Mobility Router Administration Guide

July 2023

Document Version 1.0

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.

Table of Contents

Before You Start

This guide is written for the Administrator of the Mobility Router for single-tenant and must be used in conjunction with the mobility solution. For more information about related components and documentation, refer to “Related Documentation” on page 13. The Administrator must be familiar with routing, voice and data configuration, and PBX functionality to use this guide effectively.

Organization

This guide is documented as described in the following sections.

Chapter	Title	Description
1	Mobility Router Architecture	Overview of Mobility Router and mobility solution.
2	Getting Started	High-level feature and User Interface description of the Mobility Router.
3	Configuring System Settings	Configure the date and time and logging of events to help you monitor the system.
4	Configuring Network Settings	Configure hostname, Ethernet interfaces, and routing settings.
5	Managing Remote Access	Configure protocols, IP pools, call admission control, and enable groups and users for remote access.
6	Managing Security	Generate and import certificate authority, self-signed certificates, and other security-related requirements.
7	Configuring Authentication	Configure and manage authentication using Trusted Admin App, Local users authentication database.
8	Managing IP-PBX Integration	Configuring IP-PBX settings including SIP trunk, numbering plan, media, device mobility, and options.

Chapter	Title	Description
11	Configuring Voice Settings	Configure access numbers, SIP server settings, supported mobile device types, and import/export numbering plans.
12	Managing Calling Rules	Create and manage calling rule policies.
13	Managing Groups	Configure group settings including security, remote access, call routing options, and calling rules.
14	Managing Users	Configure user profiles including line-side settings, mobile device settings, additional devices, calling rules, home locations, and options.
15	Managing Redundancy Clusters	Configure and manage Mobility Router redundancy.
16	Maintaining the System	Configure and manage the Mobility Router's backup, restore, and restart functionality, and access the directory query feature.
17	Monitoring the System	Monitor the Mobility Router's dashboard including call status, user status, redundancy cluster status, and system status.
18	Troubleshooting	Managing client logs, Mobility Router logs, use the Numbering Plan Test Panel, Transmission Control Protocol (TCP) Dump, packet capture, and run network troubleshooting commands.
Appendix A	Deployment Best Practices	Employ the best practices for using the Mobility Router by utilizing this information in conjunction with the step-by-step procedures. Mobility Router Ports URL-Based Dialing Providing Android Client Images to Users without Direct Access to the Mobility Router
Appendix B	Third-Party Software Notices	This section contains the Third-Party Software Notices of RADVISION and OpenSSL.

What's new in this document?

This section describes changes in this document due to new and changed functionality in Mobility Router 9.0.

Table 1: Document Version 1.0

Feature/Enhancement	Update	Location	Publish Date
Updated Redundancy Clusters	About media maintenance during failover.	*About Redundancy Clusters*	February 2022
Special characters in user name	About special characters in user names.	*Configuring General Settings*	February 2022

Conventions

The following typographical marking conventions are used in this document.

Marking	Meaning
Bold	Names of interface objects, such as buttons and menus.
`Courier`	Code examples.
`Courier Italic`	Variables in code examples.
Blue	Cross references with hyperlinks. Click the blue text to go to the indicated section. All chapters have a list of section links on the first page. **Note:** Table of Contents entries are also links, but they are not shown in blue.

Related Documentation

Publications in the mobility solution documentation suite include the following:

- Mobility Router Administrator’s Guide (this document)
- Mobility Router Hardware Installation Guide
- Client (mobile device) User’s Guide
- Client (mobile device) Quick Reference Card
- Client Platform Support Guide
- Client Release Notes

Documentation for the new Connect client apps (Connect for iOS and Connect for Android) is available in knowledge base articles on the Mitel Support website.

CHAPTER

1

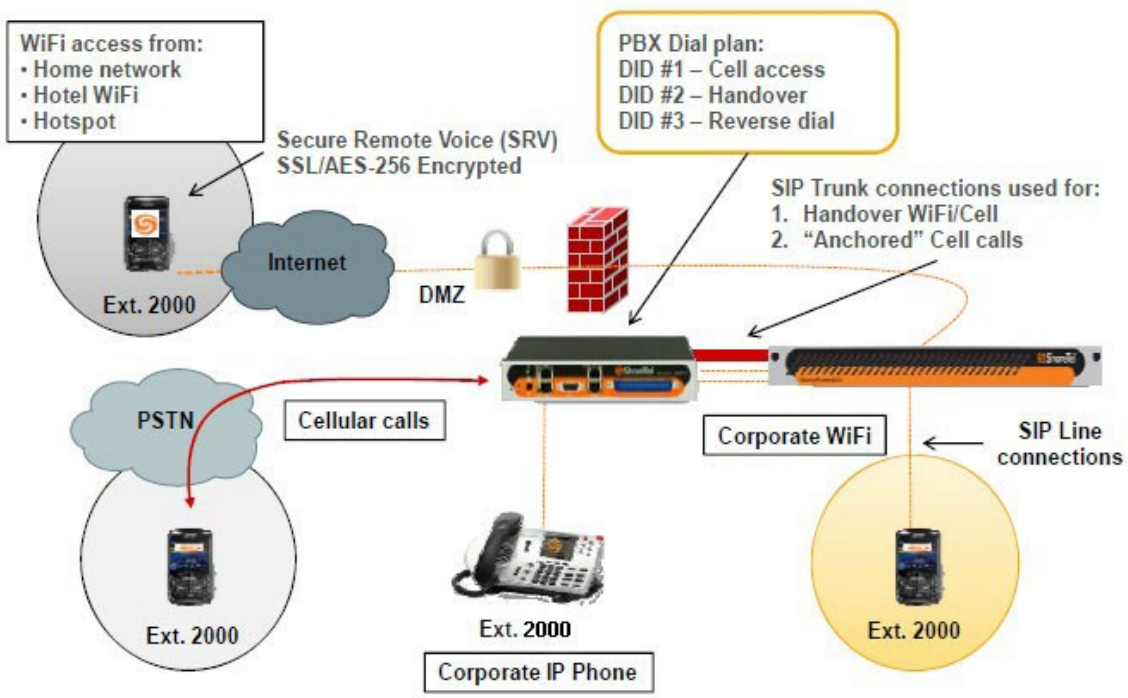
Mobility Router Architecture

The mobility solution is designed to make it predictable and simple for Administrators to create network transition points between Wi-Fi and Cellular networks where calls are expected to handover. The Mobility Router, a platform for mobile convergence, providing seamless location-based voice handover as users roam between Wi-Fi and cellular networks, uses various metrics, such as voice quality, signal strength, packet loss, jitter, Signal to Noise Ratio (SNR), and battery life to make decisions on how calls are routed. When users are within the building, calls generally stay on Wi-Fi. As users walk outside, the Connect Platform (previously known as Mobility Client) and the Mobility Router jointly make a routing decision to provide seamless, zero-impact handover of an existing call. While within the building, the solution preserves the native Access Point-to-Access Point (AP-to-AP) roaming behavior of the Wireless Local Area Network (WLAN).

Figure 1 on page 15 shows an example of the mobility deployment topology. The Mobility Router communicates with the enterprise IP-PBX over line-side and over trunk-side interfaces. You must create an IP-PBX for each enterprise IP-PBX with which the Mobility Router communicates. The Mobility Router uses line-side interfaces to register Connect Platform to the respective IP-PBXs.

This allows the Mobility Router to send and receive calls to and from the Connect Platform using the line-side interfaces. The Mobility Router uses the trunk-side interface to send and receive calls from the Connect Platform when they are in a cellular network.

Figure 1: Example of a Mobility Deployment Topology



CHAPTER

2

Getting Started

The Mobility Router ships with the operating software already installed. For information about installing and initially configuring the Mobility Router, see the Mobility Router *Hardware Installation Guide.*

After initially setting up the Mobility Router, use the web-based interface to access the mobility administration portal and manage the mobility solution.

