2.2 Backup Strategy

Before a server backup begins, server activity must be stopped prior to prevent file corruption. We provide the procedures for stopping server activity before a backup and restarting the server after the backup is complete. We recommend system backup during scheduled down times or periods of low activity.

Note:

Care should be taken to avoid backups during nightly server voicemail maintenance, since stopping the services could interfere with the maintenance. The default time for this is 2:00 AM.

When backing up an entire system, we recommend starting with the DVSs (if present) and backing up the Headquarters server last. You can back up multiple DVSs simultaneously. After DVS backup is complete, the system administrator can back up the files on the Headquarters server. This sequence allows the Headquarters server to operate while other servers are unavailable.

23.2.3 Restoration

The Mitel restore scripts perform all necessary tasks to restore the Headquarters server, DVSs, voicemail switches, and service appliances. The scripts can do either a complete restore or a selective restoration of specific files.

Operations and files saved on a server after the backup was created are lost when the files are restored to the server. When restoring a Headquarters server, all files on distributed servers that do not require restoring remain intact; however, voicemail received for mailboxes created since the backup was created may be lost regardless of the server upon which they reside.

During file restoration, the server must have no activity. The Mitel restore scripts stop the server before restoring the files and restarts the server after the restoration is complete. Restored files must come from the same folder where the backup operation stored them.

For restoring an entire system, Mitel recommends first restoring the headquarters server. Doing so establishes a functioning system. After the headquarters server restore, restore distributed servers while the headquarters server is active. This sequence minimizes the down time of the headquarters server. Restart DVS after restoring Headquarters database.

Files can only be restored to the server from which they were backed up. Backup files from the headquarters server can restore only the headquarters server. For systems with more than one distributed server, backup files are not interchangeable between the servers.

23.3 Configuring the Backup and Restore Scripts

Before using a script for backup or restore, modify the scripts to have the information in the list that follows (task descriptions follow this list):

- In the script, type the path to the folder that is the destination of the backup. For a restore operation, this same path points to the folder as a source.
- IP addresses of voicemail switches to back up or restore.
- IP addresses of the service appliances to back up or restore.
- Letter of the disk drive where the script file resides (if different from the C drive).
- Type path to the script file on the Headquarters server or DVS—if the path is different from the default path that we provide.
- Type the path on the server where the PLINK and PSCP functions reside—if the path is different from the default).

Note:

The default folder path for 32-bit and 64-bit applications differs as follows:

- For a 32-bit application, the path begins `C:\Program files (x86)\ . . .`
- For a 64-bit application, the path begins `C:\Program files\ . . .`

23.3.1 Configuring the HQ Server or DVS to Back Up Files

1. Using Windows Explorer on the server (Headquarters or DVS) that performs backups, navigate to the appropriate directory:
   - For a Headquarters server:

     ```
     C:\Program Files (x86)\Shoreline Communications\ShoreWare
     Server\Scripts\Sample_Backup_Restore
     ```
   - For a DVS:

     ```
     C:\Program Files (x86)\Shoreline Communications\Shoreware
     Remote Server\Scripts\Sample_Backup_Restore
     ```
2. Open the `sw_backup_restore.ini` file by using a text editor, such as Notepad.
3. Locate the `Window.Install.Drive` line in `sw_backup_restore.ini`.
4. On the line “`Window.Install.Drive – ”`, type the letter of the drive that has the Windows operating system. The default drive is C:.

5. In the Back Options section, specify where to create the backup files:

   a. On the line "Backup.Drive – ", type the path for the volume to which the MiVoice Connect system backs up the files.
   b. On the line "ShoreWare.Drive – ", type the letter of the drive on which the MiVoice Connect system files go. The default value is C.
   c. On the line "Backup.Root.Directory – " type the path that you want to use for backing the files up. The default path is:

      ```
      \ShorewareBackup\Backup
      ```

   d. On the line "Backup.Shoreware.Directory – " type the name of the file to which the system backs up the files. The default name is: \Shoreline Data.
6. In the Shoreware File Location section, specify the location of the Mitel files on the current server. The Headquarters server and DVSs have different default paths.

   For a Headquarters server, on the line "ShoreWare.Scripts.Root.Directory – ", type the path to the server backup scripts. The default path is:

   ```
   C:\ProgramFiles(x86)\ShorelineCommunications\ShoreWare Server
   \Scripts
   ```

   For a DVS, on the line "ShoreWare.Scripts.DVM.Root.Directory – ", type the path to the Mitel DVS server backup scripts. The default path is:

   ```
   C:\ProgramFiles(x86)\ShorelineCommunications\ShoreWare Remote
   Server\Scripts
   ```
7. On the line "VMB.ip.list – ", type the IP addresses of the voicemail switches that this server backs up. Type a comma (,) between the addresses.
8. On the line "UCB.ip.list – ", type the IP addresses of the service appliances that this server is backing up. Separate each address with a comma.
9. For the plink command: on the line "PLINK.CMD – ", type the path to the plink command. The default path is (keep in mind the difference between the servers and the operating systems):

   - On a Headquarters server:

     ```
     C:\ProgramFiles(x86)\Shoreline Communications\ShoreWare
     Server\Scripts\Sample_Backup_Restore\plink
     ```
   - On a DVS:

     ```
     C:\ProgramFiles (x86)\Shoreline Communications\ShoreWare
     Remote Server\Scripts\Sample_Backup_Restore\plink
     ```

10. For the pscp command: on the line: “PSCP.CMD – ”, type the path to the pscp command. The default path is (keep in mind the 64-bit and 32-bit OSs):

    - On a Headquarters server:

      ```
      C:\Program Files(x86)\Shoreline Communications\ShoreWare
      Server\Scripts\Sample_Backup_Restore\pscp
      ```

    - On a DVS:

      ```
      C:\Program Files(x86)\Shoreline Communications\ShoreWare
      Remote Server\Scripts\Sample_Backup_Restore\pscp
      ```

11. Click **File > Save** to save changes

23.4 Preliminary Task for Remote Devices

An RSA key must exist in a server registry cache for each Voice Switch or Service Appliance. The system uses this RSA key for backups and restores. This section describes the preliminary task of placing an RSA key in a cache on a server.

In the context of backup or restore, Voice Switches and Service Appliances are remote devices. These devices are remote from the standpoint of the Headquarters server or a DVS. On the Headquarters server or a DVS, the system administrator initiates the backup or restore operation for a voicemail switch or a service appliance.

To perform backup or restore, an SSH connection must exist between the server and the remote device. The PuTTY commands plink and pscp provide the access to remote devices. These commands use RSA keys for validation.

Note:
Beginning with Release 19.2, you must upgrade the PuTTY to Version 0.73 to establish an SSH connection between Linux devices and v-Model switches such as LDVS, vphone, vTrunk, and vUCB.

To place an RSA key in a server registry cache for a remote device:

1. Open a command prompt window on the server that initiates the backup and restore for the voicemail switch or service appliance.

2. Change directories to one of the following:

   - On a Headquarters server:

     ```
     C:\Program Files (x86)\Shoreline Communications\ShoreWare
     Server\Scripts\Sample_Backup_Restore
     ```

   - On a DVS:

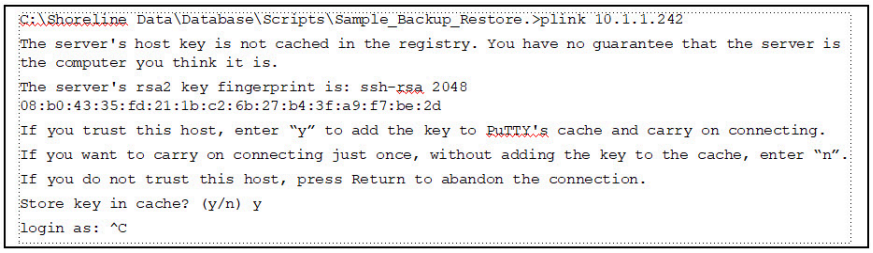
     ```
     C:\Program Files (x86)\Shoreline Communications\ShoreWare
     Remote Server\Scripts\Sample_Backup_Restore
     ```

3. At the command prompt, type the following:

   ```
   >plink <IP address of voice switch or IP address of service
   appliance>
   ```

4. Press **Enter**. The system response includes the storage status of the RSA key in the registry on the server. The following figure illustrates the response if the key is not present. It states “The server's host key is not cached in the registry.”

Figure 21: Caching the Registry Key by Using the plink Command



5. If the key is not cached to the registry, press y at the prompt (“Store key in cache? (y/n)”).
6. Repeat Step 3 through Step 5 for each remote device for which this server is to initiate backup and restore operations.
7. When the commands are run through plink, **bashrc** must be sourced manually.

   For example, command to check service status on the UCB (/shoretel/bin/svccli getsvcstatus):

   - `plink.exe -ssh -pw ShoreTel admin@10.198.104.214 source .bashrc;/shoretel/bin/svccli getsvcstatus`
   - `plink.exe -ssh -pw ShoreTel admin@10.198.104.214 source .bashrc;/shoretel/bin/CMCA`

23.5 Backing Up the Headquarters Server

This section describes how to back up the headquarters server. Its subsections describe a complete backup of the server and a partial backup of the server.

Note:

Server activity must stop before file backup to prevent file corruption. The processes from Mitel stop the server before the backup and restarts the server after the backup finishes. Mitel recommends backing up files during scheduled down times or periods of light activity.

23.5.1 Backing Up All of the Files

Performing a complete backup of the Headquarters server:

1. Access the command prompt on the headquarters server.
2. Navigate to the directory where the Mitel backup and restore script resides. The default path is:

   ```
   C:\Program Files (x86) \Shoreline Communications\Shoreware Server\Scripts\Sample_Backup_Restore
   ```
3. At the prompt, enter:

   ```
   cscript.exe shoreware_backup.wsf hq all
   ```

   A notification appears when the backup is complete.
4. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

23.5.2 Backing Up Selected Files

Using the Headquarters server to back up selected file types on specific components:

1. Open a command prompt on the Headquarters server.
2. Navigate to the directory where the Mitel backup and restore script resides. The default path is: `C:\Program Files (x86)\Shoreline Communications \Shoreware Server\Scripts\Sample_Backup_Restore`

3. At the prompt, type:

   ```
   cscript.exe shoreware_backup.wsf x y
   ```

   where x is the component type to back up, and y is the file type. For the definitions of possible x and y values and their combinations, see the table below. For example, if x equals ucb, then y must be all: cscript.exe shoreware_backup.wsf ucb all
4. Click **Enter**.

Note:

- When backing up the Headquarters server or a DVS, a notification appears when the backup is complete.
- When backing up a voicemail switch or service appliance, the status for the backup is displayed on the command line.

5. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

Table 215: Backup Arguments

component (X)		File Type (y)
Argument	**Definition**	**Applicable Arguments**
hq	Headquarters server	• all • db • vm • cdr
dvm	Distributed Voice server	• all • db - Applicable only for DVSs that have a distributed database (DDB) • vm
vmb	Voicemail Model Switch	all
ucb	Service Appliance	all

23.6 Backing Up SBE Systems

The SBE system server, the UC30, is configured with the following three scheduled backup tasks that are disabled at installation:

- DVS Backup — snapshot of the DVS
- HQ Backup — snapshot of the Headquarters
- SQL Backup — snapshot of the shoreware, webbridge and cdr directories

You can configure these backup tasks to run on demand or to run automatically.

23.6.1 Run Backup On Demand

Complete the following steps to configure the tasks to run on demand:

1. Launch the Windows Task Scheduler.
2. Select the task you want to run.
3. In the Action pane, click **Run**.

Complete the following steps to configure the tasks to run on a schedule:

1. Launch the Windows Task Scheduler.
2. Right-click the task you want to configure runtime for, and then select **Properties**.
3. In the Action pane, click Run.
4. Click the **Triggers** tab, and then click **Edit**.
5. Modify schedule settings as necessary, and then click **OK**.

The backups are stored in `<install_dir>\Shoreware Backup`. The Backup, Backup1, and Backup2 folders are created to store the information and are rotated each time the backup runs. The backup process also includes the MySQL folder, which stores database information for each run.

If the backup does not complete, refer to the log files for details. The log files are stored in `c$\Windows\OEM\shoretel\scripts hqbackup.log and sqlbackup.log`.

To safely preserve backed up data, copy completed backups to a fault tolerant location.

Note:

Periodically check the amount of free disk space on the UC30 to ensure that backed up data is not consuming too much space

23.7 Backing Up Distributed Voice Servers

This section describes how to back up a distributed voicemail server. It describes how to do a complete backup and a partial backup. To facilitate the process, we recommend that you back up files during scheduled maintenance times or periods of low system activity.

Note:

To prevent the system from corrupting files during the backup, server activity must stop before the backup begins. The processes that Mitel provides stop the server before the backup and restarts the server after the backup finishes.

23.7.1 Performing a Complete Backup of a DVS

1. Access the command prompt on the DVS you want to back up.
2. Navigate to the following directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\ShorelineCommunications\ShorewareRemote Server\Scripts\Sample_Backup_Restore
   ```
3. At the prompt, enter the following command:

   ```
   cscript.exe shoreware_backup.wsf dvm all
   ```

   A notification appears when the backup is complete.
4. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

23.7.2 Performing a Selective Backup of a DVS

1. Access the command prompt on the DVS you want to back up.

2. Navigate to the following directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\ShorelineCommunications\Shoreware Remote Server\Scripts\Sample_Backup_Restore
   ```

3. At the prompt, enter:

   ```
   cscript.exe shoreware_backup.wsf dvm y
   ```

   where y is the file type. See Restore Arguments for the possible values of y (when x is dvm).

   A notification appears when the backup is complete.

4. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

23.8 Backing Up Linux Distributed Voice Servers

Scheduling Automatic Backup for Linux DVS

To configure automatic backup for Linux DVS:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
3. Click the name of the Linux DVS to configure in the list pane.

> **Note**:
> The **General** tab in the **Details** pane displays parameters for the selected Linux server.

4. Select the **Enable daily backup** check box.
5. Under **Enable daily backup**, in the **Start time** field, type the time of day to start the daily backup.

   The default start time is 2AM.

6. In the **IP address** field, do either of the following:

   - For FTP server, enter the IP address of the FTP server to which the switch files must be backed up.
   - For HTTPS server, enter the IP address of the HQ server to which the switch files must be backed up.

7. In the **FTP port** field, enter the port number that the Linux DVS uses to communicate with the recipient FTP server.
8. In the **Directory** field, do either of the following:

   - For FTP server, enter the name of the folder on the FTP server to which you want to back up the Linux DVS files.

   Note:
   The default location is `\inetpub \ftproot\`.

   - For HTTPS server, enter the name of the folder on the HQ server to which you want to back up the Linux DVS files.

   Note:
   The default location is `\inetpub \ftproot\uploads`.

9. For HTTPS server, select the **Enable HTTPS** check box.
10. In the **Username** field, enter the user name that the Linux server uses to access the backup files on the FTP server.
11. In the first **Password** field, enter the password that the Linux server uses to access the backup files on the FTP server.
12. In the second **Password** field, reenter the password that you entered into the first field.
13. Click **Save**.

23.9 Backing Up Connect Edge Gateway

The Connect Edge Gateway configuration can be backed up to an FTP, SCP (for secure EGW backup), or TFTP server by using the On Demand method or by scheduling a backup.

Note:

To restore a configuration, refer to Backing Up Voice Mail Switches on page 876.

23.9.1 On Demand Backup

To perform on demand back up of the Connect Edge Gateway configuration:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the **List** pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **System** > **On Demand Backup**.

Table 216: On Demand Backup Parameters

Parameter	Description
Hostname or IP Address	Location to send the configuration file.
Protocol	Protocol by which to send the file.
Port	Port number.
User ID	Entry must match the User ID for the selected server (FTP/SCP (for secure EGW backup)/ TFTP)
Password	Password for the user.
Path	Path to the directory and the filename to which you want to save the configuration file, for example “/home/user/backup/test.bak

Note:

- The FTP or TFTP server must be running for the backup to succeed.
- /var/tmp should not be used in the local host machine for backups. This is a temporary folder and the file is susceptible to being deleted. Use an external host to complete the backup.

5. Select **Backup**.

The Connect Edge Gateway displays a status prompt indicating the backup is in progress. If the backup is successful, the **Backup Succeeded** message displays. If the backup fails, the **Backup failed. See server log** message displays.

23.9.2 Scheduled Backup

To schedule a back up of the Connect Edge Gateway configuration:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the **List** pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **System** >**Scheduled Backup**. The **Schedules** tab displays any previous scheduled backup yet to be performed. The **History** tab displays the previously performed backups.
5. To add a new scheduled backup, select **Add** on the **Schedules** tab.

The following table includes a list of scheduled backup parameters for the Connect Edge Gateway.

Table 217: Scheduled Backup Parameters

Parameter	Description
Name	Name displays on the Connect Edge Gateway's **Schedules** and History pages
Description	Description of the backup
Frequency	• **Daily**: Select the **Hour** in 24 hour increments. • **Weekly**: Select the **Day** of the week and the **Hour** in 24 hour increments. • **Monthly**: Select the **Date** and the **Hour** in 24 hour increments.
Hostname or IP Address	The location to send the configuration file to
Protocol	Protocol by which to send the file

Parameter	Description
Path	Path to the directory and the filename to which you want to save the configuration file, for example “/home/user/backup/test.bak
Filename Prefix	Name of the file as it displays at the backup location. This name prepends the default file name which includes the Connect Edge Gateway name, the date of the backup, and the time of the backup in the form “[filename prefix]-[hostname]-[YYYYMMDD]-[HHMMSS].bak”. For example, if “test” is the Filename Prefix, the results display “test-egw-20110826-103000.bak”

Note:

- The FTP or TFTP server must be running for the backup to succeed.
- “/var/tmp” should not be used in the local host machine for backups. This is a temporary folder and the file is susceptible to being deleted. Use an external host to complete the backup.

23.10 Restoring the Connect Edge Gateway Configuration

If you need to roll back to a previous Connect Edge Gateway configuration file, you can restore the previous configuration. You can restore a configuration file only if it has been saved and uploaded to a TFTP, FTP, or SCP (for secure EGW backup) server.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the **List** pane to launch the Connect Edge Gateway administration portal.

4. Select **Maintenance** > **System** > **Restore**.

The following table includes a list of restore parameters for the Connect Edge Gateway.

Table 218: Restore Parameters

Parameter	Description
Hostname or IP Address	IP address or name of the server where the configuration file is stored.
Protocol	Protocol by which to send the file. Depending upon the type of protocol, for example FTP or SCP, (for secure EGW backup) enter the relevant information such as **Port number, User ID,** and **Password**.
User ID	Entry must match the User ID for the selected server (FTP/SCP (for secure EGW backup)/TFTP).
Password	Password for the user.
Path	Path to the directory and the filename to which you want to save the configuration file, for example “/home/user/backup/test.bak
Filename Prefix	Name of the file as it displays at the backup location. This name prepends the default file name which includes the Connect Edge Gateway name, the date of the backup and time of the backup in the form “[filename prefix]-[hostname]-[YYYYMMDD]-[HHMMSS].bak”. For example, if “test” is the Filename Prefix, the results display “test-egw-20110826-103000.bak”

Note:

- The FTP or TFTP server must be running for the backup to succeed.
- “/var/tmp” should not be used in the local host machine for backups. This is a temporary folder and the file is susceptible to being deleted. Use an external host to complete the backup.

5. Check Include **Network Information** and/or **Include Certificates** as appropriate.
6. Select **Restore**. If the restore is successful, the “Configuration is restored. You need to restart your browser.” message displays. If the restore fails, the “Restore failed. See server log” message displays.
7. Exit and restart the browser.
8. Log in to the Connect Edge Gateway admin portal by entering the Admin login and password.

23.11 Restoring Connect EG Factory-Default Settings

If necessary, you can restore the Connect Edge Gateway to its default settings. If you restore to default settings, all settings but the following are reset to default values:

- Connect Edge Gateway IP address
- Default gateway
- Domain name

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. Click the **Name** of the Edge Gateway from the **List** pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **System** > **Factory Defaults**.
5. Click **Revert**.
6. Click **OK** to confirm setting the Connect Edge Gateway to the factory-default configuration. You are logged out.
7. Exit and restart the Web browser. Log in as administrator in to the Connect Edge Gateway admin portal by entering the Admin login and password.

23.12 Backing Up Voice Mail Switches

This section describes how to back up voice mail switches. Backup of voice mail switches must begin on the Headquarters server or a DVS. The modified backup script on the server must include the IP addresses of the voice mail switches to back up. .

Note:

See Configuring the Backup and Restore Scripts on page 860 for information about modifying the script file)

23.12.1 Requirements

- Headquarters server or DVS to implement the backup.
- `sw_backup_restore.ini` file on implementation server that include IP address of each voice mail switch.
- Ability to establish an SSH connection with the voicemail switch.

Note:
Beginning with Release 19.2, you must upgrade the PuTTY to Version 0.73 to establish an SSH connection between Linux devices and v-Model switches such as LDVS, vphone, vTrunk, and vUCB.

Backing up voice mail switches:

1. Access the command prompt on the server that is configured to backup to the voice mail switches.
2. Navigate to the following directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server\Scripts\Sample_Backup_Restore
   ```
3. At the command prompt, enter:

   ```
   cscript.exe shoreware_backup.wsf vmb all
   ```

   The status of the backup is displayed on the command line.
4. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

23.13 Backing Up All Service Appliances

Backing up service appliances begins on the Headquarters server or a DVS. The back-up script on the server must include the IP address of each service appliance to back up. For the description of how to modify a script by adding IP addresses, see Configuring the Backup and Restore Scripts on page 860.

The necessary elements for backing up service appliances are as follows:

- Headquarters server or DVS to implement the backup.
- `sw_backup_restore.ini` file on the server that initiates the backup (a file that contains the IP address of the service appliances to back up).
- Capability of the server to establish an SSH connection with each service appliance.

Note:
Beginning with Release 19.2, you must upgrade the PuTTY to Version 0.73 to establish an SSH connection between Linux devices and v-Model switches such as LDVS, vphone, vTrunk, and vUCB.

To back up all service appliances:

1. Open a command prompt on the server that backs up the service appliances.
2. Navigate to the following directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server\Scripts\Sample_Backup_Restore
   ```
3. Enter the following on the command line: `cscript.exe shoreware_backup.wsf ucb all`

   The status of the backup is displayed on the command line.

Note:

Running the `hq_backup_all` batch file also calls the command in Step 3. For details about using a batch file, see Using Batch Files on page 883.

4. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

23.14 Restoring the Headquarters Server

This section describes how to use the Mitel backup and restore script to perform complete and selective restores to the headquarters server.

23.14.1 Performing a Complete Restore

1. Access the command prompt on the headquarters server.
2. Navigate to the following directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server\Scripts\Sample_Backup_Restore
   ```
3. At the prompt, enter:

   ```
   cscript.exe shoreware_restore.wsf hq all
   ```

   A prompt appears notifying you that restoring will wipe out all existing data.
4. Click **Yes** to proceed.

   A notification appears when the restore is complete.
5. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

23.14.2 Performing a Selective Restore

The system has a script for restoring selected files. Follow this procedure to restore selected files:

1. Open a command prompt on the headquarters server.
2. Navigate to the appropriate directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server\Scripts\Sample_Backup_Restore
   ```
3. Type the following at the prompt:

   ```
   cscript.exe shoreware_restore.wsf x y
   ```

   where ***x*** is the component type to restore, and ***y*** is the file type. For the definitions of possible *x* and *y* values and their combinations, see the table below. For example, if *x* equals **ucb**, then *y* must be **all**: `cscript.exe shoreware_restore.wsf ucb all`

4. Press **Enter**.

   When backing up the Headquarters server or a DVS, a notification appears when the restore is complete.

   When backing up a voicemail switch or service appliance, the status for the restore is displayed on the command line.
5. To ensure the backup completed correctly, check that the backup files were created in the location specified in the .ini file.

Table 219: Restore Arguments

Component (x)		File Type (y)
Argument	**Definition**	**Applicable Arguments**
hq	Headquarters server	• all • db • vm • cdr
dvm	Distributed Voice server	• all • db - Applicable only for Headquarters and for DVSs with distributed database (DDB) • vm
vmb	Voicemail Model Switch	all
ucb	Service Appliance	all

23.15 Restoring Distributed Voice Servers

This section describes how to use the Mitel backup and restore script to perform complete and selective restores to DVSs.

23.15.1 Performing a Complete Restore of a DVS

Performing a complete restore (all files) of a DVS:

1. Access the command prompt on the DVS to restore.
2. Navigate to the directory where the Mitel backup and restore scripts are found. The default path is:

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware
   Remote Server\Scripts\Sample_Backup_Restore
   ```
3. At the prompt, enter the following command:

   ```
   cscript.exe shoreware_restore.wsf dvm all
   ```

   A notification appears when the restore is complete.

23.15.2 Performing a Selective Restore of a DVS

The MiVoice Connect system allows restoration of selected files to a DVS. To use the headquarters server to restore selected files to a DVS:

1. Access the command prompt on the DVS to restore.
2. Navigate to the appropriate directory where the Mitel backup and restore script resides.

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware
   Remote Server\Scripts\Sample_Backup_Restore
   ```
3. At the prompt, enter the following command:

   ```
   cscript.exe shoreware_restore.wsf dvm y
   ```

   where *y* is the file type. See Restore Arguments for the possible values of *y* (when x is dvm).

   A notification appears when the restore is complete.

23.16 Restoring a Service Appliance

A full system restore includes all connected service appliances. However, reasons might exist for restoring just the conference recordings and other files to a service appliance. For example, if a customer replaces a defective service appliance with a new unit, a system administrator uses the commands in this section to restore the files to the new unit. (Connect Director has no way to restore specific files to a service appliance.)

In general, the method consists of the following tasks:

- Creating an SSH or serial connection from the main server to the service appliance

- Executing the `restoreweb` command on the command line interface (CLI) of the service appliance.

Note:

`Backupweb` and `restoreweb` are Services Manager CLI (`SVCCLI`) commands.

23.16.1 Operational Behavior for Manual Restore

This section lists the restored files and describes the behavior of the file system in conjunction with a manual restore. The section describes regular behavior and variations in behavior of the file system during the restore. The variations depend on file system activity that does not directly involve either the backup or the restore—for example, file saves that happen after a backup.

Executing the `restoreweb` command restores the following:

- Library files
- Public: */site/vlibrary*
- Private: */site/<user_id>/vlibrary*
- Recordings: */site/<user_id>/vmeetings/<rec_meeting_id>*
- IM/Presence data: */cf/shorelinedata/UserData*
- SSL certificates: *cf/certs*

The following are notable behaviors:

- During the restore, all services on the service appliance stop running.
- The restore operation can occur on non-empty directories.
- The restore operation does not delete files that are in the file system and are not part of the last backup.
- Files that are created after the previous backup remain intact.
- If a backed-up file on the system changes after the most recent backup, the restore operation replaces the modified file with the backed-up version.
- The restore process can appear to restore files that have been deleted since the previous backup. However, these files are not accessible through the service appliance GUI because the system does not maintain database links to deleted files. To retrieve these disconnected files (if necessary), start an SSH session or serial connection to the appliance and retrieve them by using the correct Linux command.