This chapter contains the following sections:

Before You Begin

For information about supported hardware and software that can be used with the mobility solution, including web browsers, supported devices and OSs, refer to the *Mitel Connect for iOS and Android.* In addition:

- Cookies must be enabled for your browser. For information about how to enable cookies, see your browser documentation.
- JavaScript must be enabled for your browser. For information about how to enable JavaScript, see your browser documentation.

Note

The CMR UI has been upgraded for Angular JS. In view of this, some of the earlier features have not been related in this Admin Guide. Refer to Mobility Router Platform Support Guide for more information.

Note

Web browsers no longer support Adobe Flash Player.

Accessing the Administration Portal

Using the Administration Portal requires that you log in with a user account that has administrator privileges.

Note

Administrators have root level privileges on the Mobility Router.

During the initial setup of the Mobility Router, you created a password for the default administrator account (admin). When you initially log in to the Administration Portal, log in with the default admin account. When creating the password for the administrator, ensure that the password meets the organizations Password policy.

You must ensure a strong password policy (minimum password length, mix of characters and symbols).

You can continue to use the Administrator account or create other accounts with administrator privileges to use and to manage the Mobility Router. For information about creating other administrator accounts, see Chapter 8.

To access the Administration Portal:

1. Using a Web browser, enter the IP address or hostname of the Mobility Router in the address bar using the following format:

   `https://Mobility-Router-address/admin`

   where *Mobility-Router-address* is the IP address or fully qualified domain name (FQDN) of the Mobility Router (for example, https://10.11.12.13/admin or https://sj.example.com/admin).

2. Type the user name and password and click **OK**.

3. Navigate inside the portal using “#” to separate the internal pages from the main part of the portal’s URL. Frequently used pages can be stored/bookmarked for quick navigation. You can also manually type the address in the browser address line.

Working with the Administration Portal User Interface

The Administration Portal consists of three panes:

- Top pane—Use to access the following primary sections of and log out from the Administration Portal.
  - Configuration—Use these pages to configure the Mobility Router.
  - Monitor—Use these pages to monitor the Mobility Router using real-time graphics, charts, and reports.
  - Maintenance—Use these pages to manage system images and perform system maintenance.
  - Troubleshooting—Use these pages when troubleshooting the mobility solution.
- Left pane—Navigates to the Administration Portal pages.
- Right pane—Configures the Administration Portal settings.

Navigating the Administration Portal

Navigate the Administration Portal by using the left pane. When Configuration is selected in the top pane, the left pane contains the following sections:

- Groups and Users
- Policies
- Voice
- Mobility
- Clustering (Mobility Router 4000 or 6000 only)
- System

When you click a menu item in a section, the associated child pages display underneath. For example, selecting **Groups and Users** on the left displays a **Groups** child page and a **User's** child page. Selecting one of the child pages displays associated elements on the right pane.

Some pages in the Administration Portal have subpages. If you are on a subpage and want to go back to its parent page, click the name of the parent page in the subpage's title. The parent page displays in the right pane. If you are on a subpage, you can also click the parent page's menu item in the left pane to access the parent page.

Working with Administration Portal Pages

There are some settings that you cannot modify using Administration Portal pages, as they are defined when a mobile device is provisioned during the Connect Platform installation. Any settings that you cannot modify with the Administration Portal are grayed out; you cannot select items from a grayed-out list or modify a grayed-out field.

Some Mobility Router configuration fields must be filled out before you click “Apply”; if there is missing information, the Mobility Router prompts you for additional information by highlighting these fields in red. Filling in the missing data allows you to continue.

Hints

Look for this symbol for details about functionality or a description of a parameter.

Pushpins

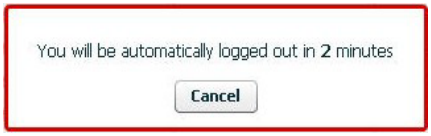
Use the pushpin to retain information on that page until you click the pushpin again or until you log out. If you pin a page that has subpages, all subpages are pinned. If you navigate away from a subpage to a page that is not its parent page, its information is retained when you return to the page. If you navigate to a parent page from a subpage that is pinned, information on the subpage is not retained.

If you click the pushpin on a page, no changes you have made on that page are lost, even after you have navigated to another page. By default, if you enter information and navigate to another page without clicking the pushpin or the Apply button, the information is not retained if you go back to the original page. If you click the pushpin on a monitoring page, the data shown reflects the current state of the Mobility Router; the data shown when you clicked the pushpin is not retained.

If you click a pushpin to “pin” the page, the information Automatic Inactivity Logout

If you do not use the Administration Portal for 17 minutes, you are automatically logged out and must log in again before you can continue. After 15 minutes of inactivity, the following message displays:

Figure 2: Inactivity Log Out Warning



To continue working with the Administration Portal, click Cancel. If you ignore the message, you are automatically logged out in two minutes.

To manually log out, see “Logging Out” on page 20.

Selecting All Rows

Right-click to select all rows on a page.

Copying a Selection

Copy a row or rows from tables to the clipboard. Select a table row and right-click to view a popup, then select **Copy selection**. This selection may then be pasted into any appropriate application.

Tip

When using expandable/collapsible tables rows, only the visible part of collapsed row is copied. Expand the folder to select each expanded row.

Saving Changes

If you make changes, click **Apply** to save. If you made changes on a page and navigate to another page without clicking the **Apply** button or using the pushpin, your changes are not saved or retained if you return to the page on which you made changes.

Logging Out

After you have finished using the Administration Portal, log out to prevent unauthorized changes. To log out:

1. From the Administration Portal, click **Logout** (located in the upper right corner).
2. Click **OK** to log out. A message confirming that you have logged out displays in the browser.

Note

Click **Cancel** to abort the logout process and remain logged in.

CHAPTER

3

Configuring System Settings

This chapter contains configuration details for setting the date and time for the Mobility Router, either manually or automatically using a Network Time Protocol (NTP) server, how to keep records and/or log events on the Mobility Router to help monitor the system, and entering Support/Contact information for Mobility Router client/user support. This chapter contains the following sections:

Refer to the following Chapters for other System settings:

- Networking: “Configuring Network Settings” on page 34
- Certificates: “Managing Security” on page 59
- Authentication: “Configuring Authentication” on page 69
- Licensing: “Managing Licenses” on page 31

Setting the System Date and Time

You can manually set the system date and time for the Mobility Router or configure it to use a Network Time Protocol (NTP) server to automatically set the system date and time. The system date and time are used to time stamp log messages, certificate time generation, licensing, and call detail records (CDRs).

Manually Setting the System Date and Time

NTP Servers must be disabled for manual settings to take effect. Refer to "If you configure the Mobility Router to get the system date and time from an NTP server, NTP polls the specified server at regular intervals and updates the system date and time so that they are synchronized with the server. By default, NTP is enabled. A default NTP server has already been defined. You can add other NTP servers." on page 22 for configuration information.

1. Click **Configuration > System > Date and Time > Manual.**
2. In the **Time Zone** list, select the time zone in which the Mobility Router is located.
3. Click **Apply**.
4. In the **Date** field, type the current date in the format *YYYY*/*MM*/*DD*, where *YYYY* indicates the year, *MM* indicates the month, and *DD* indicates the day.
5. In the **Time** field, type the current time in the format *HH*:*MM*:*SS*, where *HH* indicates the hour, *MM* indicates the minutes, and *SS* indicates the seconds. Specify the time using 24-hour clock format.
6. Click **Apply** and continue to the NTP Configuration page to disable NTP servers. Refer to "If you configure the Mobility Router to get the system date and time from an NTP server, NTP polls the specified server at regular intervals and updates the system date and time so that they are synchronized with the server. By default, NTP is enabled. A default NTP server has already been defined. You can add other NTP servers." on page 22 for information.

If you configure the Mobility Router to get the system date and time from an NTP server, NTP polls the specified server at regular intervals and updates the system date and time so that they are synchronized with the server. By default, NTP is enabled. A default NTP server has already been defined. You can add other NTP servers.

Note

NTP is enabled, the Mobility Router reads the time from the NTP server, not the time set manually. The manual date and time settings are ignored.