Consider the following scenario:

1. Some files are uploaded after a backup.
2. The service appliance fails before a subsequent backup.
3. The failed unit is replaced and the content restored.
4. Entries are visible for the files that were not backed up before the device failure.

23.16.2 Performing the Manual Restore

The DB links point to files that do not exist. Manually delete the dead links by using the Personal Library tab of the Mitel Conferencing web-based user interface. Recordings without links must be removed in the same way.

Although a restore job might accidentally restore deleted files, you cannot access them through the Conferencing web interface because the Headquarters database does not link to them. However, you can use Linux commands to log into the system and extract the deleted files.

Mitel supports backup of multiple service appliances to one machine. If multiple service appliances use the same machine for backup, a unique backup destination directory must exist for each service appliance. Although the backup or restore operation relies on command prompt commands, the enable or disable and the configuration of a multi-device backup also depends on information in Connect Director. Specifically, the location for the backed-up files is the destination directory in Connect Director.

For a subsequent file restoration, the restore process copies files from the right directory to restore each service appliance.

Note:

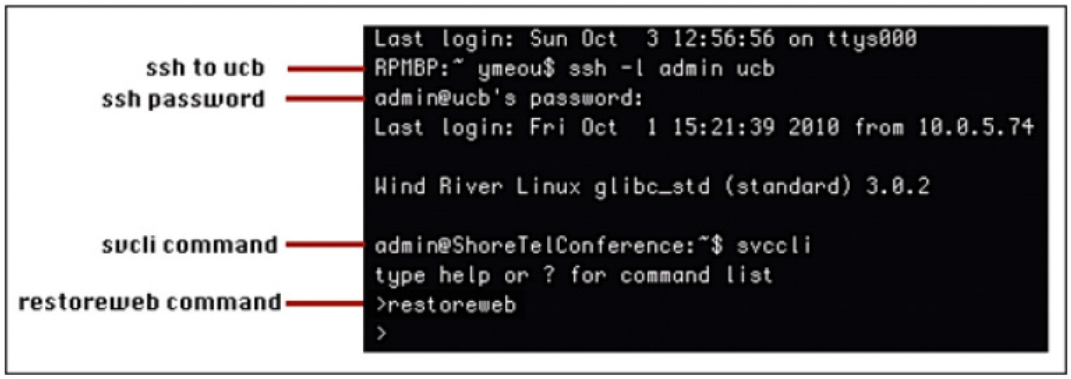
If the network has more than one service appliance, back up or restore the database and all the service appliances at the same time to avoid dead links.

To restore the backed-up files to a service appliance:

1. Activate the SVC command prompt by entering one of the following commands at the Linux prompt:
   - `$ svccli` - for admin access
   - `# svccli` - for root access
2. Start the restore using the `restoreweb` command.
3. Wait for the restore to complete. The restore is complete when the `restoreweb` command returns you to the svccli prompt ('>').

4. Verify that the restore is complete by checking the `/cf/shorelinedata/Logs/.FtpSync-<date>.<time>.Log` file, where <date> is the current date and <time> is the time when the log file was created.
5. The following figure illustrates all of the steps for accessing a service appliance through SSH and then running the `restoreweb` command.

Figure 22: The SVC Command Prompt with restoreweb Command Appliance



23.17 Using Batch Files

The batch files reside in the same folder as the scripts. These batch files let you back up or restore different Mitel components on the site, including the following components:

- Headquarters
- Distributed Voicemail
- Voicemail Model Switches
- Service Appliances

To batch file commands for backup are as follows:

- `hq_backup_all.bat`
- `dvm_backup_all.bat`
- `vmb_backup_all.bat`
- `ucb_backup_all.bat`

The batch commands for restore are as follows:

- `hq_restore_all.bat`
- `dvm_restore_all.bat`
- `vmb_restore_all.bat`
- `ucb_restore_all.bat`

Using a batch file to back up or restore files:

1. Access the command prompt on the Mitel server.
2. Navigate to the directory where the script resides. The default path is:

   ```
   C:\Program Files (x86)\Shoreline Communications\Shoreware Server\Scripts\Sample_Backup_Restore
   ```
3. At the prompt, enter the batch file to use for backup or restore.

Note:

- When backing up the Headquarters server or a DVS, a notification appears when the backup is complete.
- When backing up a voicemail switch or service appliance, the status for the restore is displayed on the command line.

23.17.1 Log Files

Log files display the commands that are performed during backup and restore operations at SwBackupRestore.log. By default, Windows maintains three log files. The log files reside in the same directory as the scripts.

23.18 Failover Support

To support high availability, Mitel provides failover at two points in the network:

- The Headquarters server
- Voice Switches

For the headquarters server, you can install a backup server that mirrors and monitors the primary server. If the primary server fails, operations are immediately transferred to the back-up server with minimal interruption of services. After the primary server is repaired, you must manually fail back the secondary server to return operations to the primary server and return the backup server to its backup role.

This section discusses failover at the server level. For more information about switch failover, see Failover for IP Phones: Spare Switch on page 178.

For switches, you set up the failover capability by either of the following methods:

- Configuring the switches with extra port capacity.

- Installing spare switches that can temporarily manage the phones upon switch failure. Spare switches can reside on a network that is remote to the failed switch and its phones, but the level of service might not equal the switches in the local network.

23.18.1 Configuring a Secondary IP Address for Server Failover

After you have created a backup server for your system, you must designate the backup server for failover function.

To designate a backup server for the failover function:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page opens.
3. In the **Name** column, click **Headquarters**.

Note:
The **General** tab in the **Details** pane displays parameters for the Headquarters server.

4. In the **Secondary IP address** field, enter the IP address of the server that you want to use for failover.
5. Click **Save**.

To convert a system to single Headquarters Server mode, remove the address from the secondary IP address field, then reboot the Headquarters server. If you are modifying the IP address of a DVM server, then reboot the DVM.

When the primary and secondary servers reside in different subnets, the IP address for each server must be static.

The DNS server that a MiVoice Connect system accesses must associate the same server name to the primary and secondary servers if:

- The primary and secondary servers are configured with static IP addresses.
- The Headquarters server supports the Connect client or clients on Citrix or Windows Terminal servers.

Note:
Mitel services cannot be running on the primary and secondary Headquarters servers at the same time. However, the servers can be on the network at the same time.

23.18.2 Conditions During Failover and Failback Operations

Mitel performs a failover operation when the primary server experiences an issue that triggers a transfer of the Headquarters server functions to the secondary server. After the failover operation is complete, the secondary server performs all Headquarters server functions.

The administrator can initiate a failback operation to restore Headquarters server function to the primary server, after ensuring the server is ready to be returned to service. After the failback is complete, the system structure that existed before the failback operation is restored.

Failover and failback operations typically last 5 to 20 minutes. The times depends on the system configuration. During these operations, no server services are available. The effects failover and failback operation are resolved after the operations are complete and the secondary (for failover) or primary (failback) server is functioning as the Headquarters server.

The effects of failover and failback operation on Connect client include the following:

- Users whose configuration exists on the Headquarters server lose most connectivity capabilities. The operations disrupt telephony and video but not IM connectivity.
- Users on distributed servers maintain all connectivity capabilities.
- Configuration changes (such as availability state, Find Me, and external assignment) are unavailable.
- Users logging into Connect client while the secondary server controls the system must specify the IP Address of the secondary server.

Refer to the *Mitel Connect Client User Guide* for instructions on specifying the server IP address.

Failover and failback operation can affect voicemail in the following ways:

- Sites that receive voicemail through the Headquarters server lose voicemail access.
- Mailboxes lose access to any voicemail whose routing includes the Headquarters server.
- Sites that receive voicemail from distributed servers retain voicemail access.

Failover and failback operation can affect other system components in the following ways:

- Account Code and Workgroup services are not available.
- Connect Director and Connect client configuration changes are not available.
- If DRS is enabled, intersite calls are unavailable to users residing on sites whose only access to a DRS server is through the Headquarters' DRS.

23.18.3 System Failover Conditions and Requirements

After the failover operation from the Headquarters server to the secondary server is complete, the secondary server performs all distributed server and application connectivity activities managed by the Headquarters server. The following sections describe required administrator tasks after the failover operation.

23.18.3.1 License Compliance

After a failover operation transfers the Headquarters server control to the secondary server, license status on the secondary server is non-compliant. To restore the system to compliance, reinstall all licenses that were originally purchased for the secondary server.

23.18.4 System Failback Conditions and Requirements

After the failback operation is complete, the primary server resumes all distributed server and application connectivity activities managed by the Headquarters server. The following sections describe required administrator tasks after the failback operation.

23.18.4.1 License Compliance

After a failback operation transfers Headquarters server control to the primary server, license status on the primary server is non-compliant. To restore the system to compliance, reenter the system key that was originally purchased for the primary server.

23.19 Failover and Restoration of IP Phones

When you enable the system parameter to fail over IP phones, the IP phones automatically fail over to another switch on the same site or to a spare switch when they lose connection with their primary switch. The spare switch is designed as a temporary measure to ensure that IP phone users have basic phone connectivity if the primary switch fails. To ensure that users have full connectivity, you must repair or replace the failed primary switch as soon as possible. If you are using the Mitel's Disaster Recovery solution, you must configure a secondary IP address.

The sections under the following sections describe how to restore normal operation after a failover occurs:

23.19.1 Re-assigning Primary Switch Profile to a Replacement Switch

If you replace a primary switch, you can re-assign the original switch profile to the new physical switch rather than create a new profile. This section describes how to re-assign the switch profile.

The requirements are:

- Obtain a replacement switch that has the same capabilities as the failed switch.
- Physically install the replacement switch on the same network as the old switch.
- Assign the new switch an IP address.
- Unplug the port connections (telephones, trunks) from the existing voice switch and plug them into the new voice switch.

Reassigning the switch profile:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
3. In the **List** pane, select the voice switch that is being replaced.

Note:
The **General** tab in the **Details** pane displays parameters for the switch.

4. Do one of the following:
   - In the **IP address** field, enter the IP address (or Ethernet address) of the new switch that you want to use to replace the original switch.
   - Click **Find switches** to search for and select the replacement switch.
5. Click **Save**.

Note:
It can take up to two minutes for the switch to come online.

23.19.2 Moving IP Phones to the Primary Switch

Moving IP phones from the spare switch to the primary switch:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **Telephones**. The **Telephones** page opens.
3. In the **List** pane, select the check box for each IP phone that you want to move.

Note:
You can select multiple phones to move at one time. The phones do not have to be registered to the same switch.

4. In the **Move to site** drop-down list, select the site where the switch you want to move the phones to is installed.
5. In the **and switch** drop-down list, select the switch to move the IP phones to.
6. Click **Move**.

The phones are moved to the selected primary switch.

Note:
Calls that are currently in progress are dropped during the move.

23.19.3 Failing Back the Spare Switch

After you move the IP phones to the primary switch on the site, you must manually failback the spare switch.

Note:

Ensure that zero (0) IP phones are connected to the spare switch before initiating the fail back. The Phones column in the list pane should display 0/N where 0 is the number of phones currently registered with the switch and N is the switch capacity.

1. Launch Connect Director.

2. In the navigation pane, click **Maintenance** > **Status** > **Switches**. The **Switches Maintenance** page opens.
3. In the **List** pane, select the spare switch to fail back.

> **Note**:
> The **Performance** tab in the **Details** pane displays details for the switch.

4. Select the **Status** tab.
5. In the **Command** drop-down list, select **Failback**.

The failback process starts. The process takes a few minutes to complete and includes rebooting the spare switch. When the process is complete and successful, the spare switch returns to the spare state.

23.19.4 Verifying Spare Switch Return Status

Once the failback process is complete, you should verify that the switch has returned to the spare state.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Spare Switches**. The **Spare Switches** page is displayed.
3. Verify the following:

   - The **Current Site** column is empty.
   - The **IP Phones in Use** column lists zero (0).

Reporting 24

This chapter contains the following sections:

This chapter describes how you can generate Call Detail and Web Conference reports for the Mitel network by using Connect Director.

24.1 Introduction

By using the Reporting feature, you can create and view reports about calls and web conferences in your Mitel system.

On Connect Director, you can generate the following types of reports:

- Call Detail Reports on page 891
- Web Conference Reports on page 957

In addition to viewing detailed call and web conference reports, you can also send call detail records (CDRs) through the serial (COM) port on the server, or archive them locally in a database. To configure these reporting options, see Configuring Reporting Options on page 959.

24.2 Call Detail Reports

All calls that are generated in a Mitel system are stored as call data records (CDRs) in the Call table in the database on the Headquarters server. The CDRs store call details and are used to generate call detail reports on Connect Director.

Note:

The CDR data that is collected from different time zones is adjusted to the time zone of the Headquarters server.

The Call Details page allows you to generate and view the following different types of call detail reports:

- Account Detail Report. See Generating the Account Detail Report on page 893 for more details.
- Account Summary Report. See Generating the Account Summary Report on page 897 for more details.
- Trunk Activity Detail Report. See Generating the Trunk Activity Detail Report on page 901 for more details.
- Trunk Activity Summary Report. See Generating the Trunk Activity Summary Report on page 905 for more details.
- User Activity Detail Report. See Generating the User Activity Detail Report on page 909 for more details.
- User Activity Summary Report. See Generating the User Activity Summary Report on page 917 for more details.
- WAN Media Stream Detail Report. See Generating the WAN Media Stream Detail Report on page 923 for more details.
- WAN Media Stream Summary Report. See Generating the WAN Media Stream Summary Report on page 928 for more details.
- Workgroup Agent Detail Report. See Generating the Workgroup Agent Detail Report on page 932 for more details.
- Workgroup Agent Summary Report. Generating the Workgroup Agent Summary Report on page 939 for more details.
- Workgroup Queue Summary Report. See Generating the Workgroup Queue Summary Report on page 945 for more details.
- Workgroup Service Level Summary Report. See Generating the Workgroup Service Level Summary Report on page 951 for more details.

Note:

1. The system can generate a maximum of five reports simultaneously. For example, you can generate a report and start another report before the first report is complete.
2. The Reporting feature utilizes CPU resources that are required for system operation. To avoid impacting or disrupting service, no more than two users should run reports at the same time. **Mitel recommends running reports during low CPU usage periods to avoid negatively impacting system performance**.

24.2.1 Generating the Account Detail Report

The Account Detail Report describes call details, such as the date and time of the call, the dialed number, the calling extension, and the call duration.

To generate the Account Detail Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Account Detail Report**.
4. Do one of the following:
   - To enter a specific account code for which to generate the report, click Add and specify the account code. Repeat this step if you want to add more account codes.
   - To generate a report for all account codes, proceed with the next step.
5. Do one of the following:
   - Specify the extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click Add and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all extensions, proceed with Steps 6 to 8.
6. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
7. In the **Time range** section, enter the start time and end time for the report period, or accept the default values. The parameters you can set for this report are described in the following table.

Table 220: Account Detail Report Parameter Descriptions

Parameter	Description
Report type	The type of report you want to generate.

Parameter	Description
Enter the Account codes you want the report on, or leave it blank for all Ac count codes:	Account codes are used to identify an account and can be used to assist in billing. Click **Add** to add account codes for which you want to generate the report or leave blank to report on all account codes. Click **Remove** to remove the account codes that you had added.
Enter the extension, or range of extensi ons, you want to report on. You can add multiple extensions, or you can leave this field blank to report on all extensions:	Click **Add** to add extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box.
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

8. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Account Detail report are described in the following table.

Table 221: Account Detail Report Field Descriptions

Field	Description
Start	The first **Start** field indicates the start date as entered prior to generating the report. If you selected **No lower limit** when generating this report, this field is left blank. The second **Start** field indicates the start time as entered prior to generating the report. If you selected **No lower limit** when generating this report, this field is left blank. If you did not enter a specific value, this field displays the default start time of *12:00 AM*.

Field	Description
End	The first **End** field indicates the end date as entered prior to generating the report. If you selected **No upper limit** when generating this report, this field is left blank. If you did not enter a specific date, this field displays the default date (typically the date that you generated the report). The second **End** field indicates the end time as entered prior to generating the report. If you selected **No upper limit** when generating this report, this field is left blank. If you did not enter a specific value, this field displays the default end time of *11:59 PM*.
Date	The date the call was placed in MM/DD/YYYY format.
Time	The time the call was placed in HH:MM:SS 12-hour format.
Dialed Number	For outbound calls, this is the number that the user dialed. It is reported in full canonical format (including country code). For inbound calls, this is the destination of the call. If the call was a DID or DNIS call, this is the DID or DNIS information for the number dialed. For other types of calls, this is the extension where the call first terminates. The information for this field is retrieved from the DialedNumber field of the Call table record.
Calling Extension	The extension number that placed the call.
Duration	The duration of the call, which is recorded from the time that the call is answered to the time it is terminated.
Total Calls	The total number of calls made for the specified account code.

Field	Description
Average Duration	The average duration of the calls made for the specified account code.
Total Duration	The total duration of the calls made for the specified account code.
Grand Total	The total number of calls made for all specified account codes.

24.2.2 Generating the Account Summary Report

The Account Summary Report describes call summary details, such as the total number of calls made, and the total and average duration of the calls.

To generate the Account Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Account Summary Report**.
4. Do one of the following:
   - To enter a specific account code for which to generate the report, click **Add** and specify the account code. Repeat this step if you want to add more account codes.
   - To generate a report for all account codes, proceed with the next step.
5. Do one of the following:
   - Specify the extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click Add and specify that extension in both the Start of range and End of range fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all extensions, proceed with Steps 6 to 9.
6. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
7. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.

8. You can choose to select the **Enable user breakdown to see the details of each user of the account** option to segregate the report for each user, or leave it with the default setting.

Note:

The parameters you can set for this report are described in the following table.

Table 222: Account Summary Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.
Enter the Account codes you want the report on, or leave it blank for all Account codes:	Account codes are used to identify an account and can be used to assist in billing. Click **Add** to add account codes for which you want to generate the report or leave blank to report on all account codes. Click **Remove** to remove the account codes that you had added.
Enter the extension, or range of extensions, you want to report on. You can add multiple extensions, or you can leave this field blank to report on all extensions:	Click **Add** to add extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box.

Parameter	Description
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.
Enable user breakdown to see the details of each user of the account	Select this checkbox to enable the user breakdown to see the details of each user of the account.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

9. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Account Summary Report are described in the following table.

Table 223: Account Summary Report Field Descriptions

Field	Description
Start	There are two start fields in the Account Summary Report. The first **Start** field indicates the start date as entered by you while generating the report. If you had selected **No lower limit**, this field is left blank. The second Start field indicates the start time as entered by you while generating the report. If you had selected No lower limit, this field is left blank. If you did not enter a specific value, this field displays the default start time of **12:00:00 AM**.
End	There are two end fields in the account detail report. The first **End** field indicates the end date as entered by you while generating the report. If you had selected **No upper limit**, this field is left blank. If you did not enter a specific date, this field displays the date of generating the report. The second **End** field specifies the end time as entered by you while generating the report. If you had selected **No upper limit**, this field is left blank. If you did not enter a specific value, this field displays the default end time of **11:59:59 PM**.
Total Calls	The total number of calls made for the specified account code.
Total Duration	The total duration of all calls made for the specified account code.
Average Duration	The average duration of all calls made for the specified account code.
Total	The sum of the number of calls made, total duration, and average duration for the specified account code.

Field	Description
Grand Total	The sum of the number of calls made, total duration, and average duration for all specified account codes.

24.2.3 Generating the Trunk Activity Detail Report

The Trunk Activity Detail report displays a list of every call for each trunk in the trunk group. All calls are classified by the trunk group, and the number of calls, the total and average duration are summarized.

To generate the Trunk Activity Detail Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Trunk Activity Detail Report**.
4. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
5. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.

Note:

The parameters you can set for this report are described in the following table.

Table 224: Trunk Activity Detail Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.
Date range: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date). If you do not want to specify an end date, you can leave it as is (current date).

Parameter	Description
Time range: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is *(00:00)* or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is *(23:59)* or select the **No upper limit** check box.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

6. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Trunk Activity Detail Report are described in the following table.

Table 225: Trunk Activity Detail Report Field Descriptions

Field	Description
Starting Date	The start date and time as entered prior to generating the report. If you left selected the **No lower limit** option while generating this report, this field does not display a date. The displayed start time is as entered by you while generating the report. If you had selected the **No lower limit** option while generating this report, this field is left blank. If you did not enter a specific value, this field displays the default start time of **12:00:00 AM**.
Ending Date	The end date and time as entered by you while generating the report. If you had selected the **No upper limit** option while generating this report, this field is left blank. If you did not enter a specific date, this field displays the default date of generating the report (current date). The displayed end time is as entered by you while generating the report. If you had selected the **No upper limit** option while generating this report, this field is left blank. If you did not enter a specific value, this field displays the default end time of **11:59:59 PM**.
Trunk Group Name / Trunk Name	Name of the trunk group and individual trunk being reported. The trunk group name is retrieved from the GroupName field, and the trunk name is retrieved from the PortName field of the Connect table record.
Date	The date that the trunk was added to the call. The date is extracted from the ConnectTime field in the Connect table record.
Time	The time that the trunk was added to the call. The time is extracted from the ConnectTime field in the Connect table record.

Field	Description
In/Out	Trunk activity is considered to be **In** if the TrunkDirection field in the Connect table record is set to 2 (Inbound). Otherwise, the trunk activity is considered to be **Out**. When an external user calls the external number of a service appliance, two records appear in the report, and each record is listed as **In**.
Dialed #	For an outbound call, this is the number that the user dialed and is reported in full, canonical format (including country code). For an inbound call, this is the destination of the call. If the call was a DID or DNIS call, then this is the DID or DNIS information for the number dialed. This information is retrieved from the DialedNumber field in the Call table record. For other types of calls, this is the extension where the call first terminates. This information is retrieved from the PartyId field of the Connect table record.
Calling #	For inbound calls, this is the calling number—ANI or Caller ID—received by the Mitel system and is reported as delivered by the PSTN (may or may not include the 1 before the area code).For outbound calls, this is the extension of the user who placed the call. This information is retrieved from the Extension field in the Call table record. For other types of calls, this information is retrieved from the CallerID field in the Call table record.
User	Name associated with the extension that was the initial target of the call. For outbound calls, the user is the extension that first initiated the call. For inbound calls, the user is the extension that was the initial target of the call. This information is retrieved from the PartyIDName and PartyIDLastName fields of the Connect table record for the party that initiated the call, or was the target of the call. In the case of tandem calls, nothing is displayed.

Field	Description
Duration	The duration of the trunk activity. For an inbound call, the duration of the call begins when the trunk is seized and includes the talk time and hold time. The duration ends when the user hangs up or when the external party hangs up and disconnect supervision is received by the Mitel system. For an outbound call, the duration of the call begins when the trunk is seized. The duration ends when the user hangs up, or when the external party hangs up and disconnect supervision is received by the Mitel system. This information is retrieved from the Duration field of the Connect table record.
Subtotal	The total number of calls for a trunk.
Total	The total number of calls for a trunk group.
Grand Total	The total number of calls for all trunk groups.

Note:

Inbound and outbound is relative to the call, and not to trunk usage.

24.2.4 Generating the Trunk Activity Summary Report

The Trunk Activity Summary report displays a summary of all calls for each trunk by the trunk group. The report displays trunk call details separately for inbound and outbound calls.

To generate the Trunk Activity Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Trunk Activity Summary Report**.

4. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
5. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.

Note:

The parameters you can set for this report are described in the following table.

Table 226: Trunk Activity Summary Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.
Date range: Date start Date end	Start and end date to define the period for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date). If you do not want to specify an end date, you can leave it as is (current date).
Time range: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

6. Click **Run report**.

> **Note**:
>
> The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Trunk Activity Summary Report are described in the following table.

Table 227: Trunk Activity Summary Report Field Descriptions

Field	Description
Starting Date	Indicates the start date and time as entered by while generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.
Ending Date	Indicates the end date and time as entered by you while generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Trunk Group Name / Trunk Name	Name of the trunk group and individual trunk being reported. The trunk group name is retrieved from the GroupName field, and the trunk name is retrieved from the PortName field of the Connect table record.

Field	Description
Inbound: Qty Duration Average Duration	The quantity, total duration, and average duration for all inbound trunk activity during the reporting period. For an inbound call, the duration of the call begins when the trunk is seized, and includes the talk time and hold time. The duration ends when the user hangs up or when the external party hangs up and disconnect supervision is received by the Mitel system. Trunk activity is considered to be inbound if the TrunkDirection field in the Connect record is set to 2 (Inbound). The quantity is a count of the Connect table records during the reporting period that indicate inbound trunk usage. Duration is the sum of all the duration fields for the Connect table records that indicate inbound trunk usage. The average duration is calculated by dividing the total duration by the reported quantity.
Outbound: Qty Duration Average Duration	The quantity, total duration, and average duration for all outbound trunk activity during the reporting period. For an outbound call, the duration of the call begins when the trunk is seized. The duration ends when the user hangs up, or when the external party hangs up and disconnect supervision is received by the Mitel system. Trunk activity is considered outbound if the TrunkDirection field in the Connect table record is set to 3 (Outbound). The quantity is a count of the Connect table records during the reporting period for this trunk that indicate outbound trunk usage. Duration is the sum of all the duration fields for the Connect table records that indicate outbound trunk usage. Average duration is calculated by dividing the total duration by the reported quantity.

Field	Description
Total Qty Duration Average Duration	The quantity, total duration, and average duration for all runk activity during the reporting period.
Total	The total number of calls for a trunk group.
Grand Total	The total number of calls for all trunk groups.

24.2.5 Generating the User Activity Detail Report

The User Activity Detail report displays details of call activity for each user. This includes the time a call was received or made, the number dialed, and the trunk used. The report always displays external Calls and can be configured to display internal Calls. External calls are ones where the record in the Call table has a CallType value of 2 (Inbound) or 3 (Outbound). By default, all specified calls that have at least a talk time greater than zero are included in the report.

To generate the User Activity Detail Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **User Activity Detail Report**.
4. Do one of the following:
   - Specify the extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all extensions, proceed with Steps 5 to 9.
5. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
6. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.

7. You can choose to select the **Break report into 30 minute intervals** option to segregate the user activities into 30 minute intervals, or leave it unselected.
8. You can choose to select the **Show internal calls** option to have the report include all internal call details.

Note:

The parameters you can set for this report are described in the following table.

Table 228: User Activity Detail Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.
Enter the extension, or range of extensions, you want to report on. You can add multiple extensi ons, or you can leave this field bla nk to report on all extensions	Click **Add** to add extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box.
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.

Parameter	Description
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.
Break report into 30 minute inte rvals	Select this check box to run interval reports in which each report is subtot aled by 30 minute intervals.
Show internal calls	Select this check box to include internal calls in the report.

9. Click **Run report**.

   The report is generated and is displayed in a different browser tab.

Note:

- You can also select to include unanswered calls in the report (Unanswered calls are displayed with a talk time of zero.) For information about including unanswered calls in the report, see Reporting Options on page 772.
- Conference calls that use a Mitel conferencing device have two entries in the User Activity Detail report. The first entry shows the amount of time (duration) used to enter a pass code or user prompt. The second entry shows the duration of the entire conference call.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the User Activity Detail Report are described in the following table.

Table 229: User Activity Detail Report Field Descriptions

Field	Description
Start Date	The start date as entered by you while generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank.

Field	Description
End Date	The end date as entered by you while generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report.
Start Time	The start time as entered by you while generating the report. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.
End Time	The end time as entered by you prior to generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Show Internal Calls	Indicates whether you selected to include internal calls in the report. Values are either True (internal calls are included) or False (internal calls are not included.

Field	Description
Name	The name of the user who placed the call in the last Name, first Name, (extension number) format. For outbound calls, the Name (Extension) field of the Call record always reports the party that initiated the call. Inbound calls are reported according to the last party involved in the call (excluding voice mail and the auto-attendant). For example, if a call to extension 320 is not answered and the user's availability state forwards the call to his or her assistant at extension 452 who answers the call, the Extension field in the Call record contains 452. When an inbound call is forwarded to voice mail, the Name (Extension) field records the party involved in the call before it was forwarded to voice mail. For example, if a user with extension 320 doesn't answer a call and his or her availability state forwards the call to voice mail, the extension field is set to 320. The details for this field are retrieved from the PartyIDLastName, PartyIDName, and PartyID fields in the Connect table records. Non-users such as Workgroups, Voice Mail, Voice Mail Login, and Auto-attendant are also included in the report. The names of these extensions are reported for calls that only interact with these extensions (not a user extension). Like many other non-user extensions, the Mitel Audio Conference extension and Route Points are not displayed.
Date and Time	The date and time for each user record. Date is displayed in MM/DD/YYYY format. Time is displayed in HH:MM:SS 12-hour format. These details are retrieved come from the StartTime field in the Call table record for the call being reported. When interval reports are generated, the actual time that the call had started is displayed, even if the call extends into another interval.

Field	Description
In/Out	Indicates if the call is inbound/outbound/internal/external. If the CallType field of the Call record for the call is 2 (Inbound), **In-Int** is displayed for internal calls and **In-Ext** for external calls. If the CallType is 3 (Outbound), **Out-Int** is displayed for internal calls and **Out-Ext** is displayed for external calls. Mitel Audio Conference Service calls in which the service calls the user, **In-Int** is displayed.
WG	Indicates if the call is part of a work group. The information for this field is retrieved from the `workgroup` field of the Call table record.
WAN-VPN-Secured	Indicates if the WAN, VPN, and security are enabled or disabled for the call. DWOD is set to 0 for displaying **Secured** and st 1 for displaying **WAN-VPN-Secured**.

Field	Description
User Activity: Time Stamp Action	Indicates the user action taken with the time stamp in HH:MM:SS 12-hour format. For instance, the action taken by the user can be one of the following: • Originate: The user initiated the call or conference. • Called: The user received the call or joined the conference after the host. • Pick up: The user answered the call. • ForwardNoAnswer: The call was forwarded without being answered by the user. • Transfer: The call was transferred to another user. • ForwardAll: The user chose to forward all calls. • WGA Agent: The user was an agent for the workgroup. • Unpark: The user unparked the receiver. • Conference: The user joined the conference call. • SilentCoach: The user was silent on the call. • Parked: The user was parked. • SilentMonitor: The user was silently monitoring a call between two or more users.
Dialed#	For outbound calls, this is the number the user dialed and is reported in full, canonical format (including country code). For inbound calls, this is the destination of the call. If the call was a DID or DNIS call, this is the DID or DNIS information for the number dialed. For other types of calls, this is the extension where the call first terminates. The dialed number is retrieved from the DialedNumber field of the Call table record for the call. For Mitel conferences, the dialed number is the same as the number the first user dialed to join the conference.

Field	Description
Calling#	For inbound calls, this is the calling number—ANI or Caller ID—received by the Mitel system and is reported as delivered by the PSTN (may or may not include the 1 in front of the area code). The calling number is retrieved from the CallerID field of the Call table record. For outbound calls, this is the extension of the user that placed the call. In the case of Outbound calls, this data is retrieved from the PartyID field of the Connect record for the party that initiated the call. For Mitel conferences, the calling number is the same as the number the first user called from to join the conference.
Trunk	Indicates the trunk used for the call. This information is retrieved from the PortName field of the Connect table record for the trunk involved in the call.
Duration	The duration of the call at the indicated extension. Duration is recorded from the time the connection is established until the time it is terminated. Ring time is not considered in incoming or outgoing calls. Duration equals Talk time + Hold time (if talk time is a non-zero value). This applies to all reports. This information is retrieved from the Duration field of the Connect table record for the connection (where the Connect.CallTableID matches the Call.ID and Connect.PartyID matches Call.Extension). **Note**: If the user joining a conference has selected to be called for the conference and has not set the out-dial prompt, then there are two records for duration. The first duration record is the time it took to connect the user to the conference, and the second duration record is the time the user was on the conference.

Field	Description
Total	Indicates the total number of calls, total duration, and average duration for the user.
Grand Total	Indicates the total number of calls, total duration, and average duration for all users.

24.2.6 Generating the User Activity Summary Report

The User Activity Summary report displays a summary of all inbound and outbound calls for each user. This includes the type of calls made, as well as the total duration for all calls. The summary can be run for selected extension numbers.

The report always displays external calls and can be configured to display internal Calls. External calls are the calls where the CallType value in the Call table record has a value of 2 (Inbound) or 3 (Outbound).

To generate the User Activity Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select User Activity Summary Report.
4. Do one of the following:
   - Specify the extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and End of range fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click Add and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all extensions, proceed with Steps 5 to 9.
5. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
6. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.
7. You can choose to select the **Break report into 30 minute intervals** option to segregate the user activities into 30 minute intervals, or leave it with the default setting.

8. You can choose to select the **Show internal calls** option to have the report include all internal call details.

Note:

The parameters you can set for this report are described in the following table.

Table 230: User Activity Summary Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.
Enter the extension, or range of extensions, you want to report on. You can add multiple extensions, or you can leave this field blank to report on all extensions	Click **Add** to add extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box.
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.

Parameter	Description
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.
Break report into 30 minute intervals	Select this check box to run interval reports in which each report is subtotaled by 30 minute intervals.
Show internal calls	Indicates whether you selected to include internal calls in the report. Values are either True (internal calls are included) or False (internal calls are not included.

Note:
When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

9. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

Note:

You can also select to include unanswered calls in the report (Unanswered calls are displayed with a talk time of zero.) For information about including unanswered calls in the report, see Configuring Reporting Options on page 959.

After the report is generated, you can print it, export it, or navigate it interctively, similar to compiled reports. The fields in the User Activity Summary Report are described in the following table.

Table 231: User Activity Summary Report Field Descriptions

Field	Description
Start Date	The start date as entered by you when generating the report. If you selected the **No lower limit** option for the date, the date field is left blank.
End Date	The end date as entered by you when generating the report. If you selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report.
Start Time	The start time as entered by you when generating the report. If you selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.
End Time	The end time as entered by you when generating the report. If you selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Show Internal Calls	Indicates whether you selected to include internal calls in the report. Values are either True (internal calls are included) or False (internal calls are not included.

Field	Description
Name	The name of the user who placed the call in the last Name, first Name, (extension number) format is displayed. For outbound calls, the Name (Extension) field of the Call record always reports the party that initiated the call. Inbound calls are reported according to the last party involved in the call (excluding voice mail and the auto-attendant). For example, if a call to extension 320 is not answered and the user's availability state forwards the call to his or her assistant at extension 452 who answers the call, the Extension field in the Call record contains 452. When an inbound call is forwarded to voice mail, the Name (Extension) field records the party involved in the call before it was forwarded to voice mail. For example, if a user with extension 320 doesn't answer a call and his or her availability state forwards the call to voice mail, the extension field is set to 320. The details for this field are retrieved from the PartyIDLastName, PartyIDName, and PartyID fields in the Connect table record. Non-users such as Workgroups, Voice Mail, Voice Mail Login, and Auto-attendant are also included in the report. The names for these extensions are reported for calls that only interact with these extensions (not a user extension). Like many other non-user extensions, the Mitel Audio Conference extension and Route Points are not displayed.

Field	Description
Inbound All: Qty Duration Average Duration	Indicates the quantity, total duration, and average duration for inbound calls during the reporting period. If the report is run with intervals, the call is only reported for the interval in which it started, even if it ends in a different interval. Duration represents the period that the specified user was on the call. Since a call is reported during the period in which it starts, but may end during another interval, the duration can be longer than the 30-minute interval period. Hence, the total call duration time is reported during the interval in which the call begins. Total Duration during any period is the sum of the duration for the Inbound calls during the period. Average duration is found by dividing the total duration by the number of calls during the period.
Outbound All: Qty Duration Average Duration	Indicates the quantity, total duration, and average duration for outbound calls during the reporting period. Duration is calculated in the same manner as for Inbound calls.
Total All: Qty Duration Average Duration	Indicates the quantity, total duration, and average duration of all calls during the reporting period. Inbound and Outbound quantity and total duration are added and averaged.
Outbound Non-Local Trunk: Duration Qty Average Duration	Indicates the quantity, total duration, and average duration for outbound non-local calls during the reporting period. The calls reported here, are a subset of the calls reported under Outbound all. Duration is calculated in the same manner as for Inbound calls.

Field	Description
Outbound WAN Trunk: Qty Duration Average Duration	Indicates the quantity, total duration, and average duration for outbound non-local calls during the reporting period. A call is considered a WAN call if a media stream was established between 2 sites. The calls reported here, are a subset of the calls reported under Outbound all. Duration is calculated here in the same manner as for Inbound calls.
Grand Total	Indicates the total number of calls, total duration, and average duration for all users.

24.2.7 Generating the WAN Media Stream Detail Report

The WAN Media Stream Detail Report displays details of each media stream placed over the WAN. You can configure the report to display information for all calls or for only inter-site calls. IP phone media streams are not included in this report.

To generate the WAN Media Stream Detail Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **User Activity Summary Report**.
4. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
5. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.
6. You can choose to view inter-site calls or all calls in the report by selecting the relevant option in the drop-down list.

Note:

The parameters you can set for this report are described in the following table.

Table 232: WAN Media Stream Detail Report Parameter Descriptions

Parameter	Description
Report Type	Indicates the type of report you want to generate.
Date range: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date). If you do not want to specify an end date, you can leave it as is (current date).
Time range: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is *(00:00)* or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is *(23:59)* or select the **No upper limit** check box.
Select the type of calls you want to report on	Indicates the type of calls you want to generate a report on. You can select Intersite to report only calls made between the sites. You can select **All calls** to report all calls made over the WAN.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

7. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled. The fields in the WAN Media Stream Detail Report are described in the following table.

Table 233: WAN Media Stream Detail Report Field Descriptions

Field	Description
Starting	The start date and time as entered by you while generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.

Field	Description
Ending	The end date and time as entered by you while generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Site A	The name of the site. This information is retrieved from the ASiteName field in the Media Stream table.
Site B	The name of the site that communicates with Site A. This information is retrieved from the BSiteName field in the Media Stream table.
Start Time	The time stamp and the date that the media stream started in MM/DD/YYYY HH:MM:SS 12-hour format. This information is retrieved from the StartTime field in the Media Stream table.
WAN	Indicates if the media stream accessed the WAN.
Call ID	The call identification number for the listed media stream. By matching the Call ID in the report to the Call ID of a WAN call with voice quality issues, you can understand the cause of the problems. This information is retrieved from the CallID field in the Media Stream table.

Field	Description
Encoding	Indicates the method of voice encoding used for the media stream. This information is retrieved from the EncodingType field in the Media Stream table. The Encoding field can have any of the following values: • AAC_LC32000 • ADPCM • ALAW) • BV16 • BV32 • CUSTOM • G722 • G729A • G729B • LINEAR • LINEARWIDEBAND • MULAW
Max Jitter	The maximum jitter encountered in milliseconds. This value is the maximum of the A MaxJitter or B MaxJitter for the corresponding record in the Media Stream table. If a significant number of calls are reported with a Max Jitter value close or equal to the Maximum Jitter Buffer value, it is recommended to increase the Maximum Jitter Buffer or investigate the cause of excess jitter in the network.
% Packets Lost	The number of packets that did not reach the destination and were probably dropped while traversing the network.
Duration	The duration of time the media stream was used across the WAN connection. This information is retrieved from the DurationSeconds field of the corresponding record in the Media Stream table.

24.2.8 Generating the WAN Media Stream Summary Report

The WAN Media Stream Summary Report displays a summary of call quality and call traffic for calls made over the WAN in multi-site deployments. By understanding the amount of time that the WAN is used for calls, you can estimate the amount of toll charges your organization is saving. In addition, by understanding the jitter and packet loss, you can get an approximation of the quality of the WAN link and use this to influence your service provider if required.

The report lists a matrix of all sites and the links to other sites on the system and summarizes media streams (not calls) between the two sites. Media streams can be for extensions or trunks. Calls can be quite complex involving multiple parties, including users, voice mail, and auto-attendant. Each media stream that is reported includes the associated Call ID (Call Identification) that can be correlated to the parties on the call for troubleshooting purposes using the CDR database.

You can configure the report to display information for all calls or for only inter-site calls. IP phone media streams are not included in this report.

To generate the WAN Media Stream Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **WAN Media Stream Summary Report**.
4. In the Date range section, enter the start date and end date for the report period, or accept the default values.
5. In the Time range section, enter the start time and end time for the report period, or accept the default values.
6. You can choose to view inter-site calls or all calls in the report by selecting the relevant option in the drop-down list.

Note:
The parameters you can set for this report are described in the following table.

Table 234: WAN Media Stream Summary Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.

Parameter	Description
Date range: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date). If you do not want to specify an end date, you can leave it as is (current date).
Time range: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (*00:00*) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (*23:59*) or select the **No upper limit** check box.
Select the type of calls youwant to report on	Indicates the type of calls you want to generate a report on. You can select *Intersite* to report only calls made between the sites. You can select All calls to report all calls made over the WAN.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

7. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the WAN Media Stream Summary Report are described in the following table.

Table 235: WAN Media Stream Summary Report Field Descriptions

Field	Description
Starting	The start date and time as entered by you while generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.
Ending	The end date and time as entered by you while generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Site A	The name of the site. This information is retrieved from the ASiteName field in the Media Stream table.
Site B	The name of the site that communicates with Site A. This information is retrieved from the BSiteName field in the Media Stream table.

Field	Description
Quality: Avg Jitter (ms) Max Jitter (ms) % Packets Lost Blocked Calls	The quality of the media streams between the sites in terms of the maximum and average jitter, percentage of packets lost, and number of blocked calls. The average of the maximum per-media stream jitter between the sites in milliseconds. This information is retrieved from the A MaxJitter and B MaxJitter fields in the Media Stream table. The maximum jitter encountered on any media stream between the sites in milliseconds. This information is retrieved from the A MaxJitter and B MaxJitter fields in the Media Stream table. The jitter buffer should be larger than this value for proper operation. The **Max Jitter** value in this report is only recorded up to the maximum jitter buffer value configured on Connect Director. The number of packets that did not reach the destination and were probably dropped while traversing the network. The number of calls that were not routed across the WAN due to insufficient WAN bandwidth (admission control reached). This could indicate that more WAN bandwidth is required. This is a count of the number of records in the Media Stream table between the two sites with FailureCode = 1 (Admission Control Inhibited Call).

Field	Description
Traffic Volume: Total Duration Avg Duration	The amount of traffic between the two sites in terms of number of media streams, duration and average duration of the streams. The number of media streams used between the two sites as recorded in the Media Stream table. The duration of all the media streams used between the two sites. The value is the sum of duration for all records between the two sites in the Media Stream table. The average duration of all the media streams used between the two sites. The value is calculated by dividing the total duration of the media streams between the two sites by the number of such media streams.

24.2.9 Generating the Workgroup Agent Detail Report

The Workgroup Agent Detail Report shows a list of every call for every agent in a workgroup.

This report includes calls routed to workgroup agents by the workgroup server, and non-workgroup calls (both inbound and outbound). The report assigns non-workgroup calls to an agent's membership within a workgroup by examining the workgroup the agent was logged into during or before the call. Non-workgroup calls made while an agent is logged out are not reported.

Workgroup agents can be a member of more than one workgroup. When they log in, their login time is reported for all workgroups of which they are a member. Non-workgroup calls are reported for the workgroup with the lowest dial number that the agent is a member of when the call is made. For example, if the agent is a member of workgroups with dial numbers of 1100, 1200, and 1250, non-workgroup calls are reported against 1100.

To generate the Workgroup Agent Detail Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the Report type drop-down list, select Workgroup Agent Detail Report.

4. Do one of the following:
   - Specify the workgroup extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all workgroup extensions, proceed with Steps 5 to 11.
5. Do one of the following:
   - Specify the agent extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all agent extensions, proceed with Steps 6 to 11.
6. In the date range section, enter the start date and end date for the report period, or accept the default values.
7. In the time range section, enter the start time and end time for the report period, or accept the default values.
8. You can choose to select the **Break report into 30 minute intervals** option to segregate the user activities into 30 minute intervals in the report, or leave it with the default setting.
9. You can choose to select the **Show internal calls** option to include all internal call details in the report, or leave it unselected.
10. You can choose to select the **Show outbound calls** option to include all outbound call details in the report, or leave it unselected.

Note:
The parameters you can set for this report are described in the following table.

Table 236: Workgroup Agent Detail Report Parameter Descriptions

Parameter	Description
Report Type	Describes the type of report you want to generate.

Parameter	Description
Enter the workgroup extension, or range of extensions, you want to report on. You can add multiple workgroup extensions, or you can leave this field blank to report on all workgroups	Click **Add** to add workgroup extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box. **Note**: If you are using on-net dialing, enter the workgroup number with the dash. For example, enter 12-345 instead of 12345. If you do not do this, the generated report can turn up blank, without the required entries.
Enter the agent extension, or range of e xtensions, you want to report on. You ca n add multiple agent extensions, or you can leave this field blank to report on all agents	Click Add to add extension numbers of the agents for which you w ant to generate the report or leave blank to report on all extensions.
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.

Parameter	Description
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.
Break report into 30 minute intervals	Select this check box to run interval reports in which each report is subtotaled by 30 minute intervals.
Show internal calls	Select this check box to include internal calls in the report.
Show outbound calls	Select this check box to include outbound calls in the report.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM)

11. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Workgroup Agent Detail Report are described in the following table.

Table 237: Workgroup Agent Detail Report Field Descriptions

Field	Description
Start	The first **Start** field indicates the start date as entered prior to generating the report. If you selected **No lower limit** when generating this report, this field is left blank. The second **Start** field indicates the start time as entered prior to generating the report. If you selected **No lower limit** when generating this report, this field is left blank. If you did not enter a specific value, this field displays the default start time of *12:00 AM*.
End	The first **End** field indicates the end date as entered prior to generating the report. If you selected **No upper limit** when generating this report, this field is left blank. If you did not enter a specific date, this field displays the default date (typically the date that you generated the report). The second **End** field indicates the end time as entered prior to generating the report. If you selected **No upper limit** when generating this report, this field is left blank. If you did not enter a specific value, this field displays the default end time of *11:59 PM*.
Workgroup	Workgroup name with extension for which you generated the report.
Agent	Name of the workgroup agent with extension number.
Date/Time	The date and time for the call being reported. The date is displayed in MM/DD/YYYY format. The time is displayed in HH:MM:SS 12-hour format. When interval reports are generated, the call is reported for the time when it starts even if it extends into another interval.

Field	Description
Dialed #	The number dialed to initiate the call. For inbound calls, this is the destination number of the call. If the call was a DID or DNIS call, this is the DID or DNIS information for the number dialed. For other types of calls, this is the extension number where the call first terminates.
Calling #	The caller who initiated the call. For inbound calls, this is the calling number—ANI or Caller ID—received by the Mitel system and is reported as delivered by the PSTN (may or may not include the **1** before the area code).
Call Type	Indicates whether this is an incoming workgroup call (**InWG**), an inbound non-workgroup call (**In**), or an outbound call (**Out**). A call is categorized as an inbound workgroup call if the user joined the call as a workgroup agent. This is determined by examining the PartyType field in the Connect table (must be 12 for a Workgroup Agent). A call is categorized as an inbound non-workgroup call if • The value of the CallType field in the Call table is 1 (internal) or 2 (inbound) • The value of the PartyType field is 1 (station) • The user was not the originator of the call, which is indicated by the ConnectReason field in the Connect table not being equal to 19

Field	Description
Call Type (continued)	A call is categorized as outbound if • The value of the CallType field in the Call table is 1 (internal) or 3 (outbound) • The user originated the call, which is shown by the ConnectReason field in the Connect table having a value of 19 **Note**: For all calls, calls with CallType value of 1 (internal) are included only if the option to include internal calls is chosen. Calls that involve multiple extensions are also reported as: • **Transfer**: Transferred call • **Conference**: Conference call • **Monitor**: Monitored call • **Barge-In**: Barged call
Trunk	The first trunk that was used for the call. This information is retrieved from the PortName field of the Connect record for the trunk used in the call. In the case of calls not using a trunk, the field is left blank (this can occur with internal calls).
Call Duration	The duration of the call in HH:MM:SS 12-hour format. Duration defined the time period that the user was on the call.This information is collected by adding the TalkTime and HoldTime fields in the Connect record for the call. Since a call is reported during the period in which it starts (as identified by the StartTime field in the Call table) but can end during another interval, the duration can be longer than the 30 or 60 minute interval. The total duration is reported during the interval in which the call begins.

Field	Description
Wrapup Duration	The amount of time, if any, the agent spent in wrapping up after completing the call. The duration is displayed in HH:MM:SS 12-hour format.This is applicable to only inbound workgroup calls. The Wrap-up Duration is the difference between the StartTimeStamp and EndTimeStamp in the Agent Activity table for that agent.
Queue Duration	The amount of time that the call was in the workgroup queue before it was assigned to the agent. The duration is displayed in HH:MM:SS 12-hour format.This is applicable only to inbound workgroup calls. This information is retrieved from the Duration field of the Queue Call table.
Total Duration	The total duration that is a sum of the Queue Duration, Call Duration, and Wrap-up Duration in HH:MM:SS 12-hour format. This value is generally lesser than the total time the call spends within the Mitel system. The period between the moment the trunk was seized and the call was accepted by the workgroup, or any time the call spends with a menu or other extension, is not reflected.
Sub Total	The total number of calls for a workgroup agent.
Total	The total number of calls for all agents in a workgroup.
Grand Total	The total number of calls for all agents in the system.

24.2.10 Generating the Workgroup Agent Summary Report

The Workgroup Agent Summary report displays a summary of inbound workgroup calls and agent activity for each workgroup.

The report includes calls routed to workgroup agents by the workgroup server, and non-workgroup calls (both inbound and outbound). Workgroup agents can be a member of more than one workgroup. When they log in, their login time is reported for all workgroups of which they are a member. Non-workgroup calls are reported against the

workgroup with the lowest dial number that the agent is a member of when the call is made. For example, if the agent is a member of workgroups with dial numbers of 1100, 1200, and 1250, non-workgroup calls are reported against 1100.

The report assigns non-workgroup calls to an agent's membership within a workgroup by examining the workgroup the agent was logged into during or before the call. No calls are reported when an agent is logged out.

While the summary report displays agent activity, which consists of agent wrap-up and login time, the report displays this information only for periods that had a call for the agent (workgroup or non-workgroup).

To generate the Workgroup Agent Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Workgroup Agent Summary Report**.
4. Do one of the following:
   - Specify the workgroup extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all workgroup extensions, proceed with the next step.
5. Do one of the following:
   - Specify the agent extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all agent extensions, proceed with Steps 6 to 10.
6. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
7. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.

8. You can choose to select the **Show internal calls** option to include all internal call details in the report, or leave it with the default setting.
9. You can choose to select the **Show outbound calls** option to include all outbound call details in the report, or leave it with the default setting.

Note:

The parameters you can set for this report are described in the following table.

Table 238: Workgroup Agent Summary Report Parameter Descriptions

Parameter	Description
Report Type	Describes the type of report you want to generate.
Enter the workgroup extension, or range of extensions, you want to report on. You can add multiple workgroup extensions, or you can leave this field blank to report on all workgroups	Click **Add**to add workgroup extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box. **Note**: If you are using on-net dialing, enter the workgroup number with the dash. For example, enter 12-345 instead of 12345. If you do not do this, the generated report can turn up blank, without the required entries.
Enter the agent extension, or range of extensions, you want to report on. You can add multiple agent extensions, or you can leave this field blank to report on all agents	Click Add to add extension numbers of the agents for which you want to generate the report or leave blank to report on all extensions.

Parameter	Description
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.
Report interval	Select the interval at which to run reports. Each report is subtotaled by the se lected interval.
Show internal calls	Select this check box to include internal calls in the report.
Show outbound calls	Select this check box to include outbound calls in the report.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

10. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Workgroup Agent Summary Report are described in the following table.

Table 239: Workgroup Agent Summary Report Field Descriptions

Field	Description
Start Date	Indicates the start date as entered by you while generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank.
End Date	Indicates the end date as entered by you while generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report.
Start Time	Indicates the start time as entered by you while generating the report. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00 AM**.
End Time	Indicates the end time as entered by you while generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59 PM**.
Duration format	Indicates the format used while displaying the duration.
Workgroup	Workgroup name and extension for which you generated the report.

Field	Description
Agent	Name of the workgroup agent with extension number.
Inbound Workgroup Calls: Qty Duration Average Duration	The quantity, total duration, and average duration for all inbound workgroup calls during the reporting period. Average duration is calculated by dividing total duration by the reported quantity for a workgroup.
Inbound user Calls: Qty Duration Average Duration	The quantity, total duration, and average duration for all inbound user calls during the reporting period. Average duration is calculated by dividing total duration by the reported quantity for a user.
Outbound Calls: Qty Duration Average Duration	The quantity, total duration, and average duration for all outbound user calls during the reporting period. Average duration is calculated by dividing total duration by the reported quantity.
Other Calls: Qty Duration Average Duration	The quantity, total duration, and average duration for all other calls during the reporting period. A call is considered to be categorized as other if the call is neither inbound nor outbound. Average duration is calculated by dividing total duration by the reported quantity.
Total Calls: Qty Duration Average Duration	The quantity, total duration, and average duration of all calls during the reporting period. Total calls are the sum of all inbound, outbound and other calls. Average duration is calculated by dividing total duration by the reported quantity.

Field	Description
Agent Activity: Total Wrapup Average Wrapup Total Login	Agent action time during the reporting period in terms of total wrapup time, average wrapup time, and total login time. The total login time is the period for which an agent was logged in as a workgroup agent and had received at least one active call.

24.2.11 Generating the Workgroup Queue Summary Report

The Workgroup Queue Summary Report displays a summary of queue activity and how the calls are managed in a queue. The key determinant in this report is the workgroup server that processes the call.