7. Click **OK** to log out. A message confirming that you have logged out displays in the browser.

Enabling NTP

To enable NTP:

1. In the Administration Portal, click **Configuration > System > Date and Time > NTP**. The NTP page displays.
2. To enable NTP, select the **Enable NTP** check box. To disable NTP, clear the **Enable NTP** check box. By default, NTP is enabled.
3. To save your changes, click **Apply**.

Adding NTP Servers

If you do not want to use the default NTP server that is defined, you can add NTP servers. If you add multiple NTP servers, the Mobility Router contacts the first NTP server listed alphabetically to get NTP information. If that server is unavailable, the Mobility Router uses the alphabetical list of NTP servers to contact another server until a connection is made.

To add an NTP server:

1. In the Administration Portal, Click **Configuration > System > Date and Time > NTP**. The NTP page displays.
2. To add a new NTP server, click **Add**. The **Add NTP Server** page displays.
3. In the **Server** field, type the fully qualified domain name or IP address of the NTP server. The name or IP address can be up to 64 alphanumeric characters. No special characters except periods (.) are allowed.
4. In the **Version** list, choose the version of NTP to be used:
   - 4—Version 4 (default value)
   - 3—Version 3
5. To activate the NTP server, select the **Enabled** check box. If you want to use this server as an NTP server, make sure you select this check box, in addition to enabling NTP, as described in “Enabling NTP” on page 23.
6. To save your changes, click **Apply**. The NTP page displays.

Modifying NTP Servers

To modify an NTP server:

1. In the Administration Portal, click Co**nfiguration > System > Date and Time > NTP**. The NTP page displays.
2. Select the NTP server you want to modify.
3. To modify an NTP server, click **Modify**.

4. Make changes as necessary. You cannot change the name of the NTP server. For information about changing properties of an NTP server, see “Adding NTP Servers” on page 23.
5. To save your changes, click **Apply**. The NTP page displays.

Deleting NTP Servers

To delete an NTP server:

1. In the Administration Portal, click **Configuration > System > Date and Time > NTP**. The NTP page displays.
2. Select the NTP server that you want to delete. Click **Delete**. The NTP server is deleted.

Configuring Logging and Monitoring Options

Use the logging options to keep record of events on the Mobility Router. Logging option levels can be set to report based on the desired level of information needed.

This section contains the following options:

Configuring Email

Use the Email page to specify an SMTP server, mail domain name, and individual email addresses that should receive notification of specific events on the Mobility Router. This setting is optional.

Setting General Email Options

1. Click **Configuration > System > Logging/Monitoring > Email**. The **Email** page displays and the **General** tab is active.
2. In the **SMTP Server** field, type the IP address or hostname of the SMTP server to which email notifications should be sent.
3. In the **Mail Domain Name** field, type the domain name associated with the SMTP server.
4. Click **Apply** to save changes.

Setting Auto Notification

To set automatic notification of events:

1. Click **Configuration > System > Logging/Monitoring > Email > Auto Notifications** tab.

2. Check the appropriate event boxes for which automatic notifications will be sent:
   - **Cluster Status Change Event** —A node has unexpectedly joined or left the cluster, or the number of nodes is unexpected.
   - **Link Status Change Event** — The interface link state changed.
   - **Process Crash Event** — A process in the system was detected as hung.
   - **Process Unexpected Exit Event** — A process in the system unexpectedly exited.
   - **High CPU Utilization Event** — CPU utilization has risen too high.
   - **High Disk I/O Utilization Event** — Disk I/O per second has risen too high.
   - **Low Free Disk Event** — File system free space has fallen too low.
   - **High Interface Utilization Event** — Network utilization has risen too high.
   - **Low Free Memory Event** — Memory usage has risen too high.
   - **High Memory Paging Event** —Paging activity has risen too high.
   - **Unexpected Shutdown Event** — The system shut down unexpectedly.
   - **Login/Logout** — The system sends email notification to administrator with user name and IP address of the user who has logged in or out.
   - **PBX Connectivity Monitoring**—The system sends email notification to administrator if there is a change in connectivity from CMR to PBX(s).
   - **Client Log upload Event** — Email notification with user's uploaded log and subject information.
   - **Scheduled Config Backup Event** — If a configured backup is scheduled, an email notification is sent whenever this backup is performed.
3. Click **Apply** to save changes.

Adding Notification Recipients

1. Click **Configuration > System > Logging/Monitoring > Email > Notify Recipients** tab.
2. Click **Add**. The **Add Recipient** page displays
3. In the **Email Address** field, type the email address of the person to receive notification. Select the appropriate boxes to receive details, information or failure information. The following is a sample output for failure information:

Table 1: Failure Sample

Failure Type	Description
`process-crash`	A process in the system has crashed.
`unexpected-shutdown`	The Mobility Router has unexpectedly shut down.

4. Click **Apply** to save changes.

Configuring Logging Settings

Use the **Logging** page to configure the settings by which to monitor events.

Configuring Module Settings

1. Click Configu**ration > System > Logging/Monitoring > Logging**. The **Modules** tab is active.
2. Specify the minimum level of events to be logged for each module. Select the level by choosing from the available list for each of the following modules:
   - Infrastructure
   - CAS Helper
   - Configuration
   - Directory
   - Database
   - Media Processor
   - Mobility
   - UC
   - Provisioning
   - Remote Access
   - Session Logger
   - SIP

   See Table 2 for a list of event levels and their definitions.
3. To save your changes, click **Apply**.

Table 2: Filtering Levels for Logging Mobility Router Events

Severity Level	Description
`debug`	Provides low-level debugging messages. Generally, this logs only developer-targeted messages that contain more detailed information about the internal state of the system. Debug messages can be used for debugging problems where the INFO-level logs do not provide enough information. Changing the logging level to debug can adversely affect Mobility Router performance.
`info`	Events that are expected to happen. These events are used to trace data flow and process activity.
`notice`	Indicates notification of a normal, expected event.

Table 2: Filtering Levels for Logging Mobility Router Events

Severity Level	Description
warning	Warning of a potential or mild error. Indicates that an unusual condition has been detected that might be cause for concern. Action should be taken to further diagnose (if necessary) and correct the problem.
err	Indicates a minor error that might require operator intervention if it recurs. Investigation and corrective action should be taken in order to prevent a more serious (for example, service-affecting) fault.
crit	Indicates that a service-affecting condition has developed, and an urgent corrective action is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the managed object and its full capability must be restored.
alert	Indicates a severe error condition that requires operator intervention. Critical parts of the system are operational. However, either a less critical part of the system is nonfunctional, or the overall system is operating at a degraded capacity.
emerg	Indicates a service-affecting error condition that requires immediate attention. A critical part of the system is either not functioning correctly or has failed.
fatal	Internal server error from which the server cannot recover and will terminate.
debug0	This is the first level of debugging and should be used for brief indications of actions or events. Usually those actions and events are either visible to customer or can be easily explained. **Note:** The higher the level (debug0 to debug4), the more details are shown. Changing the logging level to debug0 can adversely affect Mobility Router performance.
debug1	A more detailed level of debugging. This can be used to provide more detailed information about events and actions that are usually not obvious to customer. Details require a knowledgeable person to analyze them. **Note:** Changing the logging level to debug1 can adversely affect Mobility Router performance.
debug2	Reserved. Can be used for more debugging levels or to connect to third-party modules that have multiple debugging levels. Changing the logging level to debug2 can adversely affect Mobility Router performance.

Table 2: Filtering Levels for Logging Mobility Router Events

Severity Level	Description
debug3	A hexadecimal or text representation of raw data. Example: whole SIP message, RTP packet header. **Note:** Changing the logging level to debug3 can adversely affect Mobility Router performance.
debug4	Extremely detailed levels of information. Changing the logging level to debug4 can adversely affect Mobility Router performance.
SIP - Call Control	Incoming and outgoing user call information
SIP - Registration	Server and client registration information
SIP - Presence	Presence related information
SIP - Framework	SIP configuration, high availability and call detail record information
SIP - Filter by User ID	Enter the User ID for a particular user to troubleshoot for that user only. Useful for when there are multiple users in the system and needing to troubleshoot for a specific user.
SIP - Strict Filtering	Select this option to strictly filter the log specified in “Filter by User ID”.
SIP - Miscellaneous	All categories not covered by the previous selections.

Configuring Local Log Settings

1. Click **Configuration > System > Logging/Monitoring > Logging**.
2. Click the **Local Log** tab.
3. In the **Format** list, select the format for the local log files:
   - standard—Standard log format (text file)
   - welf—WebTrends Enhanced Log Format (WELF)
4. In the **Rotation** list, specify the frequency at which the log is rotated.
   - Every
     - Day: starting at 12:00:00 a.m.
     - Week: from Sunday 12:00:00 a.m. to Sat 11:59:59 p.m.
     - Month: from the 1st of each Month at 12:00:00 a.m. to the last day of the specific calendar month at 11:59:59 p.m.
   - When log reaches (thousandths of a percent of /var size)

5. In the **Max log file to keep** field, type the maximum number of log files that are stored on the Mobility Router. The value can be between 1 through 4,294,967,295.
6. To save your changes, click **Apply**.

Managing Syslog Servers

You can define syslog servers to archive the Mobility Router logs in a centralized location for auditing and reporting purposes.

Adding Syslog Servers

1. Click **Configuration > System > Logging/Monitoring > Logging**. The Logging page displays.
2. Click the **Syslog Servers** tab.
3. Click **Add**.
4. In the **Remote Address** field, type the IP address of the syslog server.
5. In the **Minimum Severity** field, select the minimum level of severity at which events are sent. See Table 2 for a list of severity levels and their definitions.
6. To save your changes, click **Apply**. The Syslog Servers page displays.

Modifying Syslog Servers

1. Click Con**figuration > System > Logging**.
2. Click the **Syslog Servers** tab.
3. Click **Modify**.
4. Change the fields as needed.
5. To save your changes, click **Apply**. The Syslog Servers page displays.

Deleting Syslog Servers

1. Click **Configuration > System > Logging/Monitoring > Logging**.
2. Click the **Syslog Servers** tab.
3. Select the syslog server that you want to delete.
4. Click **Delete**.
5. When prompted to confirm the deletion, click **OK**. The syslog server is deleted.

Configuring SNMP

Use the SNMP page to enable SNMP on a selected interface and specify a community. SNMP is disabled by default.

Note

Mitel recommends not using well-known community names such as **public** and **private**.

1. Click **Configuration > System > Logging/Monitoring > SNMP**.
2. Click **Enable**.
3. Select an **Interface**. By default, the IP address associated with the primary interface is chosen. This interface is used by the Mobility Router for communicating with the SNMP server.
4. Specify a **Community**.
5. Click **Apply**.

Configuring Support Service

Click **Configuration > System > Support Service** to enter a Support email and phone number for Connect Platform users.

When “Call Support” is initiated by the user on the Mobility app, the phone number entered here is called. If the user opts to select “send log”, the information is sent to the email address entered here.

Managing Licenses

Within version 9.1.11 we eliminated the “RoamAnywhere” license key requirement and any licensing enforcement previously done on the Mobility Router. See the 17052 – Global Product bulletin for details. So, the only remaining licensing requirement is on Director, where each user requires both a SIP Device and Mobile Access license. The good news is that every user license bundle (Essentials, Standard and Advanced) includes those licenses, and they are automatically installed via the single license key file we send.

CHAPTER

5

Configuring Network Settings

Network settings such as hostname and DNS, Ethernet interfaces, routing and static hosts are modified using the following procedures:

Configuring Hostname and DNS

The Hostname/DNS page contains basic networking information about the Mobility Router. Most of this information is entered during the Initial Configuration Wizard and should not require changing.

Note

The Internal hostname/FQDN on Eth 0 needs to be different than the external FQDN on Eth 1.

1. Click **Configuration > System > Networking > Hostname/DNS**. The **Hostname/DNS** page displays.
2. In the **Hostname** field, verify that the Mobility Router hostname is the value specified in the Hostname field during the Initial Configuration Wizard. You typically do not need to change the hostname.
3. The hostname can be up to 64 alphanumeric characters long and can contain hyphens (-), however it cannot contain spaces or underscores (_).
4. In the optional **Domain Name** field, verify the domain name. This value defaults to the domain name provided during the Initial Configuration Wizard and does not require changing.
5. In the **Primary DNS IP Address** field, verify the primary DNS IP address. This value defaults to the IP address provided during the Initial Configuration Wizard.
6. We recommend that you have at least two DNS servers available on the mobility solution.
7. In the **Secondary DNS IP Address** field, type an IP address for a second DNS server.
8. In the **Tertiary DNS IP Address** field, type an IP address for a third DNS server.
9. To save your changes, click **Apply**.

Configuring Ethernet Interfaces

After specifying the basic Ethernet interface in the Initial Configuration Wizard or completing the Hostname/DNS tab (“Configuring Hostname and DNS” on page 35), you can configure the following settings for each Ethernet interface (eth0, eth1):

- Interface speed
- Duplex settings

Some information in the fields under the Interface menu reflect the responses provided during the Initial Configuration Wizard setup. Some fields are set to system defaults that generally do not require changing.

1. Click **Configuration > System > Networking > Interface**. The Interface page displays. The **eth**1 tab is active.
2. Verify that the interface is enabled. For the eth0 interface, this check box is selected by default and cannot be changed. You can enable or disable the eth1 interface.

3. Verify the IP address. To change the IP address, select one of the following:

   - Use DHCP—If you entered N in response to the Use DHCP on eth0 interface prompt in the Initial Configuration Wizard, you can change eth0 to DHCP by selecting this field and then selecting Apply.
   - Static— This field defaults to the IP address entered in the Primary IP Address field entered in the Initial Configuration Wizard and should not be changed.

4. In the **Gateway** field, verify the gateway value. This value defaults to the IP address provided during the Initial Configuration Wizard and should not require changing.

5. Verify the interface speed. The default and recommended value are **Auto**. To change the speed, select one of the following in the Speed list:

   - 10—10 Mbps (This option is not supported if you are going to create a redundancy cluster. For information about redundancy clusters, see "Managing Redundancy Clusters" on page 181.)
   - 100—100 Mbps
   - 1000—1000 Mbps
   - Auto—Speed is auto-detected

6. Verify the duplex value. The default value is **Auto**. To change the duplex setting, select one of the following in the Duplex list:

   - Full—Full-duplex
   - Half—Half-duplex
   - Auto—Auto-detect duplex setting.

7. Review the Maximum transmission unit (MTU) value.

8. Verify the MAC address.

9. Review the online Status of the Mobility Router.

10. To save your changes, click **Apply**.

Configuring Routing Settings

Configure the default gateway or create additional static routes using the following procedures.

Configuring the Default Gateway

By default, the default gateway field is the IP address provided during the Initial Configuration Wizard and should not be changed. The default gateway is the default route for the Mobility Router.

1. Click **Configuration > System > Networking > Interface**. The Interface page displays.

2. Refer to defining the Gateway in "Configuring Ethernet Interfaces" on page 35 for more information.

Managing Static Routes

The default gateway is automatically set up as a static route. You can optionally create additional static routes to send packets to specific IP addresses or a specific network.

Adding Static Routes

1. Click **Configuration > System > Networking > Routing**.
2. Click **Add**. The **Add Route** page displays.
3. In the **IP Address** field, type the IP address for the static route.
4. In the list of subnet mask values, select the value of the subnet mask for the IP address.
5. In the **Gateway** field, type the IP address of the gateway for the route.
6. In the **Interface** list, select the Ethernet interface for the route.
7. To save your changes, click **Apply**.

Note

If Mobility Routers are used in a clustered configuration, the Static Routes must be added in both primary and secondary Mobility Routers. Refer to "Managing Redundancy Clusters" on page 181 for more information about configuring clustered Mobility Routers.

Modifying Static Routes

1. Click **Configuration > System > Networking > Routing**. The **Routing** page displays.
2. Select the static route to be modified and click **Modify**.
3. Make any necessary changes. For information about the fields on this page, see "Adding Static Hosts" on page 38.
4. To save your changes, click Apply.