When a workgroup server processes a call, a record about the call status is added to the Queue Call table. In most cases the call is recorded just once, but if forwarded, a call can be recorded twice. When a call comes in it is processed by the server where it is routed to an agent. The caller then chooses to go to voice mail or another destination, or hangs up (abandons the call) before it is routed beyond the workgroup. Since the report shows how the call was disposed of by the workgroup server, the call is reported once in the report. However, if the call is forwarded, the same call can pass through the workgroup server more than once. For example, a call goes to a workgroup server. While on the call, the user transfers it to another extension. The user extension availability state forwards the call to the same or a different workgroup. In this case, the call passes through the workgroup server more than once and is reported each time the workgroup server processes the call. For each time the workgroup server processes the call, a record is added to the Queue Call table.

External calls to a workgroup are always included in the report. Internal workgroup calls are only included in the report if the option to include them is enabled. (The default setting is to not include them.)

If the workgroup service is not operational, the call is not processed by the workgroup server (it simply goes to the backup extension) and not included in the report. When this occurs, there is no record of the call in the Queue Call table, since records are only added to that table when the workgroup server processes the call.

To generate the Workgroup Queue Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Workgroup Queue Summary Report**.

4. Do one of the following:
   - Specify the extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all workgroup extensions, proceed with Steps 5 to 9.
5. In the date range section, enter the start date and end date for the report period, or accept the default values.
6. In the time range section, enter the start time and end time for the report period, or accept the default values.
7. You can choose to select the **Break report into 30 minute intervals** option to segregate user activities into 30 minute intervals in the report, or leave it unselected.
8. You can choose to select the **Show internal calls** option to include all internal call details in the report, or leave it unselected.

Note:

The parameters you can set for this report are described in the following table.

Table 240: Workgroup Queue Summary Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.

Parameter	Description
Enter the extension, or range of extensions, you want to report on. You can add multiple extensions, or you can leave this field blank to report on all extensions	Click **Add** to add workgroup extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box. **Note**: If you are using on-net dialing, enter the workgroup number with the dash. For example, enter 12-345 instead of 12345. If you do not do this, the generated report can turn up blank, without the required entries.
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.

Parameter	Description
Break report into 30 minute inte rvals	Select this check box to run interval reports in which each report is subtot aled by 30 minute intervals.
Show internal calls	Select this check box to include internal calls in the report.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

9. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Workgroup Queue Summary Report Field Report are described in the following table.

Table 241: Workgroup Queue Summary Report Field Descriptions

Field	Description
Workgroup	Workgroup name and extension for which you generated the report.
Start Date	The start date as entered by you prior to generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank.

Field	Description
End Date	The end date as entered by you prior to generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report.
Start Time	The start time as entered by you prior to generating the report. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.
End Time	The end time as entered by you prior to generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Abandoned	Calls abandoned for the workgroup. The numbers indicate callers who hung up or disconnected while waiting in queue.
Handled by Agent	The number of calls that were answered by agents in the workgroup.
Handled by WG Voice Mail	Number of calls that went to the workgroup voice mail (either as a result of call routing or when the caller chose to transfer to voice mail).
Queue Transfer	Number of calls transferred by Workgroup agents.

Field	Description
Queue Overflow / Interflow	Number of automatic call transfers, based on caller wait time to a dial-able number (interflow), or to another Workgroup queue (overflow).
Handled by Others	Number of calls handled by others (not workgroup agents or voice mail). Any call for the workgroup that is not reported as Abandoned, Handled by Agent, Picked Up from the Queue, Unparked from the Queue, or Handled by Voice Mail is counted as Handled by Others.
Maximum Abandon Time	The maximum time that a caller stayed on the line before abandoning the call.
Average Abandon Time	The average time during the period that those callers who abandoned the call stayed on the line.
Maximum Handled Time	The maximum time during the period that a caller stayed on the line before the call was handled (by agent, voice mail, or others). **Note**: The maximum time could be zero even though there were handled calls in the case of the call being forwarded immediately to voice mail.

Field	Description
Average Handled Time	The average time during the period that a caller was on the line before the call was handled (by an agent, voice mail, or others). **Note**: The average time could be zero even though there were handled calls in the case of the call being forwarded immediately to voice mail.
Total Calls	All calls processed by the workgroup. This includes calls that go straight to agents without waiting in queue. The information for this field is retrieved by the sum of the following types of calls: • Abandoned • Handled by Agent • Handled by Voice Mail • Handled by Others

24.2.12 Generating the Workgroup Service Level Summary Report

The Workgroup Service Level Summary report provides information related to the workgroup server call processing. Every time the workgroup server processes a call, a record about the call status is added to the Queue Call table. Generally, this occurs once when the call gets processed by the server. However, in the case of call forwarding, the same call can pass through the workgroup server more than once. For example, when a call made to the workgroup server is transferred to an extension. If that extension's availability state forwards the call to the same or a different workgroup, the call passes through the workgroup server more than once. The rule in these cases is simple—every time the workgroup server processes a call, a record is added to the Queue Call table.

The report always includes external calls to a workgroup. Internal workgroup calls are included in the report only if the option to include them is selected (the default is not included).

If the workgroup service is not operational, the call is not processed by the workgroup server (it simply goes to the backup extension) and is not included in this report. When this occurs, there is no record of the call in the Queue Call table since records are only added to the table when the workgroup server processes the call.

To generate the Workgroup Service Level Summary Report:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Call Details**.
3. In the **Report type** drop-down list, select **Workgroup Service Level Summary Report**.
4. Do one of the following:
   - Specify the extensions for which you want to generate the report, as follows:
     - To enter a specific extension, click **Add** and specify that extension in both the **Start of range** and **End of range** fields. Repeat this step if you want to add more extensions.
     - To enter a range of extensions, click **Add** and specify the lowest extension in the **Start of range** field and the highest extension in the **End of range** field, or leave either field blank. Repeat this step if you want to add more extension ranges.
   - To generate a report for all workgroup extensions, proceed with the next step.
5. In the **Date range** section, enter the start date and end date for the report period, or accept the default values.
6. In the **Time range** section, enter the start time and end time for the report period, or accept the default values.
7. You can choose to select the **Break report into 30 minute intervals** option to segregate user activities into 30 minute intervals in the report, or leave it with the default setting.
8. You can choose to select the **Show internal calls** option to include all internal call details in the report, or leave it with the default setting.

Note:

The parameters you can set for this report are described in the following table.

Table 242: Workgroup Service Level Summary Report Parameter Descriptions

Parameter	Description
Report Type	The type of report you want to generate.

Parameter	Description
Enter the extension, or range of ext ensions, you want to report on. You can add multiple extensions, or you can leave this field blank to report on all extensions	Click **Add** to add workgroup extension numbers for which you want to generate the report or leave blank to report on all extensions. Enter the start range in the **Start of range** field and the end of range in the **End of range** field. If you do not want to specify a start range, you can leave it as is or select the **No lower limit** check box. If you do not want to specify an end range, you can leave it as is or select the **No upper limit** check box. **Note**: If you are using on-net dialing, enter the workgroup number with the dash. For example, enter 12-345 instead of 12345. If you do not do this, the generated report can turn up blank, without the required entries.
Enter the date range you want to report on: Date start Date end	Start and end date to define the days for which you want the report generated. If you do not want to specify a start date, you can leave it as is (current date) or select the **No lower limit** check box. If you do not want to specify an end date, you can leave it as is (current date) or select the **No upper limit** check box.

Parameter	Description
Enter the time range you want to report on: Time start Time end	Start and end time (in 24-hour format) to define the time period for each day that you want the report generated. If you do not want to specify a start time, you can leave it as is (00:00) or select the **No lower limit** check box. If you do not want to specify an end time, you can leave it as is (23:59) or select the **No upper limit** check box.
Maximum wait time	Select the maximum time that the workgroup server can take before processing the call in its queue. You can enter a value between 30 seconds to 10 minutes.
Break report into 30 minute intervals	Select this check box to run interval reports in which each report is su btotaled by 30 minute intervals.
Show internal calls	Select this check box to include internal calls in the report.

Note:

When you specify a start time and an end time, the report is generated between the specified range for each day. For example, if the start time is 10:00 (10:00 AM) and the end time is 22:00 (10:00 PM), the report is generated only for this period every day. If you want the reports generated for the entire day, every day, then use the default start time of 00:00 (12:00 AM) and the default end time of 23:59 (11:59 PM).

9. Click **Run report**.

Note:

The report is generated and is displayed in a different browser tab.

After the report is generated, you can print it, export it, or navigate it interactively, similar to compiled reports. The fields in the Workgroup Service Level Summary Report are described in the following table.

Table 243: Workgroup Service Level Summary Report Field Descriptions

Field	Description
Start Date	The start date as entered by you prior to generating the report. If you had selected the **No lower limit** option for the date, the date field is left blank.
End Date	The end date as entered by you prior to generating the report. If you had selected the **No upper limit** option for the date, the date field is left blank. If you did not enter a specific date, the date field displays the date of generating the report.
Start Time	The start time as entered by you prior to generating the report. If you had selected the **No lower limit** option for the time, the time field is left blank. If you did not enter a specific value for time, the time field displays the default start time of **12:00:00 AM**.
End Time	The end time as entered by you prior to generating the report. If you had selected the **No upper limit** option for time, the time field is left blank. If you did not enter a specific time, the time field displays the default end time of **11:59:59 PM**.
Max. Wait Time	The maximum time that the workgroup server can take before processing the call in its queue.
Workgroup	Workgroup name and extension for which you generated the report.

Field	Description
Date	Date in Month DD, YYYY format when the call was processed by the workgroup server.
Wait Time	Range of wait-for-service time in seconds for the workgroup for processing a call in its queue. The wait time is divided into 30-second intervals. Information for the calls is reported for the interval in which it falls, according to when the call moved off the workgroup. The duration is recorded from the time that the call is offered to the workgroup server until it leaves the call queue.
Abandoned	Number of callers who abandoned the call (hung up) during the period.
Handled by Agent	Number of calls handled by agents during the period. **Note**: A call that is picked up or unparked by an agent who is a member of the same workgroup is also counted as Handled by Agent.
Handled by Voice Mail	Number of calls that were sent to the workgroup voice mail (either as a result of call routing, or when the caller chose the transfer to voice mail option).
Queue Transfer	Number of calls transferred from the workgroup queue. For example, this would include any calls that are transferred from the workgroup queue to another destination.
Queue Interflow / Overflow	Number of automatic call transfers, based on caller wait time to a dial-able number (interflow) or to another Workgroup queue (overflow).

Field	Description
Handled by Others	Number of calls handled by others (neither workgroup agents nor voice mail). Any call for the workgroup that is not reported as Abandoned, Handled by Agent, or Handled by Voice Mail is counted as Handled by Others. Calls that are picked up by non-agents, or agents who do not belong to the group are counted as Handled by Others.
Total Calls	Total number of calls, which is the sum of the following type of calls: • Abandoned • Handled by Agent • Handled by Voice Mail • Picked Up from the Queue • Unparked from the Queue • Handled by Others for the period.

24.3 Web Conference Reports

You can generate Web Conference reports by using Connect Director from a local host or a remote server. You can use the Connect Director to generate the Concurrent Web Port Usage Report, in addition to the Web Conference Report on this page.

To generate Web conference reports:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Reports** > **Web Conference**.

   The Web Conference home page is displayed.
3. Click the appliance for which you want to generate the reports.

Note:

The **Web Conference Reports** page is displayed. You can view the **Concurrent Web Port Usage Report** on this page, in addition to the Web Conference Report.

4. Do one of the following:

- Click **Concurrent ports**, specify the following options, and click **Go** to view the Concurrent Web Port Usage Report:
  - From the **Time zone** drop-down menu, select the time zone in which you want the report generated.
  - From the **Show** drop-down menu, select the reporting period.
  - Select the appliance, for which you want the report generated.

Note:

The resulting report is displayed on the screen.You can click **Download** to download the report in a CSV file format to your local drive.

- Click **Conference sessions**, specify the following options, and click **Go** to view the Web Conference Report:
  - On the **Time zone** drop-down menu, select the time zone in which you want the report generated.
  - On the **Show conference sessions for** drop-down menu, select the reporting period.
  - Select the appliance, for which you want the report generated.
  - In the **Access Code** field, enter the access code you want to report on, and click **Search** to view and select the required code. If you leave this field blank, the report is generated for all access codes.

Note:

The resulting report is displayed on the screen. You can click **Download** to download the report in a CSV file format to your local drive.

The fields in the Web Conference Reports are described in the following table.

Table 244: Web Conference Report Field Descriptions

Field	Description
Session	The web conference session for which the report is generated.
Date	The date that the web conference session was held.
Time	The time that the web conference session was initiated.
Duration	The duration of the reported web conference.
Name	Name of the web conference. This usually describes the agenda of the conference, for example, Sales Weekly, Marketing Report, and so on.
Access Codes	Code assigned to a scheduled web conference that attendees must enter to join.
Hosted by	Name of the user who hosted the web conference.
Participants	Names of users who logged into the conference as attendees, by using the access code.

24.4 Configuring Reporting Options

You can configure the following options while generating reports:

- **Sending Call Detail Reports / Call Data Records (CDRs) through the serial (COM) port of the server:** The Mitel system supports the ability to send CDR data out of a serial port on the main server. The **Reporting Options** page allows you to designate the COM port to be enabled. CDR data is subsequently sent out this port, in addition to being sent to the regular text file and/or a database. Sending the CDR data out the serial port does not alter the formatting of the data.
- Enabling the creation of archive database for CDRs

The parameters you can configure to enable these options are described in the following table.

Table 245: Reporting Options parameter Descriptions

Parameter	Description
COM Port for CDR output	Select the COM port on the Headquarters server from which you want to send out the CDR data. You can select a value from 1 to 10. If you do not want to send the CDR through the COM port, select **<None>**, which is also the default. The Mitel system captures CDRs in a database in a text-file format. However, for legacy call accounting systems that cannot read CDR from a database, the CDR data can be delivered as a Station Messaging Detail Record (SMDR) using a serial (COM) port on the main server. When using SMDR, the following applies: • Formatting of the CDR data remains the same, regardless of whether it is sent out the COM port or written to the database. • The application should auto-detect the serial port configuration by extracting information about the status of the serial port configuration, for example the baud rate, from the Windows registry. • The feature will be disabled by default and must be enabled by selecting a COM port. • If the serial port should become unavailable through an event such as becoming locked by extremely high volumes of traffic, the CDR data will be queued in a buffer for 300 seconds to help prevent the loss of data. If the serial port returns to service within the 300-second time period, the streaming resumes.

Parameter	Description
Retention period for CDR data	The period for which you want the CDR data retained in the Mitel system. You can select a value from 1 to 2000 days. The default value is 36 days.
Enable CDR archiving	Enables the creation of an archive database for CDR data.
Retention period for CDR archive	The period for which you want the CDR archive retained in the database. You can select a value from 1 to 2000 days. The default value is 125 days.
Archive database name	The name of the archive database. **Note**: Saving the name of the database does not create the archive database. For information about creating an archive database, see Creating a CDR Archive Database on page 1000.
Archive database IP address	The IP address of the server on which the archive database must be saved.

Parameter	Description
Select Language Variant	The field specifies the languages that is supported on the computer running Director. Mitel supports the following Asian languages: • Japanese • Simplified Chinese • Traditional Chinese **Note**: Only one set of files, which supports one language, can be installed on a computer at a time.
Include unanswered calls	Includes unanswered calls in the reports with a duration of zero.

To configure Reporting Options:

1. Launch Connect Director.
2. In the navigation pane, click **Reporting** > **Report Options**.
3. To send the CDR data through the serial (COM) port of the server, select the respective port number from the **COM port for CDR output** drop-down list. If you do not want to configure this option, proceed to the next step.
4. Enter the duration for which you want to retain the CDR data on the Mitel system. If you do not enter a value, the default value of 36 days is selected.
5. To enable the creation of a CDR archive database, select the **Enable CDR archiving** option. If you select this option, you must follow the steps outlined in Creating a CDR Archive Database on page 1000 to create the archive database. If you do not select this option, you can proceed to Step 9 to complete configuring the reporting options.
6. Enter the duration for which you want to retain the archive database on the Headquarters server. If you do not enter a value, the default value of *125* days is selected.

7. Enter the name of the archive database you want to create for CDR data. The name you enter here must match the one you use while creating the archive database as outlined in .
8. Enter the IP address of the Headquarters server on which you are going to create the archive database.
9. Select the Asian language variant to be installed on your system. If you do not select a value, *Simplified Chinese* is selected by default.
10. Click **Install font** to install the selected font on your system. The executable file is downloaded to your system, which you can open and run to complete the font installation.
11. You can choose to select the **Include answered calls** option to include all unanswered calls in all reports. By default, unanswered calls are not included in the report.

Emergency Dialing Operations 25

This chapter contains the following sections:

This chapter explains the chain of events in the call flow when a emergency call is placed. This chapter also provides instructions for configuring your Mitel system to ensure that emergency services are dispatched to the correct location. And finally, the chapter tells you how to select which of the various pieces of caller ID information will be used to identify callers when an emergency call is placed.

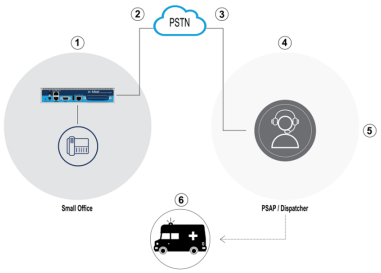
25.1 How Emergency Calls Work

This section provides a simple scenario to illustrate how emergency calls are handled with the Mitel system.

With Emergency Services support, when an emergency number is dialed, the Caller's Emergency Service Identification (CESID) is sent from the system to the service provider; who then forwards the call to the Public Safety Answering Point (PSAP). The CESID is used as a key in the Automatic Location Information (ALI) database. The ALI database displays the precise location of the caller, as well as emergency services information identifying the proper medical, fire, or law enforcement agency for the location. It is important to ensure that you communicate all CESID changes to the ALI database and always keep it updated.

The following figure displays a simple emergency call-flow scenario.

Figure 23: Simplified Emergency Call Flow Scenario



25.1.1 Emergency Call Scenario

The following is a description of the call flow depicted in Simplified Emergency Call Flow Scenario.

1. An emergency call is placed from a desk phone.
2. The Mitel system identifies the call as an emergency call and automatically routes it to an outbound trunk along with the CESID. The CESID is provided by Public Switched Telephone Network (PSTN) service provider or by any other Emergency service provider. The CESID is provided in either of the following ways:
   - If the call is sent over a PRI trunk, the Mitel system provides the CESID, which it obtained from the PSTN service provider, to the PSAP.
   - If the call is sent over a non-PRI trunk, the Mitel system provides the CESID it obtained from respective service provider to the trunk service provider, who then shares with the PSAP, necessary for identifying the location.
3. The call is routed by the service provider.
4. The service provider passes the call to a PSAP. This is the location to which emergency services will be dispatched.
5. The Automatic Location Information (ALI) database at the PSAP gets a “screen pop”, which displays information obtained from an emergency database. The emergency database contains a mapping between the caller ID number and the geographic location of the caller.
6. The dispatcher sends emergency response personnel to the calling party’s location.

Note:
PSAP maintains only one location information per CESID/caller ID. Therefore, for emergency calls placed from residential or a single-site business locations, determining the location of the calling party is simple and straightforward. However, when dealing with large offices and campus environments, the emergency configuration can get complex and might require more CESID with increased solution cost. If you are maintaining a configuration that has many remote sites, it is imperative that you do the following:

- Keep your emergency information current with your PSAP or the Emergency service provider.
- Work with your service provider to find out what kinds of CESID information they will accept.
- Work with the local PSAP/ Emergency service provider to ensure that any changes in your emergency configuration (that is, names, phone numbers, and locations of the members) are mirrored in the appropriate location service database.

25.1.2 RAY BAUM'S Act Overview

RAY BAUM'S Act is introduced in the US to ensure that proper and accurate dispatchable location information is conveyed when emergency 911 calls are made so that first responders can locate the caller quickly and accurately. The dispatchable location identifier is defined as "the civic address of the calling party and includes information such as room number, floor number, or similar information necessary to accurately identify the location of the calling party".

As per the RAY BAUM'S Act, Multi-line Telephone Systems (MLTS) must ensure to provide Public Safety Answering Point (PSAP) with the dispatchable location conforming to above definition for emergency 911 calls for identifying the location of the calling party. This information includes floor-level for multifloor installations and quadrant-level information for large buildings. When an emergency call is made, the location information can be provided directly by phones or, MLTS can provide location information based on the configuration.

In MiVoice Connect, when the RAY BAUM feature is enabled, the location information during an emergency call made is provided automatically only by the soft client. For all other endpoints, MiVoice Connect will derive the location based on the configuration and communicate it to the appropriate PSAP.

With RAY BAUM, the dispatchable location should be granular; therefore, with limited number of CESIDs, not all offices can comply without changing the existing model. The MiVoice Connect Ray Baum feature helps customers comply with the RAY BAUM'S Act. Features such as improvements to the existing CESID mapping methods as well as

a possible integration with third-party emergency service provider vendors have been included to mainly to address off-premises endpoints.

There are a few options customers will have on how they implement their solution to meet the RAY BAUM'S Act. The option selected must be primarily with regard to the type of deployment in place, such as:

- Size of the physical location site. If small enough, it might imply one dispatchable location.
- Deployment is purely on premises.
- On-premises deployment includes wireless devices.
- Deployment includes off-premises endpoints.

Depending on the solution, customer might:

- Not need to upgrade, but rather use existing CESID mappings to allow for automatic move detection of IP phones.
- Have to upgrade to get the new CESID mappings described in this document, but are not required to integrate with a third-party vendor.
- Have to upgrade to get the new CESID mappings described in this document and will be required to integrate with a third-party vendor.

1. Customer has only on-premise IP4xx and/or 69xx and/or DECT devices. In this situation, the customer can purchase one or more CESIDs from their PSTN service provider, so as to cover the entire location with required granularity and use the existing IP range and/or L2 CESID mapping features available on the MiVoice Connect without the need for any upgrade. Enabling these features provides a dynamic location update should the device be moved by the user within the premises.
2. If the CESIDs cost more, then customer will have to upgrade and integrate with a Mitel-verified third-party vendor based on cost comparison.
3. If the customer adds MiVC Connect Client softphones on laptops/mobiles or any kind of remote Teleworkers to their solution, the customer will have to upgrade and integrate with a Mitel-verified third-party vendor.

Whichever deployment model is selected, MiVoice Connect will act as a facilitator for administrators to configure and manage the location information of the endpoints. It is the responsibility of the administrators to configure the location information appropriately.

25.1.2.1 MIVC Support for Section 506 of RAY BAUM'S Act and Kari´s Law

MiVoice Connect implements Section 506 of RAY BAUM'S Act and Kari´s law support in conjunction with third-party Next Generation of 911 (NG911) emergency service providers.

MiVoice Connect is integrated with two well-known Next Generation 911 (NG911) service providers in USA; RedSky and Intrado.

MiVoice Connect can be preconfigured for direct dialing of emergency 911 calls without having to dial any prefix or access code. The 911 calls are sent through SIP trunk to the NG911 service provider selected by the customer and then, after validating the civic address, the call is redirected to the public safety answering points (PSAPs).

The notification system is provided by the NG911 service provider and uses email or SMS notifications.

MiVoice Connect has an Emergency Notification application that provides notification in emergency scenario to dedicated users, and this can be used in conjunction with NG911 notification through email or SMS messaging. Mitel Emergency application provides location information based on the Jack number configuration in Connect Director and the NG911 service provider notification will provide location information based on what is configured in the location information service (LIS) database and presents it to the PSAPs. If the administrator can sync the dynamic location properly to the **Jack #** field in the **Users** page in Connect Director, then the existing emergency application can also satisfy Kari's law.

25.1.2.2 Prerequisites for Enabling RAY BAUM

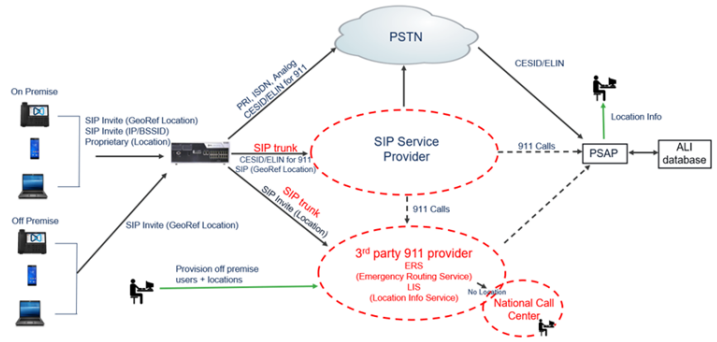
The following are the prerequisites that must be met before you can enable RAY BAUM in your MiVoice Connect system:

- Before you upgrade the MiVoice Connect to 19.2 SP2 version, you must ensure that the network is set up appropriately (identified the CESID and the IP address ranges) based on the location. Follow the instructions provided in the *MiVoice Connect RAY BAUM General Overview and Solution Deployment Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.
- Uprgade the MiVoice Connect to 19.2 SP2 version.
- Make the configuration changes for Ray Baum. For more information, see the *MiVoice Connect RAY BAUM General Overview and Solution Deployment Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

25.1.2.3 RAY BAUM 911 Third-Party Emergency Service Provider Deployment and Call Flow

MiVoice Connect Deloyment illustrates the MiVoice Connect deployment with third-party emergency service provider.

Figure 24: MiVoice Connect Deloyment



Call Flow Details

1. System administrator configures the location information for the vendor and associates it with a different location for each user-defined CESID value. CESID is the 10-digit number as prescribed by the US law. The information will be stored in the location information service (LIS) database of the server.
2. System administrator configures the vendor with information about one or more predetermined locations. Each individual location is then associated with different and unique user-defined CESID value. In US, the CESID is a 10-digit number. This information will be stored in the location information service (LIS) database of the server.
3. The system administrator configures MiVoice Connect with the CESID obtained from the preceding steps. The CESID can be configured in different pages and at different levels, as explained in the later sections in the document.
4. When endpoints initiate a 911 emergency call, based on the location information in SIP messages or L3 (phone IP address)/L2 (phone MAC address) information of the endpoint, MiVoice Connect will send the CESID or other user-specific location information to the third-party vendor.
5. The emergency routing service (ERS) will then use the CESID or location information in the SIP messages to derive the actual dispatchable location with the help of LIS.
6. Based on the location, ERS will find the nearest or appropriate PSAP entity and will place a call with all the relevant location and call-back information.
7. The dispatcher at the PSAP gets a “screen pop” which displays information as provided by the third-party vendor.
8. The dispatcher sends emergency response personnel to the calling party’s location.

For more information about RAY BAUM in MiVoice Connect, see the following documents:

- MiVoice Connect RAY BAUM’S General Overview and Solution Deployment Guide
- MiVoice Connect RAY BAUM’S General Overview and Solution Deployment Guide for RedSky

- MiVoice Connect RAY BAUM'S General Overview and Solution Deployment Guide for Intrado

25.1.3 Roles and Responsibilities

Each participant in an emergency call has a different role to fill and a different set of responsibilities to handle.