Deleting Static Routes

1. Click **Configuration > System > Networking > Routing**. The **Routing** page displays.
2. Select the static route to be deleted.
3. To select multiple contiguous items, hold the Shift key while the selecting items. To select multiple non-contiguous items, hold the Ctrl key while selecting the items.
4. Click **Delete**.
5. When prompted to confirm the deletion, click **OK**.

Configuring Static Hosts

Static hosts can be optionally defined for the most frequently used hosts. The IP address for the Mobility Router, which you provided as the primary IP address in the Initial Configuration Wizard, is automatically added as a static host. You can define additional static hosts based on your network requirements.

Note

Static Hosts can be added and deleted but cannot be modified.

Adding Static Hosts

1. Click **Configuration > System > Networking > Static Hosts**.
2. Click **Add**. The Add **Static Host** page displays.
3. In the **IP Address** field, type the IP address of the static host.
4. In the **Hostname** field, type a name for the static host. The name can up to 64 alphanumeric characters long and can contain hyphens (-) and underscores (_).
5. To save your changes, click **Apply**.

Note

If Mobility Routers are used in a clustered configuration, the Static Hosts must be added in both primary and secondary Mobility Routers. Refer to “Managing Redundancy Clusters” on page 181 for more information about configuring clustered Mobility Routers.

Deleting Static Hosts

1. Click **Configuration > System > Networking > Static Hosts**.
2. Select the static host that you want to delete.
3. To select multiple contiguous items, hold the Shift key while the selecting items. To select multiple non-contiguous items, hold the Ctrl key while selecting the items.
4. Click **Delete**.
5. When prompted to confirm the deletion, click **OK**.

Configuring Ports

Port ranges can be optionally configured. The Mobility Router uses default port ranges, but these ranges may be modified.

1. Click **Configuration > System > Networking > Ports**.
2. Enter the **Starting Port** and/or **Ending Port** as appropriate.

Note

The range for RAST TCP Flow and RAST Datagram Protocol (UDP) Flow cannot overlap the Media Server RTP port range. For example, if the Media Server RTP range is 25370 - 31999, the RAST Flow ranges cannot end higher than 25369 or start lower than 32000.

3. Click **Apply** to save changes or click **Defaults** to revert to the original port ranges.

Configuring SSH

Select **SSH** (Secure Shell) to enable the SSH service on a selected interface. SSH is enabled by default.

Note

SSH should be disabled unless being used and must not be enabled on Eth 1.

1. Click **Configuration > System > Networking > SSH**.
2. Verify **Enable** is selected.
3. Select an **Interface**. By default, the IP address associated with the primary interface is chosen. This interface is used by the Mobility Router for communicating with the SSH server.
4. Click **Apply**.

Configuring Services

Select **Services** to choose an interface for SIP (Calls towards PBX and Local CMC), RAST Internal Interface for different flows, Client Provisioning, and Client Configuration Management services. By default, the IP address associated with the primary interface is chosen. The Connect Platform application uses this IP address to communicate with the Mobility Router.

1. Click **Configuration > System > Networking > Services**.
2. Select an interface from the drop-down list.
3. Click **Apply**.

CHAPTER

6

Managing Remote Access

This chapter contains the following sections:

Overview

You can configure the Mobility Router to allow secure remote access, which consists of the following features:

- Secure Remote Voice (if your mobility solution is licensed for it)—Secure Remote Voice allows users to securely place and receive calls using any Wi-Fi network outside of the enterprise or a cellular packet-data network. Users can use Secure Remote Voice from home or any other Wi-Fi hotspot and have access to PBX and desk-phone features, just as they do when they are in the enterprise. Calls are handed over between Wi-Fi and cellular networks if users move from network to network.

- Secure Enterprise Services—Secure Enterprise Services, such as directory query and managing locations, are accessed using a Wi-Fi network that is not in the enterprise network or a cellular packet-data network. Using Secure Enterprise Services also allows users to reprovision and upgrade Connect Platform.

- Secure Instant Communications—Secure Instant Communications enables location-aware presence. By enabling remote access for Secure Instant Communications, users will be able to receive presence updates and broadcast their presence status to peers when they are outside the enterprise on a remote Wi-Fi network or a cellular packet-data network. Additionally, the system will automatically recognize which connection type the user is on and update their current location for peers.

  An SSL tunnel is used to secure communication between the Mobility Router and mobile devices. Calls placed and received while using Secure Remote Voice go through the tunnel. Data communications for Secure Enterprise Services is also sent through the tunnel.

You can allow individual users or groups to have access to Secure Remote Voice, Secure Enterprise Services, or both features. After configuring the remote-access settings, you can enable remote access when creating users or groups. For information about creating users and groups, see “Managing Groups” on page 144 and “Managing Users” on page 158.

Before You Begin

Before you start configuring remote access, make sure you have the following:

- You have received the Secure Remote Voice key.
- You have access to a Public IP address with traffic allowed on TCP and UDP ports. Mobility Router must be deployed behind the organization's Internet firewall, make sure that the firewall allows external traffic to and from the IP address and its TCP and UDP ports. For Port Range information, refer to "Mobility Router Ports" on page 193.

WARNING!

Firewall Traversal Requirements: If the Mobility Router is deployed in a network topology where there is a firewall between the Mobility Router and the PBX, firewall rules need to be configured to allow the SIP call signaling and RTP voice media packets to traverse the network.

- If you are using the eth0 and eth1 interfaces to configure Secure Remote Voice, make sure that the eth0 and eth1 IP addresses are not in the same subnet.
- eth0 must be used for the LAN interface and eth1 the connection to the internet firewall.
- If you intend to assign an internal IP address to the eth1 interface and use NAT to map a publicly accessible IP address on a firewall to the eth1 IP address, you must configure your firewall:
  - Add firewall rules to map the public IP address to the eth1 IP address.
  - If you are going to use different numbers for the publicly accessible ports on the firewall and the Mobility Router port that listens for remote-access traffic, you must configure port forwarding on the firewall.
- If you have a redundancy cluster, make sure you do the following:
  - If you are configuring Secure Remote Voice, make sure that you have two licenses—one for each Mobility Router in the cluster. You must install both licenses on each Mobility Router. Access the physical IP of each Mobility Router to install each license.
  - Access the virtual IP address of the redundancy cluster to configure remote access.

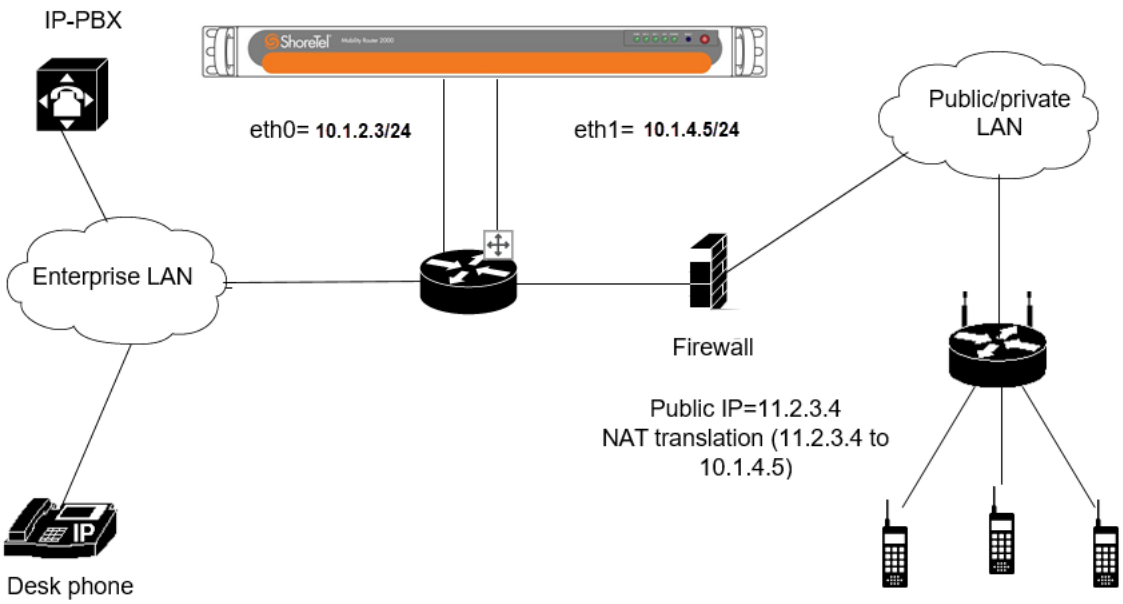
Network Configurations

How you configure remote access depends on your network configuration. The following lists the most common network configurations for which you can implement remote access:

Network Includes NAT with Firewall

In this network configuration, the Mobility Router uses the eth0 interface for communication to a default gateway and the internal network. The eth1 interface uses an internal IP address. The default gateway is connected to a firewall using NAT with a publicly accessible IP address. Users with Connect Platform running on their mobile devices access this publicly accessible IP address to create tunnels so that they can use Secure Remote Voice and Secure Enterprise Services. An example of this network configuration is shown in Figure 3.

Figure 3: Network Configuration Using NAT with Firewall

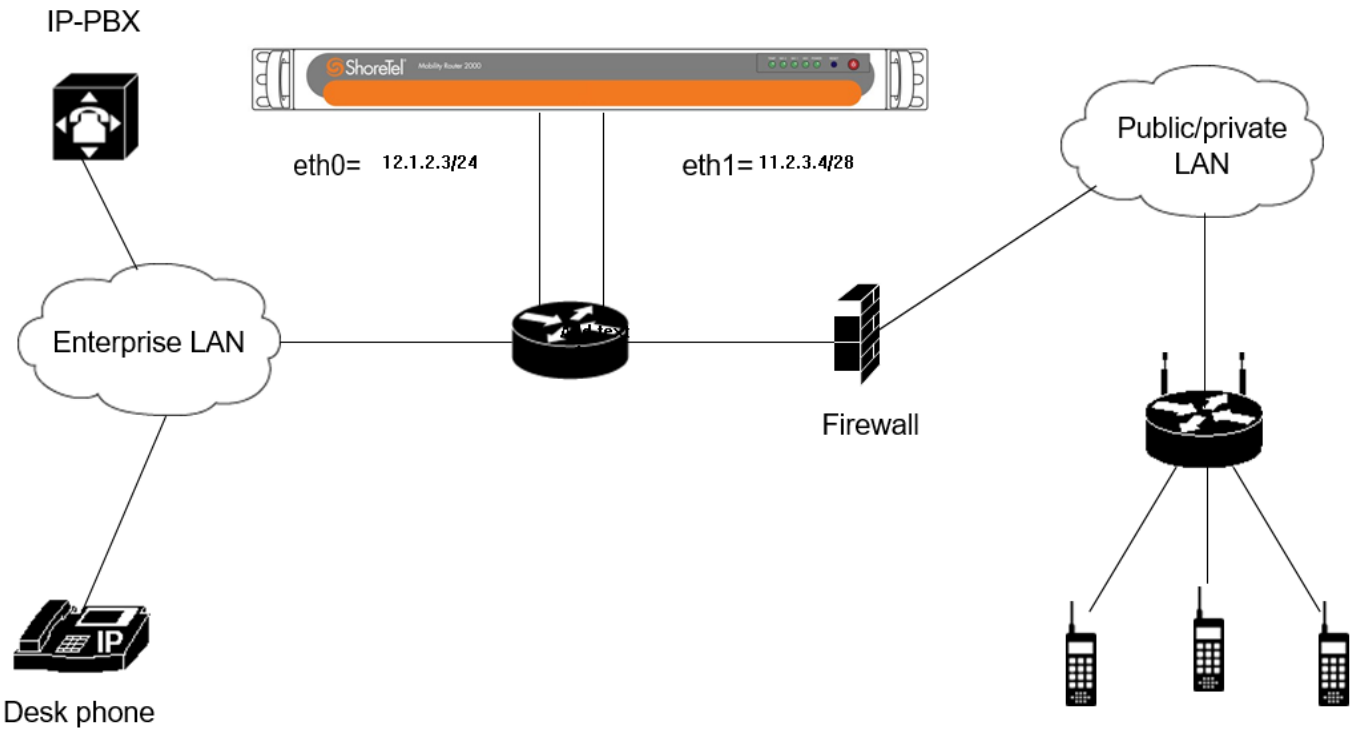


Network Excludes NAT

In this network configuration, the Mobility Router uses the eth0 interface for communications to a default gateway and the internal network. The eth1 interface uses a publicly accessible IP address. The default gateway is connected to a firewall, which must be configured to allow traffic to the publicly accessible IP address.

Users with Connect Platform running on their mobile devices access the publicly accessible IP address to create tunnels so that they can use Secure Remote Voice and Secure Enterprise Services. An example of this network configuration is shown in Figure 4.

Figure 4: Network Configuration That Does Not Use NAT



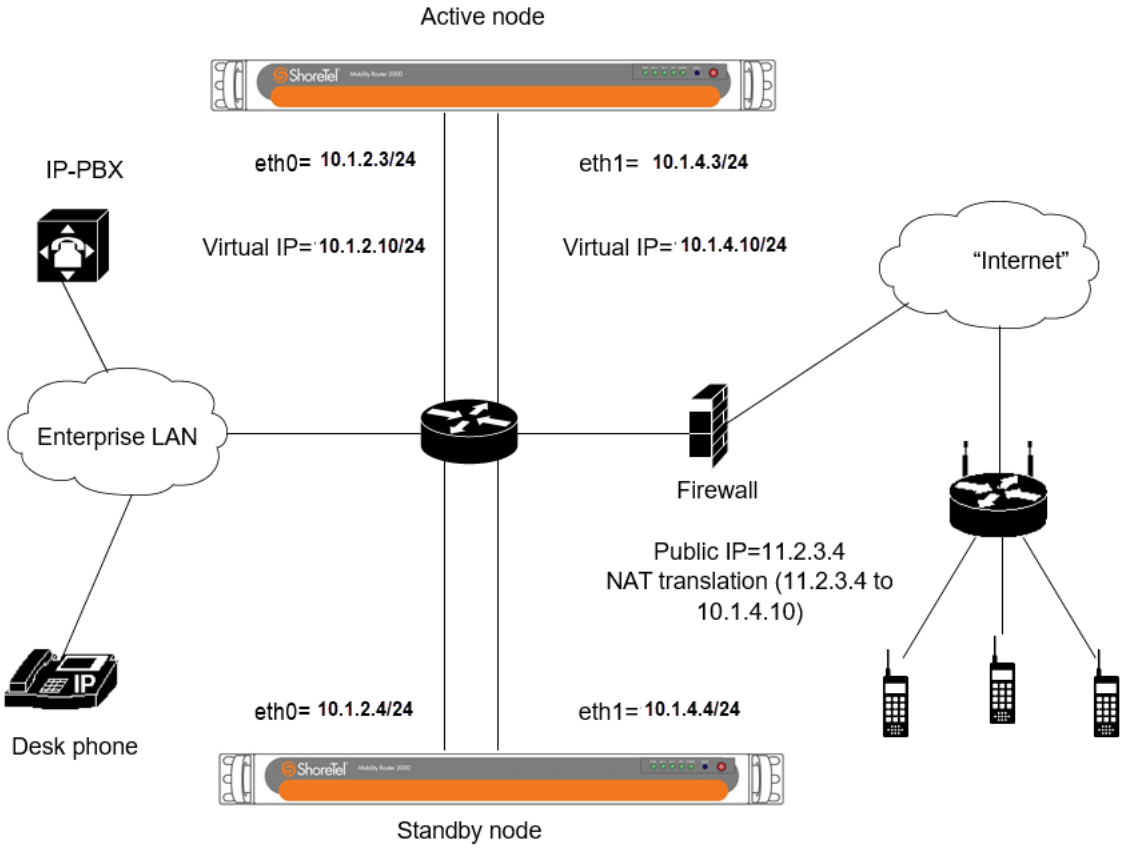
Network Uses Mobility Router Redundancy Cluster and NAT with Firewall

In this network configuration, there is a cluster of two Mobility Routers. Each Mobility Router uses the eth0 interface for communications to a default gateway and the internal network. Each eth1 interface uses an internal IP address. In addition to the physical eth0 interfaces, there is a virtual eth0 IP address that is used to manage the cluster.