The role of the PBX is to:

- Identify the call as an emergency call.
- Route the call to an outbound trunk, preferably a dedicated trunk.
- When Emergency call is initiated, pass the correct CESID information (location information) and call-back number to the configured service provider using configured trunks by using required message format.
- If the RAY BAYUM feature is enabled, PBX additionally plays a role in:
  - Supporting and integrating third-party emergency service vendor trunks.
  - Enhancing configuration capabilities for user to configure a granular wire map and map it to different locations.
  - Enabling the PBX to provide information in vendor-specific format for deriving location information.
  - Deriving CESID and call-back independently of each other and conveying these to the PSAP.

The role of the telephony exchange of the service provider is to:

- Work with the customer to ensure the correct caller ID number is passed to the PSAP.
- Pass the caller information to the PSAP.

Note:

The billing number of the trunk is used if no other caller information is available.

The role of the PSAP is to:

- Receive emergency calls.
- Host a database that maps the caller ID numbers to the physical location of the users.
- Display information about the calling party to a dispatcher.
- Send the proper emergency response personnel to the caller's location.

The role of the user is to:

- Decide which type of caller ID information best fits your needs for emergency calls.
- Work with the service provider to verify that they will accept your preferred type of caller ID information.
- Communicate any changes to your emergency configuration to ensure the PSAP location is current.

In addition to the roles and responsibilities so far, if the RAY BAUM feature is enabled, the user or administrator has some additional roles to perform:

- Planning the network mapping of the premise and associating different dispatchable locations with the logically divided network map.
- Deciding and configuring information about the appropriate third-party emergency service provider in MiVC Connect Director if required, for RAY BAUM deployment.
- Updating the third-party vendor with information about emergency configuration, and reconfiguring MiVoice Connect using Connect Director.
- Synchronizing information between MiVC Connect Director and Vendor.

25.2 Using a PS/ALI Service Provider

In addition to working with your local PSAP to provide accurate logistical information, we recommend that you subscribe to a Private Switch/Automatic Location Information (PS/ALI) service provider as well.

A PS/ALI service provider maintains a database that stores specific address information for each extension or DID on your system. Subscribing to PS/ALI services ensures that accurate automatic number identification (ANI) information is passed to the PSAP in the event of an emergency call, and prevents the emergency responder from showing up at the wrong location.

A subscription to a PS/ALI service provider is particularly recommended in situations where a Mitel system is deployed in an environment where a single PRI is used to serve multiple locations, such as a single PRI being used for several schools in the same district. In such environments, it is possible for a user to make an emergency call from one of the elementary schools and have the emergency crews dispatched to the wrong location. This can happen if the local trunks are busy and the call gets routed across an analog trunk and across the WAN to the first available PRI, which might be at one of the other schools in the district. With no PS/ALI database to provide accurate information about the origination of the call, the emergency services providers see the call originating at the wrong location. While the correct phone number is sent to emergency services, the association is with the PRI instead of the school where the call originated.

This critical error can be prevented if a PS/ALI database is in place. Such a database, which is maintained by a PS/ALI service provider, can identify the location associated with a specific DID.

Note:

- Mitel does not provide PS/ALI service. Contact the local telco carrier for information about PS/ALI service providers in the relevant areas.
- With third-party service providers integrated for RAY BAUM conformance, you must handle certain features of the vendor's location information service (LIS) rather than those of the PS/ALI database. The Using a Third-Party Location Information Service Provider on page 972 section describes such features of the vendor's LIS.

25.3 Using a Third-Party Location Information Service Provider

You do not need to work with your local PSAP to provide accurate logistical information. It is handled by the third-party vendor. However, you are responsible for planning and configuring third-party location information service (LIS) and PBX configuration properly. A third-party vendor maintains the location information service (LIS) database that stores location information and maps it to specific ID. By configuring this relationship properly in LIS, the third-party vendor ensures that accurate and dynamic location information is passed to the PSAP during an emergency call and the emergency responder reaches the correct location.

Note:
The difference here is that the mapping is between location and CESID, while in PS/ALI, the mapping is between location and user. The location-to-user mapping can lead to incorrect location being conveyed to the PSAP when user moves dynamically. Also, irrespective of the site from where the emergency call is placed, the third-party vendor trunks will derive PSAP information based on the location of caller. This ensures that the best possible PSAP is selected, and accurate location information is provided to the identified PSAP.

25.4 Feature Operation

This section describes the following features:

- Trunk Signaling for Emergency Calls on page 976

25.4.1 Digit Collection for Emergency Calls

A Mitel user who dials an emergency number (or <access_code> + emergency number) will be routed to an emergency-capable trunk.

- If the user dials an access code followed by an emergency number, digit collection terminates immediately and the call is routed to an emergency-capable trunk.
- If the user forgets to dial an access code before dialing the emergency number, the system waits five seconds before routing the call to an emergency-capable trunk. This pause has been introduced to eliminate accidental calls to the emergency number.

Note:
Systems that use 911 for the emergency number often also use 9 as an access code for outbound calls. This makes it easy for users to mistakenly dial 911 on a long-distance call by adding an extra 1 before the area code, such as dialing the following number: **9-1-1-408-555-1212**. If additional digits are entered after 9-1-1 during the five-second timeout period, the system will consider it a dialing error and the calling party will hear a reorder tone.

25.4.2 Ensuring Proper Routing of Emergency Calls

Without a dedicated emergency-enabled trunk, emergency calls may not be properly routed under the following circumstances:

- If all available emergency-enabled trunks are busy, the Mitel system will not route the emergency call.
- If a site has no emergency-enabled trunk and ‘Parent as Proxy’ is enabled for that site, the Mitel system will not route the call to the emergency-enabled trunks of the parent site if the admission control bandwidth is exceeded at either site.
- If the SIP tie-trunk is unavailable, the Mitel system will not failover and route the call through the parent site when the following are true:
  - The site is connected to the parent site by an emergency-enabled SIP tie-trunk.
  - Parent as proxy is enabled for the site.
  - The site has no available emergency-enabled trunk.

Note:
At sites with multiple trunks, the trunk selection order is SIP, ISDN, Digital, Analog. Additionally, when trunk groups are configured in the Mitel system, the default programming enables emergency services in each trunk group.

System administrators should consider that emergency calls will be routed over SIP if a SIP trunk is available and are encouraged to configure a dedicated, non-SIP, non-emergency trunk and disable Emergency Services in SIP Trunk Groups.

Note:

A dedicated emergency-enabled trunk must be configured at each site to ensure emergency calls always reach the CO and PSAP.

Call permissions are ignored when an emergency call is placed to ensure that a user can dial emergency number from any extension on the system, regardless of the permissions associated with that user or the extension from which he or she is calling.

Once the user dials an emergency number, the call leaves the extension, arrives at the switch, and is routed to any available emergency-capable trunk at the originating site. If the user belongs to a user group that does not have access to any emergency-capable trunks, then the call will not be placed.

Note:

When adding users to the Mitel system, make sure each user is placed in a user group that has access to an emergency-capable trunk group. If a user is placed in a user group that does not have access to an emergency-capable trunk, such as a user group with long distance trunks only, members of that user group will not be able to dial emergency numbers, and they will get a reorder tone when attempting to do so.

To better understand this, you must realize that users are placed into user groups when added to the Mitel system. The user groups are assigned to trunk groups, and these trunk groups have different capabilities, one of which is the ability to place emergency calls. Every user group must have access to an emergency-capable trunk. It is crucial that each site has at least one emergency-capable trunk.

For details about adding users to a user group that has access to an emergency-capable trunk, see Configuring User Groups on page 481.

Registered phones (On-premises and Teleworker) can be in the **Available** state. When the user assignment is removed, these phones will remain in the **Available** state. By default, the User group for unassigned phones is **IP Telephones**. You can configure any User group for unassigned phones.

Similarly, phones can be in the **Anonymous** state. By default, the User group for phone in the **Anonymous** state is **Anonymous Telephones**. You can configure any User group for phones that are in this state.

To ensure compliance with Ray Baum, these phones must have the capability to make emergency calls. It is mandatory to configure at least one emergency-capable trunk group to the User group configured for unassigned phones and anonymous phones. To do this, navigate to **Administration** > **Users** > **User Groups** > **General Tab** page, select the User group and do the following:

1. In the **Outgoing trunk groups (Access Code)** section, add at least one emergency-capable trunk group for every site. For example, if there are three sites and each site has one emergency capable trunk group, it is mandatory to add these three emergency-capable trunk groups to the user group.

Always confirm with your service provider that a trunk supports emergency calls. In some instances, this may not be the case, such as with long-distance trunks. If the trunk does not support emergency, be sure to un-check the emergency parameter as an available service in the associated trunk group in Connect Director.

If you have mistakenly set up a site that has no available emergency-capable trunks, emergency calls will be routed to the emergency-capable trunk at the proxy site if one has been designated. By routing the call to a proxy site, the Mitel system is making a “last ditch” attempt to place the emergency call. This failover behavior can be unreliable and should not be relied upon to ensure that users on your system can dial emergency numbers. If you use the “parent as proxy” configuration, make sure the boundary between the two sites never traverses geographic locations that would send an emergency call to the incorrect emergency-service provider. For example, if improperly configured, a caller in Houston could pick up a phone, dial 911, and reach a 911 service in Boston because the system was configured to have the Boston site as the parent of the Houston site with “parent as proxy” checked.

Each site should have at least one emergency-capable trunk. If there will only be one trunk at a particular site, that trunk should be capable of placing an emergency call. You should also be aware that if there is only one trunk at a site, only one emergency call can be placed at a time. Therefore, you should make sure you have enough emergency trunks at each site to accommodate the realistic potential emergency traffic for that site.

Note:

- If VPN phones are to be deployed in locations that are different from the site with which they are associated, placing an emergency call from a VPN phone requires special consideration.
- In the default case, an emergency call dialed from a VPN phone will be sent to the PSAP associated with the site that hosts the switch and VPN concentrator. The emergency call would be answered but likely by a response center that is out of area for the VPN phone user which could delay or prevent an appropriate response.
- Mitel strongly recommends that you deploy a 3rd party solution that can send a VPN phone's emergency call to the appropriate response center. Otherwise you should clearly mark VPN phones to alert users that emergency calls should not be attempted from such phones and you should educate your VPN phone users about the emergency-number limitations of the VPN phone.

25.4.3 Trunk Signaling for Emergency Calls

When an emergency call is routed out an analog or digital loop-start or a digital wink start trunk, the service provider is responsible for passing caller ID information to the PSAP.

When an emergency call is routed through a SGT1 PRI trunk, the Mitel System sends the proper caller ID information to the service provider, and the service provider must forward the information to the PSAP.

Contact your local telecommunications service provider to communicate your emergency implementation plans and have them approved. It is important to ensure that the service provider will accept, and subsequently pass to the PSAP, the caller ID information configured within the Mitel system. In some cases, without proper planning, a provider will reject the caller ID information as configured in the Mitel system and will simply pass the caller ID information associated with the trunk to the PSAP. If this happens, the dispatcher may get a number telling them to go to the wrong location.

User’s have a home port defined in Connect Director. If a user is not at his home port, it could change the caller ID number delivered to the service provider on emergency calls.

For mobile workers who travel between sites, the user must have access to an emergency-capable trunk at every site. In remote locations, the user should use the emergency trunk associated with that remote location.

If emergency calls are routed through a third-party emergency service vendor trunk, it is important for the user to configure proper location-to-CESID mapping in vendor database, and then use same CESID for placing emergency calls. The vendor will handle the calls based on the synchronization with PSAP.

25.5 Selecting Caller ID Type for Emergency Calls

There are a number of different caller ID choices available within Mitel that can be used by the PSAP to identify callers when they place an emergency call. The list below summarizes the available choices for sending the caller ID to the service provider for emergency calls. Options are listed in the order of precedence, meaning that if the first item on this list is not configured within the Mitel system, then the next piece of information on the list will be sent. Additional details about each of these caller ID options appears after the list.

1. User's Caller ID number
2. User's Direct Inward Dialing (DID) number
3. Caller's Emergency Service Identification ID (CESID) for an IP address range

Note:

The CESID is the telephone extension that a switch sends to a Public Safety Answering Point (PSAP). A CESID helps to locate callers who require emergency services.

4. CESID of the controlling switch.
5. CESID of the site.
6. Nothing sent by Mitel system (the service provider sends the caller ID number associated with the trunk)

As part of RAY BAUM, the following CESID options are used and are applicable for US customers:

1. Caller's Emergency Service Identification ID (CESID) for an IP address range
2. CESID of the controlling switch.
3. CESID of the site.
4. Nothing sent by Mitel system (the service provider sends the caller ID number associated with the trunk)

Note:
The user's Caller ID number and user's DID number options are not applicable for RAY BAUM because when a user plugs out the IP phone from one socket to other socket in the premises, the IP address might change; but the user assignment will not change. Therefore, if the user changes the location, there is no means for the administrator to know this and this causes the CESID to be assigned. The CESID used in this case would be mapped to the previous location. So, these options will become dysfunctional.

For details on selecting the best choice for your situation, refer to Available Caller ID Options on page 978.

If you are configuring a system in the Netherlands, see Special Considerations for Netherlands on page 990.

25.5.1 Available Caller ID Options

Refer to the following sections for information about caller ID options.

25.5.1.1 User's Caller ID Number

Note:
As mentioned earlier in Selecting Caller ID Type for Emergency Calls on page 977, this section is not applicable for US customers as part of RAY BAUM.

Each user can be assigned a caller ID number that will identify him during outbound calls. This caller ID number is typically used for outbound calls from the Mitel system when you do not want the receiving party to know the calling party's DID number. For example, an ACD agent may use caller ID to ensure that returned calls will go to a queue of sales agents, rather than directly to his desk. Similarly, this caller ID number can be sent to the service provider to identify the user when he places an outbound emergency call. The user's caller ID number is a very specific way of identifying the location of an individual user and is therefore likely to become less accurate over time as the PSAP's emergency database becomes out of date. Sending the CESID for outbound emergency calls is best for smaller organizations (see the figure below) and is defined on the User Edit page. You must select the **Send Caller ID as Caller's Emergency Service Identification** check box on the user group page.

In the scenarios described above and below, the user's caller ID number will only be sent when the user is at his home port. If the user is not at his home port, then the next available caller ID type is sent.

25.5.1.2 User's DID Number

Note:
As mentioned earlier in Selecting Caller ID Type for Emergency Calls on page 977, this section is not applicable for US customers as part of RAY BAUM.

The Direct Inward Dialing (DID) number is the number someone dials from outside the Mitel system to reach a user at her desk. The DID is what most people would consider to be a "normal" telephone number. This DID number can be sent to the service provider to identify the user when she places an outbound emergency call. Although this is the most granular way of identifying users, it is also the most likely to become out of date in the PSAP's emergency database as people come and go. Sending the DID number for outbound emergency calls is most appropriate for smaller organizations and is defined on the **User Edit** page. You must select the **Send DID as Caller's Emergency Service Identification** check box on the **User Group** page.

25.5.1.3 CESID of the Specified IP Address Range

The CESID of an IP address range can also be delivered to the service provider during outbound emergency calls. A single CESID number is assigned to a range of IP addresses such that any IP phone that has an IP address that falls within the specified range will have this CESID sent for outbound emergency calls. This option works best for identifying a phone in an office that has many floors and many extensions. Typically, a specific IP address range is configured for each floor of a building so that all users on that floor use the same CESID for emergency calls.

If a DHCP server is present, an IP phone will automatically receive an IP address within the specified range when it is connected to the network.

Sending the CESID for a specified IP address range for outbound emergency calls works best for larger organizations where simply identifying the site's street address would not provide enough information for an emergency response team to locate the caller. Furthermore, this option offers the best flexibility, the highest accuracy, and is the least likely to become out of date in the PSAP's emergency database. This option is defined on the **IP Phone Address Map** page.

In addition to the information already mentioned in this section, the following information is applicable for US customers as part of RAY BAUM.

The following are the IP address mappings that you can create:

- IP address (range-based): This is used to determine the site the phone is registered to and also to derive the CESID/callback number.
- MAC based entry: This is used only to derive the CESID/callback number.

For Teleworker phones, MAC-address-based entry is mandatory for RAY BAUM conformance. If an administrator wants a teleworker phone to register for a particular site, then an IP-address-based map must be created considering the EGW private IP range and with the following conditions:

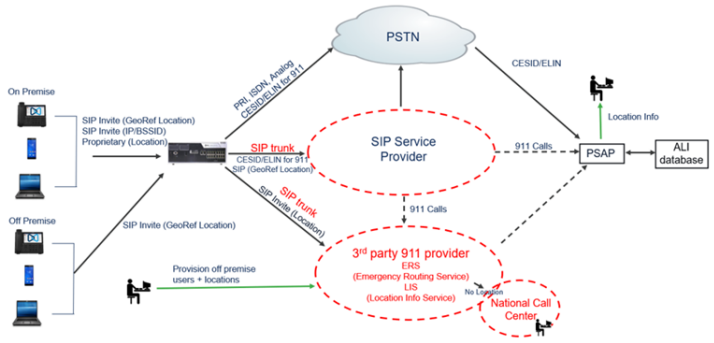
- No CESID number must be assigned to this entry
- No callback number must be assigned to this entry.

To help illustrate the options, if a customer whose physical deployment is big enough that more than one dispatchable location (CESID) is required, such as a single floor of a large building, for which four dispatchable locations are required, one for each corner.

1. Customer has only on-premise IP4xx and/or 69xx and/or DECT devices. In this situation, the customer can purchase one or more CESIDs from their PSTN service provider, so as to cover the entire location with required granularity and use the existing IP range and/or L2 CESID mapping features available on the MiVoice Connect without the need for any upgrade. Enabling these features provides a dynamic location update should the device be moved by the user within the premises.
2. If the cost of the additional CESIDs is prohibitive, then the customer should investigate integration with Mitel-verified third-party vendors (RedSky, Intrado) based on cost comparison.
3. If the customer adds MiVC Connect Client softphones on laptops/mobiles or any kind of remote Teleworkers to their solution, the customer will have to upgrade and integrate with a Mitel-verified third-party vendor.

Whichever deployment model is selected, MiVoice Connect will act as a facilitator for administrators to configure and manage the location information of the endpoints. It is the responsibility of the administrators to configure the location information appropriately.

Figure 25: MiVoice Connect Deployment



For more information, see Reviewing the IP Phone Address Map on page 286.

In the **IP Phone Address Map** page, the following fields are enabled and are mandatory for US customers using teleworker phones.

- **Teleworker User**
- **MAC Address**
- **Callback Number**
- **Ignore CID/DID for Callback**
- **Caller's emergency service identification (CESID)**

For more information about these fields, see IP Phone Address Map.

25.5.1.4 CESID of the Controlling Switch

Similar to the previous option, the Caller's Emergency Service Identification ID (CESID) of the controlling switch can also be sent to the service provider during outbound emergency calls. With this option, a CESID number is assigned to a phone switch and for any phone plugged into this switch, the switch's CESID is sent for outbound emergency calls. This option is best for larger organizations in which users are calling from analog phones. Using the IP Phone Address Map method will not work with analog phones. This approach ensures that the emergency response team is sent to the approximate vicinity of the calling party. This option is defined on the Switch Edit page.

Site Caller's Emergency Service Identification (CESID) – This option delivers the CESID associated with the site to the service provider during emergency calls. This approach might not be granular enough for larger enterprises, but it could work well for single-site organizations or for situations in which it would be adequate to provide the emergency response personnel with a building address. This option is defined on the Site Edit page.

Note:
For analog phones, you must enter the CESID for the analog port. This is required for RAY BAUM compliance. This is applicable for US customers only.

The following table shows several customer scenarios and provides recommendations for how to configure E911 along with reasons for the recommendation.

Rules and regulations for E911 can vary between geographical regions. Consult with the local public safety agency to ensure the system configuration meets the local requirements.

Table 246: E911 Configuration Options

Scenario	Note
Small site with analog trunks	No emergency configuration necessary

Scenario	Note
College dormitory rooms (with PRI)	• Emergency response personnel must be dispatched to a specific room • Consider sending Caller ID or DID. Mitel recommends turning off extension assignment for this application. See the Configuring Extension Assignment on page 549for more information about extension assignments.
Classroom (with PRI)	• Emergency response personnel must be dispatched to a specific room • Send DID or Caller ID. Consider turning off the extension assignment feature. See the Configuring Extension Assignment on page 549for more information about extension assignments.
Multi-building campus or office complex (with centralized PRI)	• Caller ID or DID might be too granular and involve too much management overhead. • Consider using IP phone address mapping and/or the switch's CESID.
Large building with multiple floors (with PRI)	• Caller ID or DID may be too complex. • Consider using IP phone address mapping and/or the switch CESID.
SoftPhones or travelling user	Use home phone or hotel phone for emergency calls.
Remote IP phones (with PRI at headqu arters)	• Dial an emergency number with home phone. • Use the IP phone address map (home CESID) as a backup.
VPN Phone – Fixed Location	• Remote worker install phone once, then never moves it. • Configure Caller ID of phone to reflect geographic location. One option is setting Caller ID to be identical to worker's home phone number.

Scenario	Note
VPN Phone – Variable Location	• Remote worker uses phone when traveling from various locations. • Use home phone or hotel phone for emergency calls.

25.6 Configuring a System for Emergency Calls

The following sections provide information for configuring a Mitel system for emergency calls.

25.6.1 Trunk Groups

Make sure you have an outbound trunk group with outbound access that also supports the emergency trunk service. If there is no emergency-capable trunk group configured, create one on the appropriate Trunk Group edit page

Note:

- You should uncheck 911 option while configuring SIP tie trunk groups.
- Admin must configure type of the third party 911 service provider and corresponding server parameters in the trunk page.

Complete the following steps to configure a trunk group to support emergency service:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **Trunk Groups** > **Trunk Groups**. The **Trunk Groups** page is displayed.
3. In the **List** pane, select the trunk that you want to configure to support emergency dialing.

Note:
The **General** tab in the **Details** pane displays parameters for the selected trunk group.

4. Select the **Outbound** tab.

5. Check the **Emergency (e.g. 911)** check box.
6. Click **Save**.

As a precaution, you should review all other trunk groups to ensure that the **Emergency (e.g. 911)** check box is not inadvertently enabled on a trunk that is not emergency-capable.

25.6.2 User Groups

Ensure each user group has access to a emergency-capable trunk group. You can select the desired emergency Caller ID choice on the **User Groups** page.

- To send the Caller ID as the CESID number, ensure that the **Send caller ID as caller's emergency identification (CESID)** check box is selected (not used when Ray Baum feature is enabled).
- To send the DID as the CESID number, ensure that the **Send DID as caller's emergency identification (CESID)** check box is selected (not used when RAY BAUM feature is enabled).

Complete the following steps to enable a user group for supporting emergency dialing:

1. Launch Connect Director.
2. Click **Administration** > **Users** > **User Groups**. The **User Groups** page is displayed.
3. In the **List** pane, select the user group that you want to configure to support emergency dialing.

Note:
The **General** tab in the **Details** pane displays the parameters for the selected user group.

4. Select the **Send caller ID as caller's emergency identification (CESID)** check box to send the caller ID as the CESID number.

Note:
If Ray Baum is enabled, then this option is not applicable for US sites.

5. Select the **Send DID as caller's emergency identification (CESID)** check box to send the DID as the CESID number.

Note:
If RAY BAUM is enabled, then this option is not applicable for US sites.

6. Click **Save**.

Ensure that you give access to trunk groups at other sites in case users in the group use the Extension Assignment feature from another site. See the Configuring Extension Assignment on page 549 for more information about extension assignments.

25.6.3 Users

Ensure the **Caller ID** field is configured if you are sending Caller ID as CESID for this user. Similarly, make sure the **DID** check box is selected (and contains a valid number in the **DID** field) if you are sending DID as CESID for this user.

Verify each user belongs to the correct user group. See Configuring a User Account on page 488 for more configuration information.

Complete the following steps to configure a user to send Caller ID as CESID:

1. Launch Connect Director.
2. Click **Administration** > **Users** > **User**. The **User Groups** page is displayed.
3. In the **List** pane, select the user that you want to configure to send caller ID as CESID.

Note:
The **General** tab in the **Details** pane displays parameters for the selected user.

4. Do one of the following:
   - In the **Caller ID** field, enter the number that you want to send for this user.
   - Select the **Enable DID** check box and select the desired **DID range** in the DID Range list.
   - Select the **Enable DID** check box and make sure there is a valid number listed in the **DID number** field.
5. In the **User group** list, select a user group that has the type of emergency support that users must have enabled.
6. Click **Save**.

You cannot configure any user, workgroup, or route points to have a 911, 911n, or 911nn extension. The 911 feature reserves these extension ranges.

Note:
Outside the U.S., be sure that extension numbers do not overlap or otherwise conflict with local emergency phone numbers.

25.6.4 Specifying CESID for IP Phone Address Range

When you have sites in different geographical areas, you must make sure that the correct local emergency number is associated with the site. You can do this by associating the local CESID number with the IP address range the system uses to assign number to new phones at the site. To associate the CESID with numbers assigned to phone at the site, do the following:

1. Launch Connect Director.
2. Click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page is displayed.
3. In the **List** pane, select the site to which you want to associate the local CESID.

Note:
The **General** tab in the **Details** pane displays the parameters for the selected site.

4. In the **Caller's emergency service identification (CESID)** field, enter the emergency phone number that is local for the site.
5. Click **Save**.

To associate the CESID with numbers assigned to phones at the US site, do the following:

Note:
You can associate the CESID with numbers for either IP-address-based or MAC-address-based phones; but not for both. However, to associate the IP phone address for the teleworker phone, you must create two entries, one for IP-address based mapping and the other for MAC-address-based mapping.

1. Launch Connect Director.
2. Click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page is displayed.

3. In the **List** pane, select the site to which you want to associate the local CESID.

> **Note**:
> The **General** tab in the **Details** pane displays the parameters for the selected site.

4. In the **Caller's emergency service identification (CESID)** field, enter the emergency phone number that is local for the site.
5. Select the **Teleworker User** check box for Teleworker users.

> **Note**:
> If this option is enabled, the **Caller's emergency service identification (CESID)**, **MAC Address**, and **Call-Back Number** fields are mandatory.

6. In the **MAC Address** field, enter the MAC address of the endpoint.
7. In the **Call-Back Number** field, enter the callback number for mapping that is based on IP address or MAC address.
8. Click **Save**.

25.6.5 Switch

Complete the following steps to configure a switch with a CESID.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
3. In the **List** pane, select the switch that you want to configure **with a CESID number**.

> **Note**:
> The **General** tab in the details pane displays parameters for the selected switch.

4. In the **Caller's emergency service identification (CESID)** field, enter the CESID number that is local for the area the switch services.
5. Click **Save**.

25.6.6 Sites

Use the Sites page to configure a site's CESID number. Refer to Viewing Configured Sites on page 100, for additional information about configuring sites.

Complete the following steps to configure a site to support emergency numbers.

1. Launch Connect Director.
2. Click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. In the **List** pane, select the site that you want to configure to support emergency numbers.

> **Note**:
> The **General** tab displays parameters for the selected site.

4. In the **Caller's emergency service identification (CESID)** field, enter the number that you want the site to send for emergency responses.

> **Note**:
> Ensure this field is configured with the appropriate number for the country or area the site services. For example, sites serving phones in the United States and Canada use 911.

5. To add an emergency number, do the following:
   a. Under **Emergency number** list, click Add.
   b. Type the exact emergency number required to contact the associated Emergency Service Provider.
   c. Select the **Trunk access code required** check box with the trunk access code over which you want to send emergency calls.
6. Click **Save**.

25.7 Planning Your Emergency Response

When an emergency call is made, the system automatically generates an event in the Windows event log at the beginning of the call. With the use of an event filter, you can automatically send an e-mail message to the appropriate people in your organization to

help coordinate your local response, for example, at the organizational level, whenever the emergency number is dialed.

We recommend training the personnel at all sites on the emergency operations of your Mitel IP voice system. All users should know how to access emergency services during normal and power outage situations.

25.7.1 Call Notification

You can set up an event filter to generate an e-mail message to help coordinate your emergency response. For more information about event filters, refer to Database Maintenance for more configuration information.

1. Launch Connect Director.
2. Click **Maintenance** > **Event Filters**. The **Event Filters** page is displayed.
3. Click **New** to create an event filter for emergency calls.

> **Note**:
>
> The **General** tab displays the default parameters for the new event filter.

4. In the **Server** section, do one of the following:
   - Select the server that you want to monitor for emergency events from the list.
   - Select **All** to monitor all servers for emergency events.
5. In the **Source** section, select **ShoreWare**, and then select **Switch** in the list.
6. In the **Event ID** field, enter 1319.
7. In the **Type** section, select All.
8. In the **Email** field, enter the email address of the party to whom you want emergency notification sent.
9. Click **Save**.

We suggest naming your switches with location information such that you can understand which site the call was made from.

25.8 International Emergency Numbers

The Mitel system allows dialing of emergency numbers with and without trunk access codes. For this reason, you should reserve the dialing plan space for this feature. Consider the following:

- **112** is used in Europe and other countries.
- **000** is used in Australia.
- **999** is used in Asia.

Ensure extensions do not begin with “112”, “911”, or “999”.

Note:

Extensions should never begin with “0”

Each site can have a maximum of ten emergency numbers to accommodate locations where multiple emergency service numbers are required.

For more information on international installations, refer to the *MiVoice Connect Planning and Installation Guide*.

25.8.1 Special Considerations for Netherlands

It is against the law in the Netherlands to “spoof” Caller ID. Caller ID will only be sent if the configured caller ID corresponds to the incoming DID that is associated with a particular trunk.

Any number entered in the CESID field in the **Switch Edit Page** and **Site Edit Page** will only be sent if the number matches the number associated with the incoming DID for that trunk.

25.9 Verifying Your Emergency Configuration

After you have finished configuring your system for emergency operation, we recommend working with your local emergency dispatch center to test your configuration in order to verify that it has been correctly configured, is sending out the desired caller ID information, and is dispatching emergency response personnel to the proper location.

We recommend calling your local law enforcement agency’s non-emergency number to understand how to go about the test and to arrange a call time during non-peak hours. Do not place your emergency test call without making prior arrangements. Depending on your location, an officer may be required on-site when making test calls.

The following table is intended to help you plan your test call to the local dispatch center.

Table 247: Emergency Call Test Matrix

Site	Extension	User	Expected Caller ID	ActualCaller ID	Pass or Fail

25.10 Additional Recommendations

All sites should be configured with a designated power failure emergency phone configured appropriately. Each designated power failure emergency phone should be configured on the following ports, based on type of switch, to take advantage of Mitel's emergency line power failure feature:

- SG40 – Port 4: Analog Trunk; Port 5: Analog Emergency Phone
- SG60 – Port 8: Analog Trunk; Port 9: Analog Emergency Phone
- SG120 – Port 8: Analog Trunk; Port 9: Analog Emergency Phone
- SG30 – Port 1: Analog Trunk; Port 12: Analog Emergency Phone
- SG50 – Port 1: Analog Trunk; Port 12: Analog Emergency Phone
- SG50V – Port 1: Analog Trunk; Port 12: Analog Emergency Phone
- SG90 – Port 1: Analog Trunk; Port 12: Analog Emergency Phone
- SG90V – Port 1: Analog Trunk; Port 12: Analog Emergency Phone
- SG220T1A – Port 1: Analog Trunk; Port 12: Analog Emergency Phone

Call Detail Record Reports 26

This chapter contains the following sections:

Call detail record (CDR) reports allow the system administrator or other individual to review the ongoing call activity on the Mitel system.

26.1 Overview

Note:

All collected CDR data from sites in different time zones are adjusted to the time zone of the Headquarters (Director) server.

The Mitel system tracks all of the call activity and places CDRs in a database and a text file on the server. The system uses the records to generate CDR reports. A new Mitel system has 12 CDR reports based on data from the CDR database. In addition, the text files provide a simple and standard way to access the call data to third-party call accounting systems.

Note:

Call activity is not tracked and call detail records are not recorded for users who have the Call History Privacy feature enabled. For more information about this feature, see Configuring Call History Privacy on page 548.

If the server is not running, it does not generate call detail records, and calls from the associated period do not appear in CDR reports.

In the WAN fails, CDR data is stored for up to two hours on the distributed server. When WAN connectivity returns, the stored data goes to the Headquarters database. After two hours, the distributed server deletes the data and logs an error to the NT event log.

26.1.1 Call Accounting Service

The Mitel system operates a call accounting service on the main server. This service generates and then places call detail records in a database and a space-delimited text file for use by accounting applications from third-party vendors. The call accounting service is also responsible for archiving all the CDR data. The CDR files reside in `C:\Shoreline Data\Call Records 2`.

26.2 CDR Reports

A new Mitel system includes 12 CDR reports that it can generate by using data from the CDR database on the server. CDR reports present information about users, trunks, WAN links, workgroup queues, account codes, and workgroup agents. The two categories of reports are summary and detail.

Summary reports provide a high-level view of the activity that occurred in a particular area, and detail reports provide a detailed view of activity. The most common use of the summary report is to identify discrepancies or problems. The detail report uncovers specific information.

- User Activity Summary: Summarizes all calls for each user.
- User Activity Detail: Lists every call for each user.
- Trunk Activity Summary: Summarizes all calls for each trunk.
- Trunk Activity Detail: Lists every call for each trunk.
- Workgroup Agent Summary: Summarizes all inbound workgroup calls for each agent. The workgroup queue report has only a summary report.
- Workgroup Agent Detail: Lists every inbound workgroup call for each agent and optionally, outbound calls. Non-workgroup calls for the agent are also reported.
- Workgroup Queue Summary: Summarizes queue activity for every workgroup, including calls that went directly to agents.
- Workgroup Service Level Summary: Summarizes data on call processing by the workgroup server.
- WAN Media Stream Summary: Summarizes media stream traffic and call quality for calls made over the WAN in multi-site deployments.
- WAN Media Stream Detail: Lists media stream made over the WAN in multi-site deployments.

- Account Code Summary: Summarizes call information for each account; counts of calls each day, along with their total and average duration. There are also totals for the reporting period.
- Account Code Detail: Provides a detailed list of calls that occurred for each account. For each call the date/time of the call, number dialed, the extension making the call and the duration of the call is included. For each account, a summary is provided of the number of calls, along with their total and average duration.

For more information about the CDR reports, see Call Detail Reports on page 891.

26.3 TMS-CDR Media Stream Statistics

The TMS-CDR Media Stream Statistics feature offers a method of formatting and storing Call Detail Records (CDR) data on media streams and stores that formatted information into a log file on the system, making it easier for the Mitel system to integrate with various third-party SNMP monitoring tools, and enabling users to acquire a more accurate picture of the traffic patterns in their network. This information can be useful in performing load analysis, identifying peak traffic times, and assisting the customer in setting up competitive pricing strategies.

The system processes media statistics for all calls and formats the raw data into separate lines, with each line partitioned into several columns separated by a comma. Formatted data is then saved in a text file and is subjected to appropriate rollovers similar to the other server logs.

One media stream statistic record will be generated for each RTP stream on a call. Thus, a 3-way fully-meshed conference call would generate 6 records.

26.3.1 Formatting

Media statistics are collected and deposited line by line into a file. A delimiter separates one column from the previous one, with no delimiter prior to the first column and none after the last column. The column values will be left-justified and padded with spaces to the right. A value that exceeds the fixed-width column limit will be truncated so that it fits within the limit.

Each line looks like the following line:

- `value-1,value-2,value-3,…..,value-n`

The following summarizes the details of the individual columns.

Table 248: CDR Media Stream Statistics Formatting

Column number	Type	Width	Description
1	Integer	20	ID of the line in decimal
2	String	20	Extension Number For anonymous calls, extension number is not available. In such cases, an empty string will be placed at this column.
3	String	16	Name of Extension or Trunk or Phone (UTF-8)

Column number	Type	Width	Description
4	Integer	2	Party type, decimal 0 Unknown 1 Station 2 Trunk 3 Virtual 4 Workgroup 5 AutoAttendant 6 VMForward 7 VMLogin 8 BackupAA 9 Anonymous Phone 10 Nightbell 11 Paging 12 Workgroup Agent 13 Unknown 14 RoutePoint 15 ACC 16 Hunt Groups 17 Group Paging
4	Integer	2	
5	String	32	SIP Call ID
6	String	16	Local IP Address (Switch, Trunk Switch, or IP Ph one, and so on.) in dotted decimal form
7	String	16	Remote IP Address (Remote end point. Switch or T runk or IP Phone etc.) in dotted decimal form
8	Integer	20	Local Site ID (Site ID of extension or trunk or phone that generated starts)
9	String	16	Local Site Name (UTF-8)

Column number	Type	Width	Description
10	Integer	3	Code Type 1 ALAW, PCMA/8000 (or G711A)\ 2 MULAW, PCMU/8000 (or G711µ) 3 LINEAR, L16/16000 4 ADPCM, DVI4/8000 5 G729A, G729A/8000 6 G729B, G729B/8000 7 LINEAR, WIDEBAND, L16/16000 8 G722, G722/8000 9 BV32, BV32/16000 10 BV16, BV16/8000 11 AAC_LC32000, AAC_LC/32000 12 CustomCodec added by administrator
11	Integer	10	Payload size (in milliseconds)
12	Integer	2	Status code 0 – Norma 1 – Failure
13	String	12	Starting time of the collection in string HH:MM:SS.MSEC format
14	Integer	20	Number of seconds of this collection, in decimal.
15	Integer	20	Number of received packets
16	Integer	20	Number of lost packets
17	Integer	20	Max jitter
18	Integer	20	Underruns
19	Integer	20	Overruns

This feature applies only on the main (headquarter) server. By default, it is disabled. Enabling the TMS-CDR Media Stream Statistics feature requires making the appropriate changes to the registry settings.

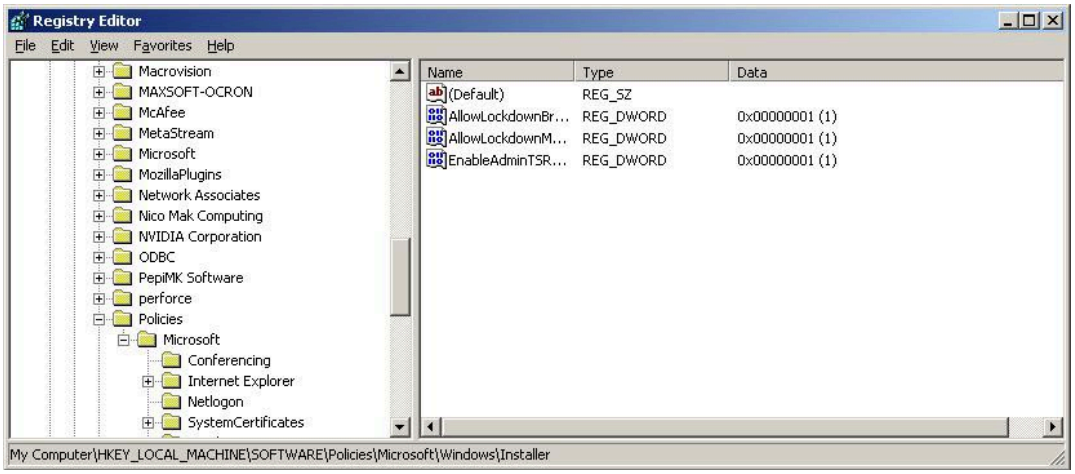
Note:

Do not make changes to the registry settings unless you are certain of what you are doing

To change the registry settings, follow these steps:

1. Click **Start** and select **Run**.
2. Select the **regedit** application to display a window similar to the one shown in below figure.

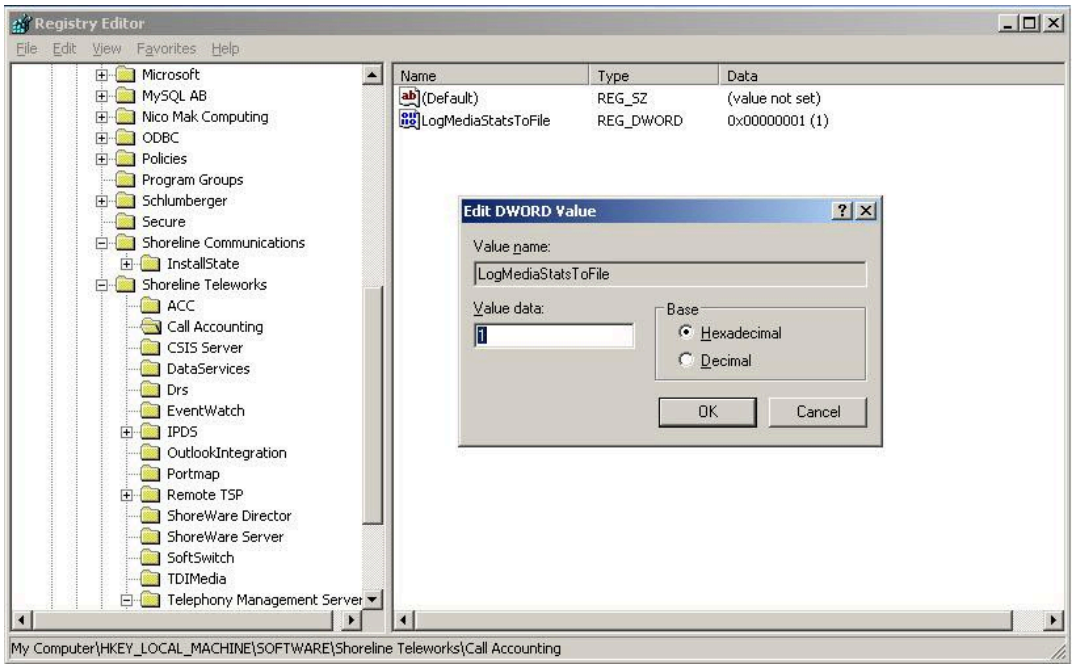
Figure 26: Registry Editor window



3. Navigate to `SOFTWARE\Shoreline Teleworks\Call Accounting`.

4. Double-click the file named **LogMediaStatsToFile** to open the **Edit DWORD Value** dialog box shown in below figure.

Figure 27: Value Data Field



5. Type **1** in the Value data field.
6. Click **OK** to store changes and enable this feature.

26.4 CDR Database

The call accounting service generates call detail records into the active CDR database. This file includes all call activity for the period of time specified in the Retention Period for CDR Data parameter in the Director Reporting Options page.

To access this page, select **Reporting** > **Report Options** from the Director menu.

When Enable Archiving is selected on the **Report Options** page, a nightly routine automatically moves call detail records that are older than the limit specified by the Retention Period for CDR Data into the Archive database.

This appendix describes how the system stores data in the CDR database tables. The CDR database records the call data in the following tables:

- **Call Table:** An entry is made in the Call table for each call in the Mitel system. Other tables often reference the entries to the Call table.
- **Connect Table:** An entry is made in the Connect table for each connection to a call. When used with the Call table, a complete call history is provided.

- **Media Stream Table:** An entry is made in the Media Stream table each time there is a media stream between two switches that are at different sites. In some cases, such as for conference calls, there may be multiple media streams per call.
- **Agent Activity Table:** An entry is made in the Agent Activity table each time a workgroup agent logs into a workgroup and when he or she completes wrap-up.
- **Queue Call Table:** An entry is made in the Queue Call table for each call that is handled by a workgroup server. The entry identifies how the call leaves the workgroup —either by abandonment or for handling.
- **Queue Step Table:** An entry is made in the Queue Step table for each step where the workgroup server either hunts for agents or walks through workgroup queue steps. This provides more detailed information about how the call was disposed of by the workgroup server.
- **Queue Depth Table:** An entry is made in the Queue Depth table each time the depth of a workgroup server's call queue changes.

In addition to these tables, the database contains enumeration tables, which are documented below when discussing the tables that reference these enumeration/lookup tables.

Logged data reflects the time of its logging. For example, certain records contain the name of a trunk group from the configuration database. The name of the trunk group can be changed in the configuration database. New log entries reflect the changed name, but existing logs continue to have the old name.

26.4.1 Creating a CDR Archive Database

If the size of the CDR database grows beyond about 1.5 million records or 4 GB of disk space, it can begin to interfere with the performance of the HQ server, potentially affecting other phone system functionality. To resolve this issue, the administrators must create a separate CDR Archive Database on a separate server, limits the CDR retention period on the HQ server but still provides easy access to the historical records in the CDR Archive DB for reporting, and so on.

To implement an external CDR Archive Database, see the instructions provided in the following KB Articles:

- For Partners: https://mitelcommunity.force.com/partner/s/article/How-to-deploy-a-secondary-CDR-Archive-on-Connect
- For Customers: https://mitelcommunity.force.com/customer/s/article/How-to-deploy-a-secondary-CDR-Archive-on-Connect

26.4.2 Call Table

The CDR database reflects all calls within the system with a few exceptions which are listed below. These exceptions reflect the Telephony Management Server (TMS)

that allows calls to continue even when portions of the system or network are not available. As the TAPI service provider for the Server, TMS manages the call control communications between all other Mitel services.

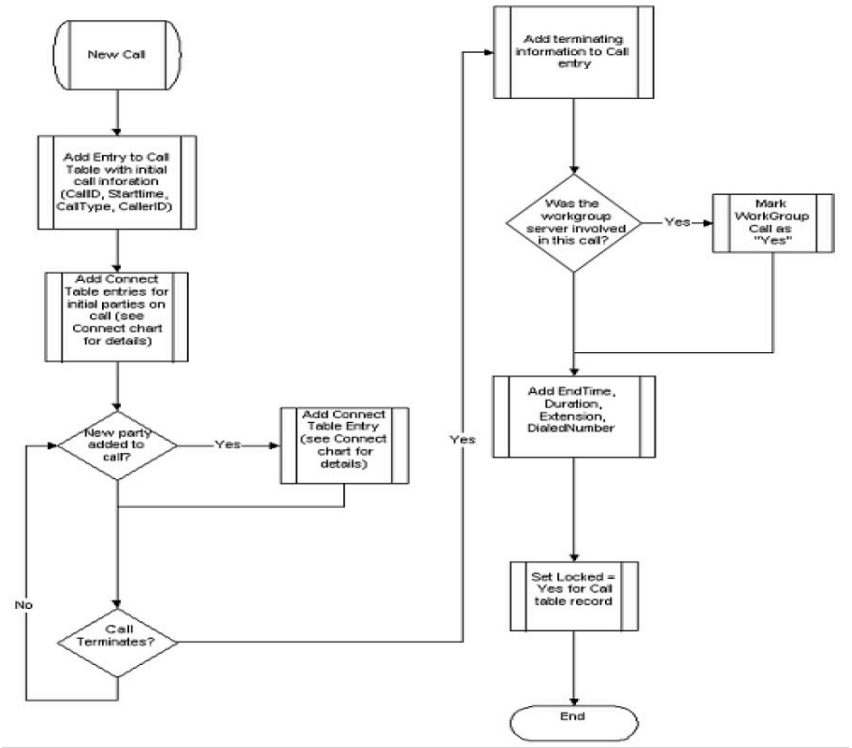
The exceptions are:

- If TMS is not connected to any of the call endpoints, the call is not recorded in the Call table. Because of network outages, TMS may not be connected to call endpoints, yet the call endpoints may have the connectivity necessary to complete the call (for example, the switches are able to communicate with each other but not to TMS).
- If TMS is not connected to some of the call endpoints (for example, a switch involved in the call), the information about the call can be incomplete (for example, the information in the Connect table as explained in the next section would only reflect some of the parties involved in the call).
- If TMS is restarted, any call entries that were incomplete, along with their associated Connect entries are destroyed. Incomplete calls do not show “Yes” in the locked field.
- Also at TMS restart time, TMS logs any calls in progress.

The following figure illustrates how new entries are added to the Call table whenever there is a call in the Mitel system.

Note:
An entry is added to the Call table when the call begins (or when TMS starts up, for any calls in progress) and is updated when the call ends.

Figure 28: New Entries in the Call Table



The Call table is reference by other tables, most important among them being the Connect table. You can analyze the Call and Connect tables to understand the complete disposition of a call as attempts are made to add parties, transfers occur, and so on. Other tables can index the Call table, through the primary key “ID,” which is unique for each record.

There is a CallID field that is used internally by the Mitel system to identify calls. This, however, should not be used as the index into the table).

Close examination of the Call table shows that there are more calls recorded than you may initially expect. For example, if a call is made to a workgroup, you will see an initial call, generally from an incoming trunk. As agents are hunted, calls are made by the workgroup server to agents. If multiple agents are hunted, there will be multiple calls. Once one of the agents is successfully hunted, if you looked at the Connect table you see the agent being attached to the original call. The following table provides information about the elements in the Call Table.

Table 249: Call Table Field Descriptions

Field Name	Data Type	Description
CallID	Number	Number for the existence of the call. (4-byte integer)
ID	AutoNumber	Unique identifier. (4-byte integer, required)
SIPCallId	Text	SIP Global ID number. (31 characters)

Field Name	Data Type	Description
StartTime	Date/Time	For an inbound call, this is when the trunk has been seized. For an outbound call, this is when the user has completed dialing. (8-byte date/time, required)
StartTimeMS	Number	Append this information to the StartTime to reduce the absolute start ti me to the millisecond when the call began. (2-byte integer, required)
EndTime	Date/Time	Time when the call terminates (either by the near end hanging up or when the end external to the system hangs up) and the switch receive s the notification of the disconnect. (8-byte date/time)
EndTimeMS	Number	Append this information to the StartTime to reduce the absolute start ti me to the milliseconds of when the call began (milliseconds). (2-byte in teger, required)
CallNote	Text	User entered Call Note. This can be added from the desktop client. (64 characters, 0-length)
BillingCode	Text	Account code assigned to the call. (32 characters, zero-length)
Locked	Yes/No	Read-only status for this call (set once call has ended). Not locked means the call is still in progress. (boolean)
Extension	Text	For an outbound or extension-to-extension call, the extension has the dialed number of the originator of the call. This field is blank for an outbound call from an anonymous phone with no currently assigned DN. For an inbound call, the extension field contains the DN of the last party involved in the call (excluding voice mail or auto-attendant). For example, an incoming call to an extension that transferred the call to extension 300 has “300” in the extension field (the complete history of parties connecting to the call is in the Connect table). All calls to an extension that are forwarded to voice mail have the extension of the called party and not the voice mail number (15 characters, 0-length).
Duration	Date/Time	Elapsed time of the call from beginning to end. Calculated by subtra cting StartTime from EndTime. Start time begins when the first party is added to a call. End time is when the last party leaves resulting in the end of the call. (8-byte date/time).
CallType	Number	See enumeration in CallType table. (1-byte integer, required)

Field Name	Data Type	Description
WorkGroupCall	Yes/No	Is this a workgroup call? Yes indicates that the workgroup server was involved in processing the call. If the call was directed toward a workgroup server, but that server was unavailable, then this field is set to “No” because the workgroup server never becomes involved in the call. (boolean)
LongDistance	Yes/No	From the perspective of the trunk for the call, did this call involve a long distance connection? The first connect record of the call is used to determine whether a call is long distance. If the first leg is an extension call, the value is always **No**. A trunk call can be transferred or conferenced, so the total long distance time can only be determined by examining all Connect records. (boolean)
DialedNumber	Text	Extension-to-extension and outbound: Number dialed plus trunk ac cess code if any. (15 characters, zero-length)
CallerID	Text	For CallType=Inbound only: Caller-ID number if present. If blocked or unavailable text is provided by the PSTN to indicate caller ID as unav ailable it is included here; for example, the text may be blocked or una vailable (15 characters, zero-length)
Archived	Yes/No	Has this call been archived? (boolean)

26.4.3 Enumeration Tables: Use for the Call Table

Call Type

Table 250: Call Type Descriptions

Call Type	Name	Description
0	Null	
1	ExtToExt	Extension-to-extension call.
2	Inbound	A trunk is the originating party.

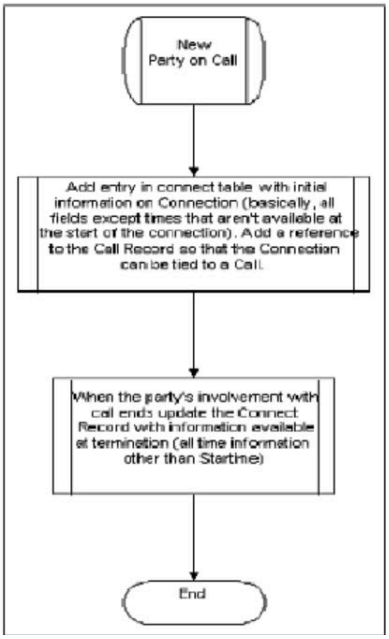
Call Type	Name	Description
3	Outbound	An extension is originating and a trunk is called.

26.4.4 Connect Table

The Connect table contains a record for each party in a call. There are many different types of parties that can be reflected in the table including individual user extensions, workgroups, workgroup agents, and trunks.

The following figure illustrates how new entries are added to the Connect table each time a party is added to a call within the Mitel system.