The default gateway is connected to a firewall using NAT with a publicly accessible IP address. Users with Connect Platform running on their mobile devices access this publicly accessible IP address to create tunnels so that they can use Secure Remote Voice and Secure Enterprise Services. An example of this network configuration is shown in Figure 5.

There is also a virtual eth1 IP address, which is the IP address to which traffic sent to the publicly accessible IP address is forwarded. For a redundancy cluster, the virtual IP address is used rather than the physical IP address because the virtual IP address remains constant if failover occurs and the standby takes the active role. For information about redundancy clusters, see “Managing Redundancy Clusters” on page 181.

Figure 5: Network Configuration That Uses Redundancy Cluster with NAT



Network Uses Mobility Router Redundancy Cluster Without NAT

In this network configuration, there is a cluster of two Mobility Routers. Each Mobility Router uses the eth0 interface for communications to a default gateway and the internal network. The eth1 interface uses a publicly accessible IP address. In addition to the physical eth0 interfaces, there is a virtual eth0 IP address that is used to manage the cluster.

The default gateway is connected to a firewall, which must be configured to allow traffic to the publicly accessible IP address. Users with Connect Platform running on their mobile devices access the publicly accessible IP address to create tunnels so that they can use Secure Remote Voice and Secure Enterprise Services. An example of this network configuration is shown in Figure 6.

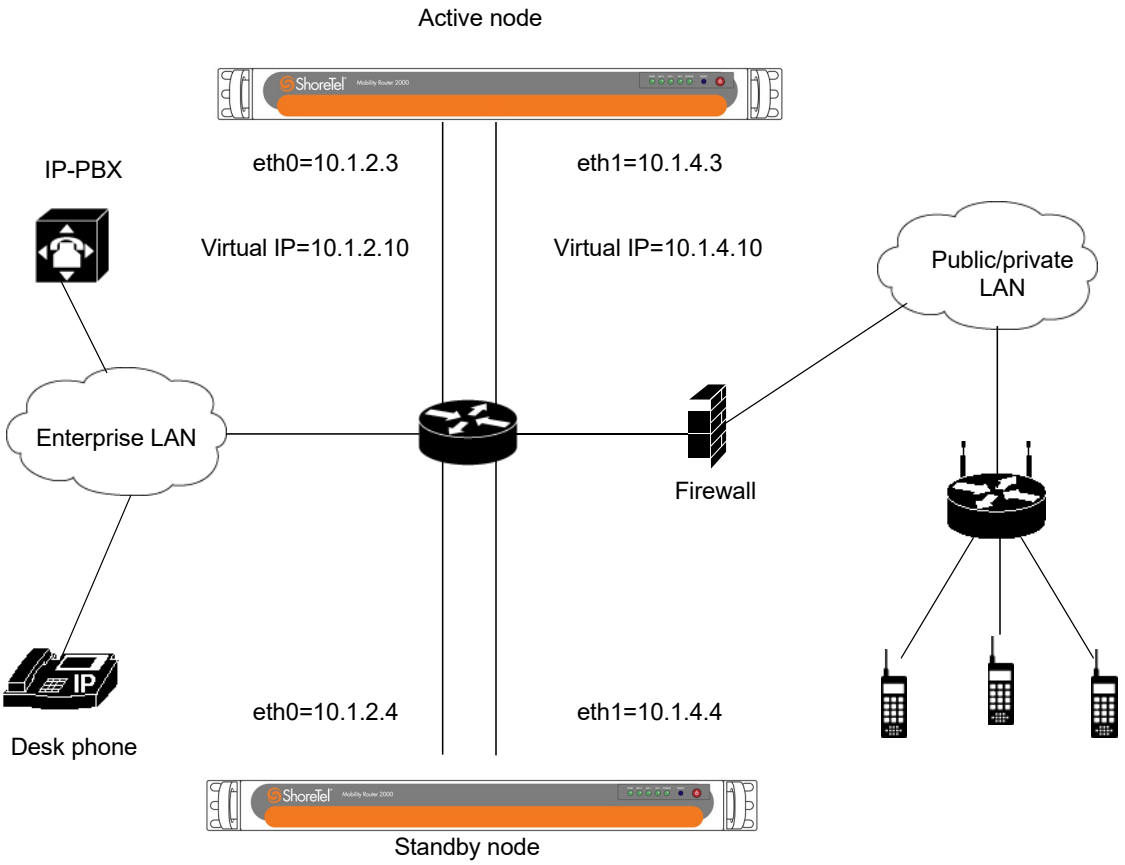
There is also a virtual eth1 IP address, which is a publicly accessible IP address. For a redundancy cluster, the virtual IP address is used rather than the physical IP address because the virtual IP address remains constant if failover occurs and the standby takes the active role. For information about redundancy clusters, see “Managing Redundancy Clusters” on page 181.

Note

You must ensure the following conditions while using this network configuration without NAT:

- With remote access enabled, eth1 is reachable from the public network.
- With remote access disabled, eth0 is reachable by the CMC (mobile) devices.

Figure 6: Network Configuration That Uses Redundancy Cluster Without NAT



Configuring General Settings

After setting up your network, as described in “Before You Begin” on page 42, configure general settings for remote access:

- Ethernet interface used for remote access
- Virtual IP address of the cluster (only if you have created a redundancy cluster)
- Public NAT information
  - External IP address
  - UDP port
  - TCP port
- Tunnel interface MTU
- Remote client IP lease duration

To configure general settings:

1. Click **Configuration > System > Networking > Remote Access**. The **Remote Access** page displays with the **General** tab active.
2. To enable remote access, make sure the **Enable** check box is selected. By default, this check box is not selected. To disable remote access, clear the Enabled check box.
3. In the **Remote Access IP Interface** list, select the Ethernet interface used for remote access. Typically, this is the eth1 interface.
4. Do one of the following:
   - If you do not have a redundancy cluster enabled, go to step 6.
   - If you do have redundancy cluster enabled, go to step 5.
5. To establish a secure remote connection from an external network, enter a valid FQDN in the **Remote Access FQDN** field.
6. In the Public NAT area, configure the following:
   - To enable a public network address translation (NAT) IP address for the Mobility Router, make sure that the **Enable** check box is selected. By default, this check box is selected. To disable the NAT IP address, clear the **Enable** check box.
   - In the **IP Address** field, type the external IP address used for NAT.
   - In the **UDP Port** field, type the port number for the external IP address to which clients connect. The port number can be between 80 through 49151. The default value is 443.
   - In the **TCP Port** field, type the port number for the external IP address to which clients connect. The port number can be between 80 through 49151. The default value is 443.
7. In the **Tunnel Interface MTU** field, type the tunnel interface MTU for traffic to and from the enterprise LAN. The MTU can be a value between 576 through 9000. The default value is 1360.

Typically, you should not need to change the MTU value. If you do change the MTU, its value must be 16 bytes less than the MTU values defined for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), as described in "Configuring Protocols" on page 48.

8. In the **Remote Client IP Lease Duration** field, type the amount of time that a client retains an IP address during a session using Secure Remote Voice or secure enterprise Services. The lease duration can be a value between 30 through 65535 minutes. The default value is 1440 minutes.

9. Click **Apply**.

Configuring Protocols

After configuring general settings, you can configure the security protocols for the tunnels that are established between clients and the Mobility Router for sessions using Secure Remote Voice and Secure Enterprise Services. The mobility solution supports the following security protocols for tunnels:

- Datagram Transport Layer Security (DTLS)—Protocol that allows secure communications over datagram protocols, such as User Datagram Protocol (UDP). DTLS is based on the Transport Layer Security (TLS) protocol but can be used in environments that use UDP transport.
- Transport Layer Security (TLS)—Protocol that allows secure communications using Transmission Control Protocol (TCP) as the transport protocol.