Figure 29: New Entries in the Connect Table



26.4.4.1 Connect Table Field Descriptions

The following table describes the Connect Table data fields:

Table 251: Connect Table Field Descriptions

Field Name	Data Type	Description
ID	Auto-Number	Unique identifier. (4-byte integer – required)
PartyType	Number	Party that initiated the call. Value corresponds to value from Connect Type Party Type table (See the Party Type Enumeration table below). (6-bit integer – required)

Field Name	Data Type	Description
CallTableID	Number	Link to Call Table ID Key. (20-bit integer – required)
LineID	Number	TAPI permanent line ID for this party. (20-bit integer – required)
SwitchID	Number	Party's Switch ID – unique ID assigned to configuration database to switch. Data only available through database – not Director. Value of 0 indicates the party is a workgroup, voicemail, or an unassigned user. In these cases, DN is are not assigned to a switch/port. (11-bit integer)
PortNumber	Number	Party's port number corresponding to physical port or channel number on the switch. Value of 0 indicates the party is a a workgroup, voicemail or unassigned user. (11-bit integer)
PortID	Number	Party's port ID – if any. Unique ID assigned to switch port by configuration database. Data is available through the database, not Connect Director. A value of 0 indicates the party is a workgroup, voicemail, or an unassigned user. This is a 20-digit integer.
PortName	Text	Name of port (Trunk or Extension) – user defined in Director. (50 characters)
GroupID	Number	Unique ID assigned by configuration database. (11-bit integer) Value is a TrunkGroupID if PartyType – Trunk. Value is UserGroupID if PartyType – Station. Value is 0 if it is not applicable.

Field Name	Data Type	Description
GroupName	Number	Data is defined is Director by use. (50 characters) If PartyType – Station, value is name of the User-Group If PartyType – Trunk, value is Trunk-Group.
ConnectTime	Date/Time	Time when party was added to call. Initial parties on inbound call, value indicates time trunk was seized. Initial parties on outbound call, value indicates time dialing was complete.
ConnectTimeMS	Number	Append to ConnectTime to determine start time of call with milli second precision. (11-bit integer, milliseconds)
DisconnectTime	Date/Time	Time when party disconnected from call.
DisconnectTimeMS	Number	Append to DisconnectTime to determine end time of call with mill isecond precision. (11-bit integer, milliseconds)
ConnectReason	Number	Connect reason code. Refer to the Connect Reason Enumeration Table below. (6-bit integer – required)
DisconnectReason	Number	Disconnect reason code. Refer to the Disconnect Reason Enume ration Table below. (6-bit integer – required)
PartyIDFlags	Number	Caller ID flags that specifies the data available in ID and Name fields Internal party: number, name and last name from system address book. External party: data corresponds to caller ID field provided by the PSTN. Refer to Party ID Flag Enumeration Table below. (6-bit integer – required)
PartyID	Text	Number of party. Refer to PartyIDFlags field. (50 characters)
PartyIDName	Text	Name of party. Refer to PartyIDFlags field. (50 characters)
PartyIDLastName	Text	Last name of party. (50 characters) Field is blank for external party – PartyIDName contains first and last name, as provided by PSTN Caller ID service.

Field Name	Data Type	Description
CtrlPartyIDFlags	Number	Caller ID flags that specifies the data available in ID and Name fields for the controlling party. Controlling party causes the event. Example: for an entry listing a call was transferred from extension 400 to extension 300, the controlling party is extension 400. Original call will not have a control party.Refer to Table 240. (6-bit integer – required)
CtrlPartyID	Text	Number of controlling party. Refer to CtrlPartyIDFlags field. (50 ch aracters)
CtrlPartyIDName	Text	Name of controlling party. Refer to CtrlPartyIDFlags field. (50 char acters)
CtrlPartyIDLastName	Text	Last name of controlling party. (50 characters)
MailboxID	Text	Mailbox ID if PartyType – VMForward or VMLogin PartyType – VMForward – specifies mailbox receiving forwarded message. PartyType – VMLogin – specifies original target mailbox.
RelatedCallTableID	Number	Reserved. (20-bit integer).
TalkTime	Date/Time	Total connect time. Calls with more than 24 hours include the date. Date not included on calls shorter than one hour. (8-byte date/time) **Example:** A 25 hour call has a TalkTime of 1 day and 1 hour.
TalkTimeSeconds	Number	The seconds component of the TalkTime. (20-bit integer, seconds)
HoldTime	Date/Time	Time on hold. Includes date on calls with more than 24 hours hold time. Date not included on calls with less than one hour hold time. (8-byte date/time) **Example:** A call with 25 hour time has a HoldTime of 1 day and 1 hour.

Field Name	Data Type	Description
RingTime	Date/Time	Inbound calls: time spent offering Outbound calls: ringback time
Duration	Date/Time	The time between ConnectTime and DisconnectTime
LongDistance	Number	Lists trunk connected long distance for outbound calls if PartyType – trunks
TrunkDirection	Number	Indicates inbound / outbound direction. Refer to Trunk Direction Enumeration Table.
SecurityFlag	Number	AES/SRTP flags that indicates call encryption status. (6-bit integer)
SiteName	Text	Reserved (50 characters)
ServerName	Text	Reserved (64 characters)

26.4.4.2 Enumeration Tables Used for Connect Table

PartyType

The following table lists the Connect Table party types.

Table 252: Party Type Enumeration Table

Type #	Party Type	Dexcription
0	Null	
1	Station	User extension which is currently assigned a home port; sometimes referred to as a logged in user.
2	Trunk	Trunk (of any kind).
3	Virtual	A user extension which does not currently have an assigned home port (sometimes referred to as a logged out user).
4	Workgroup	Workgroup extension.
5	AutoAttendant	Auto-Attendant extension.
6	VMForward	Voice mail forward extension (take a message).
7	VMLogin	Voice mail login extension.
8	BackupAA	Backup auto-attendant (built into switch).
9	AnonPhone	Anonymous telephone.
11	Paging	Paging extension.
12	WorkgroupAgent	Records marked as WorkgroupAgent for calls transferred from a Wo rkgroup to an Agent. Direct inbound calls to an agent are Station ty pe.
13	Unknown	Unknown type.
14	RoutePoint	Route point.

26.4.4.2.1 PartyIDFlag

The following table lists the Connect Table party ID flags.

Table 253: Party ID Flag Enumeration Table

Flag #	Party ID Flag Name	Description
0	Null	
1	Blocked	Blocked
2	OutOfArea	Out-Of-Area
4	Name	Name
8	Address	Address
12	NameAddress	Name & Address
16	Partial	Partial
32	Unknown	Unknown
64	Unavailable	Unavailable

26.4.4.2.2 ConnectReason

The following table lists the Connect Table connect reason codes.

Table 254: Connect Reason Enumeration Table

Connect #	Connect Reason	Description
0	Null	
1	Direct	TMS was not available when the party connected t o the call. Connection information is logged, but th ere is no more ConnectReason information
2	ForwardBusy	The party was connected because the previous par ty's availability state was set to forward calls if the previous party was busy.

Connect #	Connect Reason	Description
3	ForwardNoAnswer	The party was connected because previous party's availability state was set to forward calls if the previous party didn't answer.
4	ForwardAll	The party was connected because previous party's availability state was set to forward all calls.
5	Pickup	The call was connected because the called party answered the call.
6	Unpark	Unpark
7	Redirect	Redirect
8	Completion	Completion
10	Reminder	Reminder
9	Transfer	The call was connected after the call was transferred to the party.
11	Unknown	Unknown
12	Unavailable	Unavailable
13	Intrude	Intrude
14	Parked	Parked
15	CampedOn	CampedOn
16	RouteRequest	RouteRequest
17	Called	The party was added to the call because it was the initial target of the call.
18	Forward	Forward
19	Originate	The party initiated this call.
20	Conference	The party was added to the call because the party was conferenced into the call.
21	Silent Monitor	Silent monitoring was initiated.
22	Barge In	Barge In was initiated.
23	Record	Call recording was initiated.
24	Silent Coach	Silent Coach was initiated.
25	StatertMeetMeConf	A Meet Me conference was started
26	JoinMeetMeConf	A user joined a Meet Me conference.
27	RingAllCalled	RingAll called.

26.4.4.2.3 Disconnect Reasons

The following table lists the Connect Table disconnect reason codes.

Table 255: Disconnect Reason Enumeration Table

Reason #	Disconnect Reason	Description
0	Null	
1	Normal	Normal termination
2	Unknown	Unknown reason
3	Reject Call	Call was rejected
4	Pickup Call	Call picked up by other destination
5	Forwarded Call	Call forwarded to another destination
6	Busy	Busy destination
7	NoAnswer	No answer by destination
8	BadAddress	Bad address
9	Unreachable	Destination cannot be reached
10	Congestion	Inadequate bandwidth
11	Incompatible	Destination is incompatible
12	Unavailable	Destination is unavailable
13	NoDialTone	No dial tone from the trunk
14	NumberChanged	Destination number changed
15	OutOfOrder	Destination out of order

Reason #	Disconnect Reason	Description
16	TempFailure	Temporary failure
17	QoSUnavailable	QoS not available
18	Blocked	Destination blocked
19	DoNotDisturb	Do not disturb
20	Cancelled	Call cancelled
21	Unpark	Call unparked to different destination
22	EndConsultCall	End consult call
23	RingAllAnsOther	RingAllAnsOther
24	HangUp	Hang up

26.4.4.2.4 Trunk Direction

The following table lists the Trunk Direction flags.

26.4.4.3 Media Stream Table

Table 256: Trunk Direction Enumeration Table

Flag #	Party ID Flag Name	Description
2	Inbound	The trunk direction is established by the central office
3	Outbound	The trunk direction is established by the local system.

The Media Stream table logs media information about InterSite Calls. At a high level, there is one such entry for each InterSite call. Information about both parties involved in the call is recorded. The following table describes the elements in the Media Stream table.

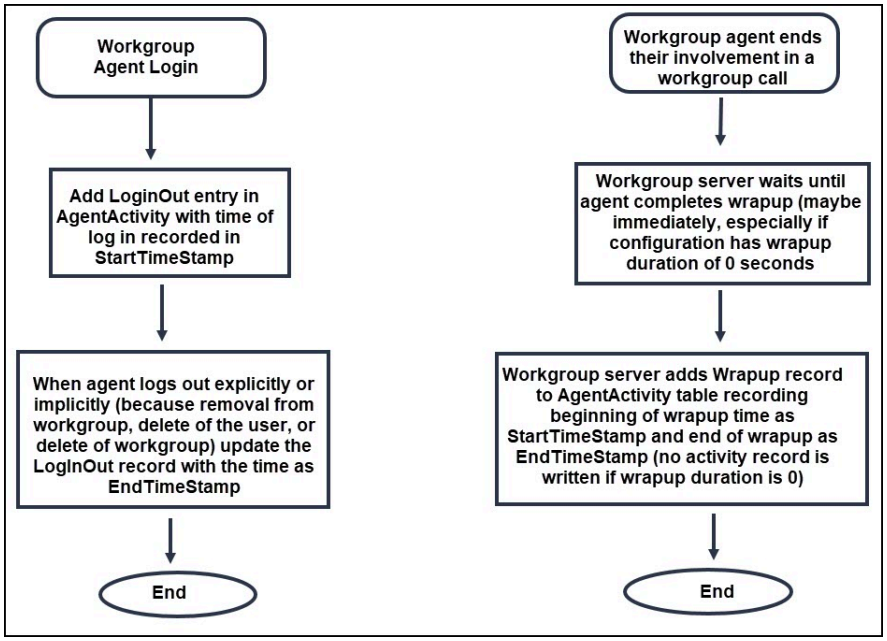
Table 257: Media Stream Data Field Descriptions

Field Name	Data Type	Description
ID	AutoNumber	Unique identifier. (4-byte integer, required)
CallID	Number	Unique number for the existence of the call. (4-byte integer)
SIPCallId	Text	SIP Global ID number. (32 characters)
EncodingType	Number	Encoding type used for media stream. (1-byte integer)
PayloadSize	Number	Media payload size in bytes for each media packet. (4-byte integer)
StartTime	Date/Time	Date and time the call started.
Duration	Date/Time	Elapsed time of call from begin to end. (8-byte date/time)
DurationSeconds	Number	Elapsed seconds time of call from begin to end. (4-byte integer)
FailureCode	Number	Error code. See MediaFailureCode table for enumeration. (1- byte int eger)
A PartyType	Number	Party A's type enumeration. See the PartyType table. (1-byte integer)
A SiteID	Number	Party A's Site ID. (4-byte integer)
A SiteName	Text	Party A's Site Name. (50 characters, zero-length)
A LineID	Number	TAPI permanent line ID for party A. (4-byte integer)
A Name	Text	Call type name for party A. (50 characters, zero-length)
A_Extension	Text	Call extension number for party A (32 characters, zero-length)
A IP Address	Text	Local IP Address for party A. (15 characters, zero-length)
A TotalPackets	Number	Total packets received by party A. (4-byte integer)
A LostPackets	Number	Total packets lost by party A. (4-byte integer)
A MaxJitter	Number	Maximum jitter (ms) for party A. (4-byte integer)
A Underruns	Number	Number of receive underruns for party A. (4-byte integer)
A Overruns	Number	Number of receive underruns for party A. (4-byte integer)
B PartyType	Number	Party B's type enumeration. (1-byte integer)
B SiteID	Number	Party B's Site ID. (4-byte integer)
B SiteName	Text	Party B's Site Name. (50 characters, zero-length)
B LineID	Number	TAPI permanent line ID for party B. (4-byte integer)
B Name	Text	Call type name for party B. (50 characters, zero-length)
B_Extension	Text	Call extension number for party B (32 characters, zero-length)
B IP Address	Text	Local IP Address for party B. (15 characters, zero-length)
B TotalPackets	Number	Total packets received by party B. (4-byte integer)
B LostPackets	Number	Total packets lost by party B. (4-byte integer)
B MaxJitter	Number	Maximum jitter (ms) for party B. (4-byte integer)
B Underruns	Number	Number of receive underruns for party B. (4-byte integer)
B Overruns	Number	Number of receive overruns for party B. (4-byte integer)
InterSite	Yes/No	Indicates a logged call is InterSite. Only Intersite calls are logged.
Archived	Yes/No	Has this entry been archived? (boolean)

26.4.4.4 Agent Activity Table

The Agent Activity Table has information about the workgroup agents' availability. Entries are made to record agents' Login/Logout from the workgroup and to reflect their time in Wrapup mode. The following figure illustrates the flow of new entries being added to the Agent Activity table.

Figure 30: Entries to the Agent Activity Table



The left flow shows how each time a workgroup agent logs in, a LogInOut entry is added, which is then updated at logout time. The right flow shows how the Agent Activity table is also updated as agents complete their handling of workgroup calls. The following table describes the elements in the Agent Activity table.

Table 258: Agent Activity Table field descriptions

Field Name	Field Name	Description
ID	AutoNumber	Unique identifier. (4-byte integer, required)
CallID	Number	Unique number for the existence of the call. Provided in wra pup records. (4-byte integer)
AgentDN	Text	WorkGroup Agent's dialed number (extension). (15 characters, zero-length)
AgentFirstName	Text	WorkGroup Agent's First Name (50 Characters, zero-length).

Field Name	Field Name	Description
AgentLastName	Text	WorkGroup Agent's Last Name (50 Characters, zero-length) **Note**: This field might be blank if the agent doesn't have a last name in the configuration database
State	Number	Enumerated Agent State—set AgentStateLUT for possible va lues.
WorkGroupDN	Text	WorkGroup dialed number (extension) for which this agent act ivity is for (15 characters, zero-length)
WorkGroupName	Text	Workgroup's name. (50 Characters, zero-length)
StartTimeStamp	Date/Time	Start time stamp. For LogInOut records, StartTimeStamp indic ates the time when the agent logged into the workgroup. For wrapup records, the StartTimeStamp indicates the time when t he agent entered wrapup time. See notes below. (8-byte date/ time).
EndTimeStamp	Date/Time	End time stamp (8-byte date/time).
Archived	Yes/No	Has this entry been archived? (boolean)

- Two types of records are placed in the Agent Activity table. The State field identifies the type of record.
- LogInOut Records record the time that an agent is logged into the workgroup.
- Wrapup records record the time that an agent is in wrapup state.
- All records in the table should have ID, AgentDN, AgentFirstName, AgentLastName (unless blank), State, WorkGroupDN, WorkGroupName, StartTimeStamp, and Archived.
- LogInOut Records may exist for agents that have Logged into the workgroup but have not yet logged out. For these records the StartTimeStamp indicates the time when the agent logged into the workgroup. The EndTimeStamp is updated when the agent logs out of the workgroup with the time of the logout.
- For wrapup records the StartTimeStamp indicates the time when the agent entered wrapup time and EndTimeStamp indicates when they exit wrapup state.
- Wrapup records can contain a CallID to identify the Call that the agent was wrapping up from for the Wrapup record. This will not be provided in cases where the agent is manually placed in wrapup state when not on a call.
- There is always a wrapup record when an agent wraps up a call, even for the case where wrapup time is set to zero.

26.4.4.4.1 Enumeration Tables Used for Agent Activity

The following table lists the Agent Activity Enumeration Tables.

Table 259: Agent Activity Enumeration Table

State #	AgentState	Description
0	Null	
1	Reserved	Previously used for Login
2	Reserved	Previously used for Logout
3	Wrap_Up	Agent performing post-call wrap-up
4	Reserved	Temporarily used for Outcalls
5	LogInOut	Agent Login later updated with Logout time.
6	SecLogInOut	Secondary login activity for agents belonging to multiple Workgroup.

Note:

Login and Logout are no longer used.

26.4.4.5 Queue Call Table

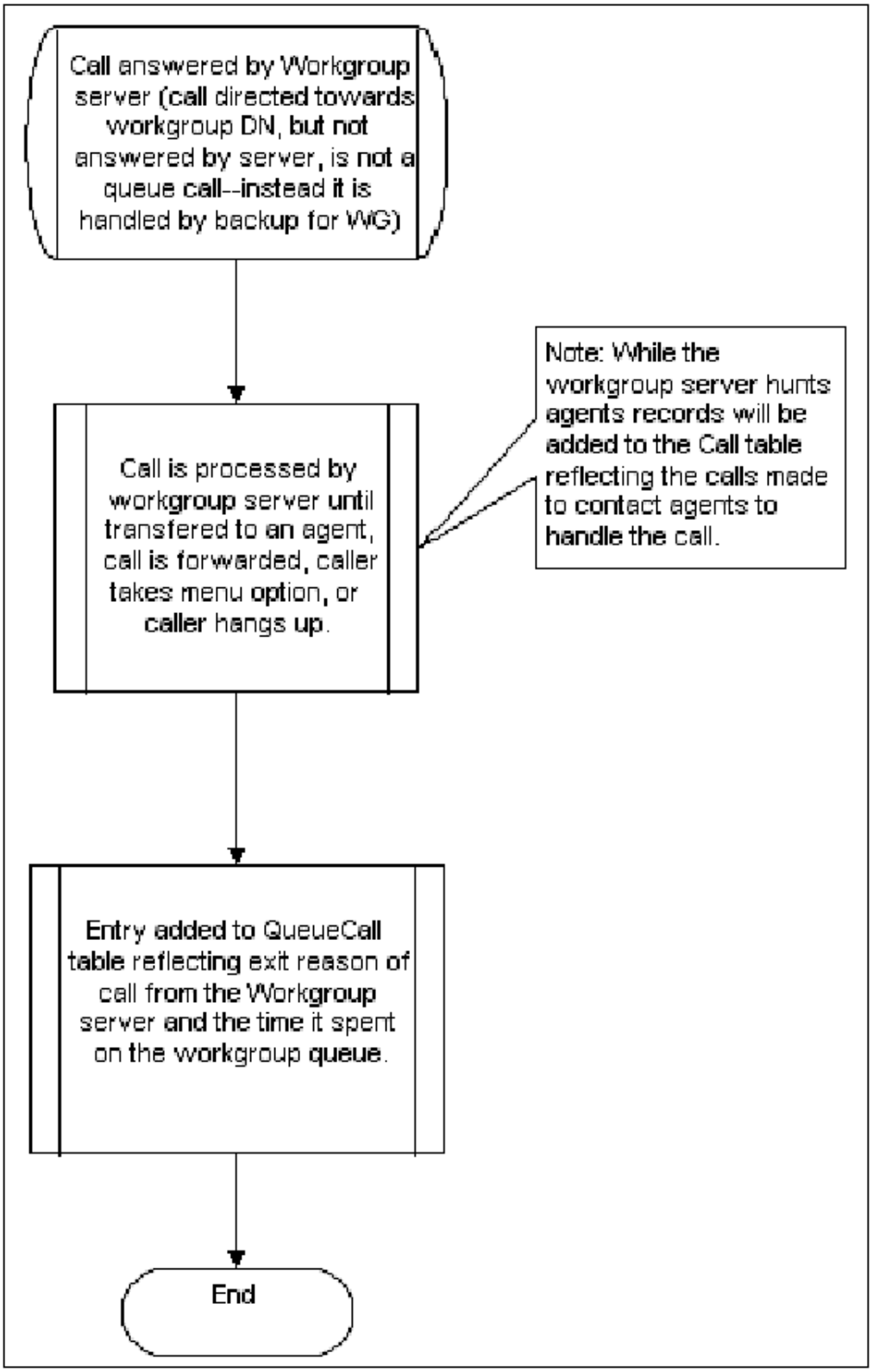
Each time a call is processed by the workgroup server, an entry is made in the Queue Call table. A workgroup is a call queuing mechanism, thus the name “Queue Call” in the CDR database.

Each time a call is made to a workgroup when the workgroup server is operational, an entry is made in the Queue Call table; moreover, there is only one entry for each call. In other words, one and only one entry appears for each call. A call can be made to the

workgroup dialed number, but if the workgroup server does not process the call, an entry is not made in the Queue Call table for the call. Moreover, the call will not be marked as a workgroup call in the call table.

The following figure illustrates how updates are made to the Queue Call table.

Figure 31: New Entries to the CallQueue Table



Each entry in the Queue Call table contains the following fields as shown in the following table.

Table 260: Queue Call Table Field Descriptions

Field Name	Data Type	Description
ID	AutoNumber	Unique identifier. (4-byte integer, required)
CallID	Number	Unique number for the existence of the call. (4-byte integer)
ConnectTableID	Number	Link to Connect Table ID Key. You can find more information about the connection to the call in the connect table. The Connect table entry here is for the Workgroup DNs connection to the call. If you want information from the Call table entry for this call, the reference to the Call table in the Connect entry should be used to find the Call table entry. (4-byte integer)
StartTime	Date/Time	The time at which the call is answered by the workgroup server, thereby beginning it's time on the call queue (workgroup) DN. (8-byte date/time)
Duration	Date/Time	Time from when the call is offered to the workgroup DN until it leaves the call queue. The call leaves the queue when it is answered by an agent, is abandoned by the calling party, or leaves the queue for other reasons. The complete lists of reasons for leaving the queue are found in the QueueExitReasonLUT table. (8-byte date/time)
DurationSeconds	Number	Duration expressed in number of seconds. (4-byte integer)

Field Name	Data Type	Description
QueueName	Text	Name of the call queue (workgroup). (50 characters, zero-length)
QueueDN	Text	Extension number of the call queue (workgroup). (15 characters, zero-length)
ExitReason	Number	Enumerated reason the call left the call queue (see the QueueExitReasonLUT for enumerations). (1-byte integer)
TargetType	Number	Enumerated type of handoff target (see TargetTypeLUT for enumerations). (1-byte integer)
TargetFirstName	Text	Name or first name of target. (50 characters, zero-length)
TargetLastName	Text	Last name of target if applicable (blank if the target agent doesn't have a last name in the configuration database). (50 characters, zero-length)
TargetDN	Text	Dialed number of target. (15 characters, zero-length)
Archived	Yes/No	Has this entry been archived? (boolean)

- Partial records are never written. A record is written only once, either when the call is abandoned, the call is connected to an agent, or leaves the queue for other reasons as enumerated in QueueExitReasonLUT.
- If QueueExitReason – Abandon, target information (TargetType, TargetFirstName, TargetLastName, TargetDN) is meaningless and will be blank.
- If QueueExitReason is TransferToAgent, the TargetFirstName and TargetLastName are filled in with information about the agent.

- If the QueueExitReason is Forwarding (2, 3, 4, or 5 for forward always, busy, no answer, or no logged in agent) or transfer (9, 10, and 11 for transfer to a menu, extension or voice mail), the DN that the call is being forwarded or transferred to is provided in the TargetDN field. However, the TargetFirstName and TargetLastName are not provided.
- A QueueExitReason is always entered. The field will never be blank. “Unknown” will only be used in the case of failure (and maybe not at all).

26.4.4.5.1 Enumeration Tables Used for Queue Call

The following table describes the elements in the Queue Call Exit Reason Enumeration table.

Table 261: Queue Call Exit Reason Enumeration Table

ExitReason	Name	Description
0	Null	
1	TransferToAgent	Hunt succeeded and transferred to agent.
2	ForwardAlways	Workgroup forwarding all calls.
3	ForwardBusy	All logged in agents on call.
4	ForwardNoAnswer	All available agents did not answer.
5	FwdNoLoginAgent	No logged in agents.
6	ForwardMaxRings	Reached max number of rings before agent found.
7	Abandon	Call dropped while in WG or Queue.
8	Reserved	

ExitReason	Name	Description
9	TransferVM	Option taken to transfer to voice mail
10	TransferExtension	Option taken to transfer to an extension.
11	TransferMenu	Option taken to transfer to a menu.
12	Pickup	Agent picked up call from queue.
13	Unpark	Agent picked up from queue out of order.
14	Overflow	Overflow
15	Interflow	Interflow

- ForwardMaxRings is no longer used.
- Exit Reasons for Forwarding (2-5) reflects the call being forwarded from the workgroup. These are used when the call leaves the workgroup as a result of call routing and the call routing indicates to forward the call to an internal or external number. Call routing can also indicate that the call is entering the call queue for the workgroup. In that case, these exit reasons are not used because the call does not exit the queue at that point.
- Exit Reason 8, Abandon, is used when the caller drops the call either by physically hanging up or by taking an option on a Queue Step to hang up.
- Even after a call is forwarded to the queue, it remains on the queue and it may still be successfully transferred to an agent or abandoned. Exit Reason 1 or 7 is recorded if either of these occurs.

- In addition to a call being successfully hunted or abandoned while on the queue, it may exit the queue because of an option taken during a queue step. The call will exit the queue if the caller takes any of the following options:
  - **Take a message**
  - **Transfer to extension**
  - **Go to menu**
  - **Exit reasons 9, 10, and 11 have been added to cover these cases**.

The following table describes the elements in the Queue Call Target Type Enumeration table.

Table 262: Queue Call Target Type Enumeration Table

Target #	TargetType	Description
0	Null	
1	Agent	Workgroup agent.
2	Menu	A menu on the Mitel system.
3	Mailbox	A mailbox on the Mitel system.
4	OtherIntrnExtrn	Any other extensions to which the call is targeted.

26.4.4.6 Queue Step Table

The Queue Step table logs data about time spent in queue steps or in hunting for agents. The following table describes the elements in the Queue Step table.

Table 263: Queue Call Field Descriptions

Field Name	Data Type	Description
ID	AutoNumber	Unique identifier. (4-byte integer, required)

Field Name	Data Type	Description
QcallTableID	Number	Link to the Autonumber field in the Queue Call table. Thisessentially identifies the Queue Call that this step is associatedwith. (4-byte integer)
StartTime	Date/Time	Time at which the call first enters this step. (8-byte date/time)
Duration	Date/Time	Elapsed time spent in this step. (8-byte date/time)
DurationSeconds	Number	Elapsed seconds spent in this step. (4-byte integer)
StepNumber	Number	Step number if this is not a hunting record (as identified by theHunting field set to Yes). The step number corresponds to thestep number in the workgroup configuration.
ExitReason	Number	Enumerated reason for exit from step. (1-byte integer)
Hunting	Yes/No	If true the times correspond to hunting, or else this indicates aqueue step. (boolean)

There is a record for each period that the call spends hunting and for each period a call spends in a queue step. For example, if a call to a workgroup initially hunts for agents, then goes to the queue and exits the workgroup from that queue step, there will be two records for the call in the Queue Step table. The first record would be for hunting (the duration may be zero if, for example, no agents were logged in). The second record is for the first queue step from which the call exited.

26.5 Web Tables

Web tables log call data for audio only, web only, and audio and web conferences.

26.5.1 Audio Only Conference

- The Connect table includes a record for each leg of the conference.
- All legs in the same conference have a similar Call.CallID.
- No records are added to web_session and web_attendee tables.

26.5.2 Web Only Conference

- A meeting session record is written to the web_session table after the meeting ends.
- A record is written to the web_attendee table for each attendee.
- No records are added to the Call and Connect tables.

26.5.3 Audio and Web Conference

- The Connect table includes a record for each leg of the conference.
- All legs in the same conference have a similar Call.CallID.
- A meeting session record is written to the web_session table after the meeting ends.
- A record is written to the web_attendee table for each attendee.
- The Web_session table holds a CallID that references Call.CallID. If a web attendee reconciles his or her audio leg, web_attendee.caller_id references Connect.PartyID.

26.5.4 Web Session Table

The following table provides information about the elements that appear in the log for web sessions.

Table 264: Elements in the Web Session Log

Field Name	Data Type	Description
Id	AutoNumber	The session ID referenced by the attendee table
meeting_title	Text	Title of the meeting

Field Name	Data Type	Description
meeting_desc	Text	Description of the meeting
meeting_type	Text	Normal, open or panel
start_time	Date/Time	Local time of the service appliance when the meeting session started
start_local_time	Date/Time	Local time of Headquarters server when meeting session started
start_utc_time	Date/Time	UTC time meeting session started
start_local_dst_flag	Yes/No	Flag to set the service appliance server dst flag
start_hq_dst_flag	Yes/No	Flag to set HQ dst flag
end_time	Date/Time	Local time of service appliance server when meeting session ended
end_local_time	Date/Time	Local time of Headquarters server when meeting session ended
end_utc_time	Date/Time	UTC time meeting session ended
end_local_dst_flag	Yes/No	Flag to set local dst flag of service appliance server
end_hq_dst_flag	Yes/No	Flag to set HQ dst flag
host_login	Text	Login name of meeting host
login_type	Text	Name, password, registration, none

Field Name	Data Type	Description
Scheduled	Yes/No	'Y' or 'N'
Public	Yes/No	'Y' or 'N'
Server	Text	IP address of a Service Appliance
moderator_code	Text	Moderator's access code
Attendee_code	Text	Attendee's access code
CallID	Number	CallID associated with conference call. NULL for web only conference.
Archived	Yes/No	Has this entry been archived?

26.5.5 Web Attendee Table

The following table provides information about the elements that appear in the log for web session attendees.

Table 265: Elements In Web Attendee Log

Field Name	Data Type	Description
session_id	Number	References ID from web_session table
start_time	Date/Time	Local time of service appliance server when attendee joined session
start_local_time	Date/Time	Local time of Headquarters server when attendee joined session
start_utc_time	Date/Time	UTC time attendee joined session

Field Name	Data Type	Description
start_local_dst_flag	Yes/No	Flag to set service appliance server dst flag
start_hq_dst_flag	Yes/No	Flag to set HQ dst flag
end_time	Date/Time	Local time of service appliance server when attendee left session
end_local_time	Date/Time	Local time of Headquarters server when attendee left session
end_utc_time	Date/Time	UTC time attendee left session
end_local_dst_flag	Yes/No	Flag to set service appliance server dst flag
end_hq_dst_flag	Yes/No	Flag to set HQ dst flag
break_time	Number	Time attendee is absent from meeting
user_name	Text	Login name of attendee
user_ip	Text	Attendee's IP address
caller_id	Text	Caller's phone number

26.6 Legacy CDR Text Files

The call accounting service automatically generates a daily legacy CDR text file for use by third-party call accounting applications. These packages typically provide numerous reports, including:

- Call accounting, cost allocation
- Most frequently dialed numbers

- Most costly dialed numbers
- Most costly users
- Trunk utilization
- Toll fraud

The `CDR*.log` files are text files created daily at midnight. It contains call records from midnight to midnight. Any call records that span the midnight hour will be recorded on the day that calls are completed.

26.6.1 Format

The file name format for the daily CDR-YYMMDD.HHMMSS.log where

- YY, MM, and DD are zero-padded character strings that represent the year, month, and day of the date when the file was created.
- HH, MM, and SS are zero-padded character strings that represent the hour, minute, and second of the time when the file was created.

Call records are entered in the log file in the order of when the call was completed and not when it began.

It is the responsibility of the third-party reporting application to delete the daily log files.

The format of the record is column based, must be justified correctly, and end with a carriage return and line feed. A single blank character is inserted between each data field for readability. The following table provides information about elements in the CDR text file.

Table 266: CDR Text File Field Definitions

Field	Column	Length	Comment
Call ID	1	10right just ified	A unique ID that represents the call. The Call ID is mea nt to be unique for the duration while it's active.
Date	12	10	Date of the call given in month, day, and year: mm/dd/ yyyy
Time	23	8	Start of the call given in hours, minutes, and seconds: hh:mm:ss
Extension	32	16left justified	Inbound or outbound extension ID. Last valid party on the call. Valid parties include user extension and ope rator but not voice mail or auto-attendant.
Duration	49	8	Call duration given in hours, minutes, and seconds. hh:mm:ss

Field	Column	Length	Comment
Call Direction	58	1	Incoming/outgoing flag 0 – Incoming 1 – Outgoing 2 – Inbound Tandem Call (Tandem Trunking) 3 – Outbound Tandem Call (Tandem Trunking) **Note**: A call is recognized as a tandem call based on the configuration setting in the Trunk Group involved in the call.
Dialed Number	60	16 left just ified	Contains the number dialed but does not include any access code, such as 9, to seize the trunk. Valid only f or outbound calls.
Caller ID	77	16 left just ified	Blocked or unavailable information will be reported as b locked or unavailable in text. Valid only for incoming c alls.
Trunk Group	99	3 right just ified	The Trunk group ID.
Account Code	103	20	The account code entered by the caller.
CR /LF	124		Carriage return.

26.7 Talk Time Record

Call Detail Records provide a complete logging of all non “Private” calls placed in or out of the Mitel system. These logs include call volume, call origination, call destination and the length of each call.

The Talk Time Enhancement feature increases the usability of log data from the Call Detail Records by compiling only the actual time spent in a conversation between the calling parties. All call ring back time is eliminated from the Call Detail Records retaining only the actual Talk Time spent on the call.

When a call is placed the destination phone acknowledges and a ring tone is provided to both parties. The time of the call starts on the first ring and terminates when the calling parties hang up. The Mitel Appliance uses the Telephony Management Service (TMS) to report the call and it's the time to the Headquarters server. There the call is captured in the Call Detail Records. The entire length of the call is logged here, including the first ring up to the entire call tear down.

Talk Time Enhancements uses the FarEndAnswered event provided by certain trunks to determine when the called party answers the call. The length of time the call has been answered is reported to the CDR. If you choose to include unanswered calls in the CDR, these calls are reported with a duration of zero. For information about including unanswered calls in the report, see Configuring Reporting Options on page 959.

Calls placed over Digital Wink, PRI, BRI or SIP trunks support FarEndAnswered events. These events mark the moment when the called party answers the call. Talk Time Enhancement uses this event to report the Talk Time of the call to the Call Detail Records. The Call time represents only the actual Talk Time of the call. Calls over Analog loop start and Digital loop start trunks do not support FarEndAnswered events. These calls still report to the CDR through TMS, but their time values include the time for Ring Back.

As administrators evaluate CDR reports, an understanding of the trunk types that support Talk Time Enhancement helps them to gain an accurate picture of the talk time being reported in the CDR.

26.8 MySQL Database

The system supports CDR records and related queries in a MySQL database. The maximum supported size for MySQL database and database table depends on the operating system and MySQL version on the main server. For more information, refer to the documentation specific to your operating system and MySQL version.

The data in the MySQL files can be viewed using a new **Web-Based Reporting** feature from Connect Director. (See the Introduction on page 891 for more information.) Alternatively, administrators can use common database command utilities in a command line interface to dump and restore files.

Connect Director provides the access for generating CDR reports, as Introduction on page 891 describes.

Connect Director also lets you start, stop, and monitor the health status of MySQL databases. To do so, navigate to **Maintenance** > **Services** and then select **MySQL** in the table on the **Services** page.

26.8.1 Compatibility and PreConfiguration Requirements

This section describes the issues that an administrator must understand and accommodate before installing or upgrading the MySQL databases.

26.8.1.1 Disk Space Requirements

Storing call detail records for 50,000 workgroup calls requires a 1.5 GB MySQL database. Implementing a database of this size typically requires 4.0 GB of disk space. This requirement includes disk space for the main database (1.5 GB), the archive database (1.5 GB), and temporary space required to generate reports (1.0 GB).

Although the main and archive databases are typically stored on the same server, MySQL permits the storage of the databases on different servers.

26.8.1.2 Compatibility with Utility Programs

Mitel should run on a dedicated server. Other programs that access MySQL databases might not be compatible with Mitel, resulting in installation and data integrity issues. Before installing Mitel on a server, remove all existing MySQL programs and databases.

Virus Checkers: Virus checker utilities that run on the server must exclude MySQL database files. Specifically, if a virus checker is running on the server, it must exclude the MySQL CDR Database file from the anti-virus utility (wherever ShoreLine Data installed, such as \Shoreline Data\Call Records 2\Data\[ibdata1, ib_logfile0, ib_logfile1]). If these files are not in the exclusion list, the MySQL service stops.

Disk or Backup utilities: MySQL database files must be excluded from all disk or backup utilities running on the server. Failure to exclude the database causes a MySQL failure.

To restart the database after a failure, access the MySQL Service page from Connect Director by selecting Maintenance > Services in the menu page and then selecting MySQL in the table on the **Services** page.

26.8.2 Archival and Backup Utilities

This section introduces the database archival, backup, and replication tools. The following table summarizes the service availability for these features.

Table 267: Archival, Backup, and Replication Services Availability

Field	Backup	Archive (Secondary S erver)	Replication
Technical Assistance Support	Yes	Yes	No

Field	Backup	Archive (Secondary S erver)	Replication
Additional MySQL License Required	No	Yes	Yes
Execution	Manual	Daily	Online
Reports run on remote machine	No	Yes	No
Complete restoration if HQ fails	Yes	Possible through manual recovery	Yes

26.8.2.1 Record Retention Periods

In the **Reporting Options** page, you can specify the number of days that a database keeps a Call Detail Record. To access the **Reporting Options** page, navigate to **Reporting** > **Options** in Connect Director.

- **Retention Period for CDR Data** specifies the number of days that records remain in the main CDR database. The system deletes the oldest records from the archive database each day. The default period for CDR data retention is 36 days.
- **Retention Period for CDR Archive** specifies the number of days that records remain in the MySQL archive database on a secondary server. The system deletes the oldest records from the archive database each day. The default period for CDR archive retention is 125 days.

26.8.2.2 Database Archive Utility

The archive utility provides a method of removing older records from the main database and storing them in an archive database. Archiving older records into a separate database reduces the storage requirements of the main database, which reduces the time required to search for specific records or generate reports. The archived database provides the same set of services as the main database.

Archival services are configured and enabled in Connect Director, where you can specify the number of days that records are maintained in the main database and in the archive database. When archiving is enabled, archival services are performed daily. The archival service copies records to the archive database that exceed the main database age limit, then removes those records from the main database. Records that exceed the age limit for the archive database are removed from the archive database. Age limits are established separately for each database; valid limits range from one to 2000 days. The default age limits for each database is 125 days.

Example: A sample implementation sets a 30 day limit on the main database and a 365 day limit on the archive database. In this case, the main database contains records for calls handled during the past 30 days while the archive database contains records for calls handled during the past 365 days.

The Backup utility can be used for record storage requirements that exceed 2,000 days.

Creating an archive database:

1. Run `MakeCDRArchive -d databasename`, where `databasename` is the name of the archive database to be created.
2. Access the **Reporting Options** page in Connect Director (**Reporting** > **Options** from the Menu page) to configure Mitel to access the archive database.

26.8.2.3 Database Backup Utility

The Backup utility creates a copy of a database. The copy can be restored at a later time and at a different location. The Backup utility differs from the Archival utility as follows:

- Archiving is configured once then performed daily. Backups are performed only when a command is executed.
- Archival operations are configured from Connect Director. Backups are performed from the command line.
- Archive databases can be accessed directly to generate reports. Backup databases must be restored before performing search and report generation tasks.

Backup and Restore operations can be performed without shutting down the MySQL service. Performing these operations during off peak hours reduces the execution time and the impact on other system services.

The file located at `C:\Program Files (x86)\Shoreline Communications \ShoreWare Server\MySQL\MySQL Server\Examples\BackupCDR.bat` is an example of a batch file that backs up a MySQL CDR database under generic default conditions. This file can be used as a template for creating a batch file that backs up the database under specific conditions. The password is **shorewaredba.** Backing up a 1.5 GB database requires 200 seconds.

Search at http://dev.mysql.com for MySQL backup tools, add-ons, and documentation.

26.8.2.4 Database Restore Utility

Restoring a database copies the records in the backup database file to the database specified in the restore command. Records in the backup file that are duplicates of records in the target database are listed in the log file and are not restored.

The file located at `C:\Program Files (x86)\Shoreline Communications \ShoreWare Server\MySQL\MySQL Server\Examples\RestoreCDR.bat` is an example of a batch file that restores a MySQL CDR database under generic default conditions. This file can be used as a template for creating a batch file that restores the database under specific conditions. The password is **shorewaredba**.

Note:

Restoring a 1.5 GB database typically takes 1200 seconds.

26.8.2.5 Database Replication

MySQL provides a Database Replication tool. For information, see the following websites:

- http://www.howtoforge.com/mysql_database_replication provides information for setting up the replication of MySQL databases.
- http://www.mysql.com/ to search for tools and add-ons that assist with database replication.

26.8.3 Installing and Upgrading MySQL Archive and ODBC Connector on Secondary Server

Mitel supports the archiving of MySQL databases on a Secondary server (separate from the Headquarters server). This section describes how to:

- Install and activate an archive of the CDR database on a secondary server
- Upgrade the archive on a secondary server to MySQL 5.7.37 Community Edition (the current release)

Note:
Before you upgrade your system from 19.1 or earlier versions to 19.2, it is mandatory that you disable the Distributed Database feature. After the upgrade process is complete, if required, you can manually re-enable the Distributed Database feature.

For a new MySQL installation, the tasks are as follows:

- Install the MySQL database on the Secondary server.
- Specify that database as an archive.

Although similar to a new installation procedure, the upgrade of the archive from MySQL 5.6.40 to 5.7.37 Community Edition involves some additional tasks.

To conserve resources on the main server, the most logical place for an archive database is a secondary server (although the archive can also exist on the main server). For

the current release of Mitel software, a separate, licensed copy of 5.7.37 Community Edition is required for a new Mitel system or an upgrade of the database that resides on a secondary server.

26.8.3.1 Installing MySQL on a Secondary Server

To install MySQL on a secondary server, perform the steps that follow. In these steps, replace the default location of **C:\Program Files (x86)\...** with the location on the server of the installed MySQL if the location is different from the default.

In general, this task includes the following details:

- The type of installation is Custom (for specifying individual features).
- Changing the default User ID from “root” to the customer’s preference.
- Changing the default password from “shorewaredba” to the customer’s preference.
- Specifying the UTF8 character set as part of the installation.
- Specifying port 4309 and it specifying pacing the port in firewall exception list.

Note:

- For the current release of the Mitel system, the version of MySQL to be installed on the secondary server is MYSQL Server 5.7.37 Community Edition
- Before you upgrade your system from 19.1 or earlier versions to 19.2, it is mandatory that you disable the Distributed Database feature. After the upgrade process is complete, if required, you can manually re-enable the Distributed Database feature.

1. On the Secondary server, open a browser and navigate to MySQL.com.
2. Download the appropriate MySQL 5.7.37 Community Edition installer to the following default location or to an alternative location of the customer’s choice:

   ```
   C:\Program Files (x86)\Shoreline Communications\ShoreWare
   Server\MySQLCDR\MySQL Server
   ```

   Note:
   MySQL 5.7.37 Community Edition is supported.

3. Launch the installer. The first window to appear is the Welcome window. It displays the version of MySQL that will be installed.

4. Click **Next** in the Welcome window.

   The Setup Type page of the wizard is displayed.
5. Select the default option and then click **Next**.

> **Note**:
>
> While installing MySQL on the secondary server, use the default MySQL installation options unless otherwise specified in this Administration Guide.

6. Select **C Include Files / Lib Files**, and then click **Next**.

   The MySQL dialog box is displayed.
7. Click **Next**.

   The Wizard Completed page is displayed.
8. Select the following check boxes, and then click **Next**:

   - **Configure the MySQL Server now**
   - **Register the MySQL Server now**

   The MySQL Server Instance Configuration Wizard Starts.
9. Select **Detailed Configuration**, and then click **Next**.

   The select server page is displayed.
10. Select **Developer Machine**, and then click **Next**.
11. Back up the file to C:\Program Files\MySQL\MySQL Server 5.7\my.ini from the Secondary server to a safe location (C:\MySQL_backup, for example).
12. Back up the files c:\Program Files\MySQL\MySQL Server 5.7\Data\[ib_logfile*] from the Secondary server to a safe location (C:\MySQL_backup, for example).
13. Select **Start** > **Administrative Tools** > **Services** > **MySQL** on the server.
14. Click **Stop the service** and check that MySQL service status is blank.

15. Compare the following values of specific fields in the archive_*MySQL_my.ini* file in the Main server directory with the values in the Secondary server's *my.ini* file:

    Main server directory—*C:\Program Files\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server 5.7\Examples\archive_MySQL_my.ini*

    Secondary server file— *C:\Program Files\MySQL\MySql Server 5.7\my.ini*

    Ensure that all the values in the *archive_MySQL_my.ini*are appropriate and update the same values to my.ini file of the secondary server. The *archive_MySQL_my.ini* values should be:

    [mysql]

    default-character-set – utf8

    [mysqld]

    default-character-set – utf8

    tmp_table_size – 30M

    key_buffer_size – 2M

    read_buffer_size – 2M

    read_rnd_buffer_size – 2M

    sort_buffer_size – 2M

    innodb_additional_mem_pool_size – 2M

    innodb_flush_log_at_trx_commit – 0

    innodb_file_per_table

    innodb_buffer_pool_size – 150M

    innodb_log_buffer_size – 5M

    innodb_log_file_size – 24M

    default-storage-engine – INNODB

16. Delete the file `ib_logfile*` from the Secondary server directory (c:\Program Files \MySQL\MySQL Server 5.7\Data).
17. Ensure that the value for innodb_flush_log_at_trx_commit is 0 on the Secondary server (C:\Program Files\MySQL\MySql Server 5.7).

Note:

If the value is not 0, the archiving operation is more than 20 times slower.

18. Select **Start** > **Administrative Tools** > **Services** > **MySQL**
19. Click **Restart the service** and verify that MySQL has returned to service.

26.8.3.2 Install and Verify the ODBC 5.3.4 (32-bit) Driver

You must install this 32-bit ODBC driver because the MakeCDRArchive is a 32-bit application.

Note:

Please note the following pre-requisites to installing this 32-bit application on 64-bit operating systems:

- For any supported version of Windows Server, the Microsoft C++ 2010 x86 runtime libraries must be installed. If they are not, visit the Microsoft web site to download the Microsoft Visual C++ 2010 Redistributable Package (x86).

Refer to the *Release Notes* (formerly called Build Notice) for information about supported versions of Windows Server.

Complete the following steps to install the 32-bit ODBC driver:

1. Launch the MySQL Community installer that you installed in Installing MySQL on a Secondary Server on page 1037.
2. Click **Add**, expand the **MySQL Connectors** item, and then select **Connector/ODBC 5.3.4 X86**.
3. Click the right arrow to move **Connector/ODBC 5.3.4 X86** to the **Products/Features To Be Installed** section.
4. Click **Next**, and then click **Execute** to complete the installation.

When installation is complete, view the ODBC driver version in the registry editor to verify that the 5.3.4 X86 version is installed.

26.8.3.3 Upgrading MySQL on a Secondary Server

To upgrade MySQL on a secondary server, perform these steps:

1. Upgrade the MySQL version if required. To upgrade the MySQL version, follow the steps in Installing MySQL on a Secondary Server on page 1037.
2. Upgrade the OBDC connector if required. To upgrade the OBDC connector, see the steps in Install and Verify the ODBC 5.3.4 (32-bit) Driver on page 1040.
3. Upgrade the Archive database (db) required. To upgrade the Archive database, perform these steps:

   a. Copy the following files from `<Install Drive>\Program Files\Shoreline Communications\Shoreware Server` to the Archive server:

      - `Archive.ini`
      - `MakeCDR.dll`
      - `MakeCDR.sql`
      - `MakeCDR_sp.sql`
      - `MakeCDRArchive.exe`

   b. Open **Command Prompt** with admin privileges and run the `MakeCDRArchive.exe -d <DBName>` and `MakeCDRArchive.exe –h` commands. These commands give the help information and the options that are required to run Archiving.

26.8.3.4 Convert the Database

Complete the following steps to convert the database on the secondary server into an archive database:

1. Verify the following files are placed in an equivalent location on the Secondary Server to that on the Main servers (default location is \\Shoreline Communications \Shoreware Server)

   - `Archive.ini`
   - `MakeCDR.dll`
   - `MakeCDR.sql`
   - `MakeCDR_sp.sql`
   - `MakeCDRArchive.exe`

2. Run `MakeCDRArchive –d databasename`, where `databasename` is the name for the archive.

Note:

Navigate to **Reporting** > **Options** to specify the name of the archive database.

26.8.3.5 Performance Tuning for Report Generation

When improving on the CDR report generation performance, increase INNODB_BUFFER_POOL_SIZE defined in `C:\windows\my.ini` based as specified

Default setting:

- INNODB_BUFFER_POOL_SIZE – 150 MB

  If the database contains more than 350,000 records, set

- INNODB_BUFFER_POOL_SIZE – 200 MB

  If the database contains more than 500,000 records, set

- INNODB_BUFFER_POOL_SIZE – 250 MB

26.8.3.6 Report Generation Time – CPU Utilization

The time to display a report from the first page to the last page can take up to ten minutes (for the largest possible report). Although the priority of Report Generation process is low, generating large reports can affect the performance of call processing. To avoid performance degradation, do not generate large CDR reports during peak call loads.

26.8.3.7 MySQL CDR Database and Internationalization

MySQL CDR Database supports the UTF-8 character set. All CDR data in the database is stored in the UTF-8 character set.

26.8.3.7.1 Monitor MySQL service

To monitor and, when necessary, restart the Mitel-MYSQLCDR service, in Connect Director select **Maintenance** > **Status** > **Servers** to see the **Servers** page, and then select **Mitel-MYSQLCDR** in the list of services at the bottom of the page. If the service needs to be restarted, select the service and in the **Command** section, select **Start** and click **Apply**.

26.8.4 Tools for Browsing MySQL Database Tables

MySQL provides MySQL Query Browser as part of their GUI Tools. You can use the MySQL Query Browser to browse and view the queries. To download MySQL tools, open the MySQL home page and download the MySQL Workbench.

The open source tool (http://www.webyog.com/en/downloads.php) is available to view the CDR tables defined in MySQL.

Browsing a large CDR database on the Headquarters server may potentially degrade the call processing server.

A large amount of temporary disk space may be used by these MySQL browser tools. To avoid affecting call processing performance on the Headquarters server, you can use a query with LIMIT criteria to show a subset of rows.

26.8.5 Restrictions in the Number of Records Returned by the MySQL CDR Query

A CDR database query that exceeds 300,000 records might degrade performance if it includes certain reports, such those for Trunk Activity Detail and Trunk Activity Summary. Increasing the amount of free disk space can reduce this problem. Changing the query filter so the number of returned records is under 300,000 can also help.

Centralized Dial Number (DN) 27

MiVoice Connect supports Centralized Dial Numbers (DN), which guarantee the data integrity for DN references within the system. When administrators delete a particular DN, Centralized DN checks all the references to that DN across the system. Depending on the significance of references to the DN to be deleted, the system either allows the deletion by removing all the DN references or prevents the deletion by prompting the administrator with a message indicating that the referenced DN cannot be deleted.

To delete non-significant references together with the DN eliminates the unnecessary pop-up messages when administrators delete an unwanted DN, which simplifies DN management for the administrator. The following table provides information about the centralized dial number table as it relates to the MiVoice Connect system.

Table 268: Centralized Dial Numbers (DN) Table

Deleting an Extension	System Behavior
Hunt Group	
Backup Extension	deletion not available
Call-forwarding destination (call stack full)	delete silently
Call-forwarding destination (no answer)	delete silently
Members	delete silently
Escalation Profile	
Automatic Message Forwarding	delete silently
Escalation Step (Notification Number)	delete silently
Find Me	
Primary destination	delete silently

Deleting an Extension	System Behavior
Backup destination	delete silently
Users	
Mailbox for Recorded Calls	delete silently
Delayed Ringdown	delete silently
Programmable Button	
Toolbars	delete silently
User Availability States	
Always Destination:	set to DN Type =4
Busy Destination	set to DN Type =4
No Answer Destination	set to DN Type =4
Personal Assistant	delete silently
Extension List	
User Ext List	delete silently
User Availability States Defaults	
Always Destination:	set to DN Type = 4
Busy Destination	set to DN Type = 4

Deleting an Extension	System Behavior
No Answer Destination	set to DN Type = 4
Personal Assistant	delete silently
Availability States Delegation	delete silently
Bridged Call Appearance (BCA)	
Backup Extension	delete silently
Call Stack Full	delete silently
No Answer	delete silently
System Distribution Lists	delete silently
Workgroup	delete silently
Backup Extension	set to DN Type = 4
Availability States Workgroup Assistant	delete silently
Workgroup Assistant	delete silently
Members (Work Group Agents)	manual deletion required
Queue Handling Steps (Operation)	manual deletion required
Overflow DN (Queue Handling Steps)	manual deletion required
Route Point	

Deleting an Extension	System Behavior
Availability States	set to DN Type = 4
Assistant	delete silently
Auto-Attendant Menu	
Extension in Steps	manual deletion required
Group Paging	delete silently
Pickup Group	delete silently
AMIS	
Delivery Number	no impact
Callback Number	no impact
Class of Service	
Directed Paging	delete silently
Barge In	delete silently
Record Other's Calls	delete silently
Silent Monitor	delete silently