  You can enable one or both security protocols. By default, DTLS and TLS are enabled. If your network environment does not allow incoming UDP packets, you can use TLS, which allows TCP packets. If DTLS and TLS are enabled, DTLS is used first, and then TLS is used, depending on what the client supports.

For DTLS and TLS, you can configure the following settings:

Note

TLS 1.2 is recommended

- Cipher
- Port
- Maximum transmission unit (MTU)
- Keepalive time
- Session timeout
- Renegotiation time

To configure tunnel security protocols:

1. Click **Configuration > System > Networking > Remote Access** > **Protocol** tab.

2. In the **Datagram TLS/UDP** area, to enable **DTLS**, make sure that the **Enable** check box is selected. By default, this check box is selected. To disable DTLS for troubleshooting, clear the **Enable** check box.

1. In the **Cipher** list, select one of the following:
   - NULL-MD5—Uses no encryption (null cipher) and Message-Digest Algorithm 5 (MD5) for authentication. (This is the weakest cipher.)
   - AES128-SHA—Uses Advanced Encryption Standard (AES) with 128-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication.
   - AES256-SHA—Uses Advanced Encryption Standard (AES) with 256-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication. (This is the strongest cipher.)

Note

Although choosing the strongest cipher increases security, using the strongest cipher uses more resources on the mobile devices and Mobility Router.

2. In the **Port** field, type the number of the port on which the Mobility Router listens to remote-access requests. The port number can be between 80 through 49151. The default port number is 443.

   If you enabled public NAT on **General** tab, this port number must match the UDP port configured for public NAT. If the port number does not match, you must configure port forwarding on the firewall.

3. In the **MTU** field, type the MTU value. The MTU can be a value from 576 through 1440. The default MTU value is 1376.

   If you do change the MTU, its value must be 16 bytes more than the MTU value defined for the tunnel, as described in “Configuring General Settings” on page 47.

4. In the **Keep Alive** field, type the interval at which the Mobility Router sends echo messages over the tunnel after client inactivity. The keepalive time can be a value between 2 through 3600 seconds. The default value is 55 seconds.

5. In the **Session Timeout** field, type the amount of time that the client can be inactive before the session is disconnected. The timeout can be a value between 60 through 65535 seconds. The default timeout is 600 seconds.

6. In the **Renegotiation Time** field, type the amount of time that elapses before the encryption key is refreshed. The renegotiation time can be a value between 0 through 65535 minutes. Setting the time to 0 disables the refreshing of the encryption key. The default value is 0.

3. In the **TLS/TCP** area, to enable TLS, make sure that the **Enable** check box is selected. By default, this check box is selected. To disable TLS, clear the **Enable** check box.

Tip

Enable TLS for remote provisioning to work correctly in situations where UDP packets are not allowed in the network environment.

7. In the **Cipher** list, select one of the following:
   - NULL-MD5—Uses no encryption (null cipher) and Message-Digest Algorithm 5 (MD5) as authentication.
   - RC4-MD5—Uses a common algorithm created by RSA Security as the encryption method and Message-Digest Algorithm 5 (MD5) as authentication.
   - AES128-SHA—Uses Advanced Encryption Standard (AES) with 128-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication.
   - AES256-SHA—Uses Advanced Encryption Standard (AES) with 256-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication. (This is the strongest cipher.)

Tip

Although choosing the strongest cipher increases security, using the strongest cipher uses more resources on the mobile devices and Mobility Router.

8. In the **Port** field, type the number of the port on which the Mobility Router listens to remote-access requests. The port number can be between 80 through 49151. The default port number is 443.

   If you enabled public NAT on **General** tab, this port number must match the TCP port configured for public NAT. If the port does not match, you must configure port forwarding on the firewall.

9. In the **MTU** field, type the MTU value. The MTU can be a value from 576 through 1500. The default MTU value is 1376.

   If you do change the MTU, its value must be 16 bytes more than the MTU value defined for the tunnel, as described in “Configuring General Settings” on page 47.

10. In the **Keep Alive** field, type the interval at which the Mobility Router sends echo messages over the tunnel after client inactivity. The keepalive time can be a value between 1 through 3600 seconds. The default value is 55 seconds.

11. In the **Session Timeout** field, type the amount of time that the client can be inactive before the session is disconnected. The timeout can be a value between 60 through 65535 seconds. The default timeout is 600 seconds.

12. In the **Renegotiation Time** field, type the amount of time that elapses before the encryption key is refreshed. The renegotiation time can be a value between 0 through 65535 minutes. Setting the time to 0 disables the refreshing of the encryption key. The default value is 0.

4. Click **Apply** to save your changes.

Options

Call Admission Control

Use Call Admission Control (CAC) to define the thresholds for Secure Remote Voice calls and to prevent overloading the enterprise WAN connection. An Administrator can allocate maximum amount of available bandwidth for Secure Remote voice traffic as well as restrict the maximum number of simultaneous voice calls allowed through the secure remote access. When the Secure Remote Access Bandwidth limit is reached or number of simultaneous call limit is reached, the Mobility Router does not accept new VoIP calls from remote clients. If a remote client attempts to make a VoIP call when there is no available bandwidth to support the new call, the Mobility Router instructs the client to place the call through the cellular voice interface. Similarly, when the Mobility Router receives a call destined to a Remote access client when there is no available resource to handle that call through secure remote voice, it routes the call to the client through the cellular voice network.

CAC can be enforced either on the amount of allocated secure remote access bandwidth, or on the number of simultaneous SRV calls, or on both. If “both” is selected, the restriction applies as soon as either the bandwidth or the calls limit is reached. The value of bandwidth is specified in kpbs (Kilobits per second) and the bandwidth represents unidirectional bandwidth. The restriction is imposed when either receive or transmit bandwidth reaches the specified limit. Default value of bandwidth is 1500 kpbs.

Maximum secure remote voice call applies the call limit to the SRV calls. Default value is 100.

If CAC is not enabled, there is no limitation on the number of calls or network bandwidth used by the SRV calls.

Enabling Call Admission Control

To enable Call Admission Control:

1. Click **Configuration > System > Networking > Remote Access** > **Options** tab.
2. In the Call Admission Control area, select **Enable**.
3. In the **Restriction On** field, choose **Bandwidth**, **Calls**, or **Both**.
    1. **Bandwidth** - when the total bandwidth used by Secure Remote Voice calls reaches the configured level in kbps, any new calls will be routed through the cellular network.
    2. **Calls** - when the number of calls reaches the configured amount, all new calls are routed through the cellular network.
    3. **Both** - when the number of calls reaches the configured amount, all new calls are routed through the cellular network.
4. In the Max Secure Remote Voice Bandwidth field, enter the maximum amount of bandwidth allowed. The maximum is when the total bandwidth used by Secure Remote Voice calls reaches the configured level in kbps. At this point, any new calls will be routed through the cellular network. The number of calls allowed will depend on which voice codecs are in use, based on each codec’s bandwidth.

Supported codecs in order of priority for PBX and Enterprise Client:

- G.711 µ-Law
- G.711 A-Law
- G.722 Codec
- G.729 Annex-B
- AMR
- iLBC 30

Supported codecs in order of priority for Remote Wi-Fi and Cell Data Client:

- iLBC 30
- G.729 Annex-B
- AMR
- G.711 µ-Law
- G.711 A-Law

5. In the **Max Secure Remote Voice Calls** field, enter the maximum number of calls allowed. The default is 100. The valid range is 0-1000.

6. Click **Apply** to save your changes.

For information about configuring routing settings, refer to "Configuring Routing Settings" on page 36.

Monitoring Call Admission Control

To monitor Call Admission Control:

1. Click **Monitor > Calls > Call Admission Control**.

2. View the **Current Bandwidth Usage** and **Current Active Calls** usage for the users in the system, and view **Rejected Calls** due to configuration parameters set in "Enabling Call Admission Control" on page 52.

Voice Recording Support

Use Voice Recording Support to make voice traffic between two Secure Remote Voice clients visible on the eth0 interface. In cases other than when two Secure Remote Voice clients are in use, voice traffic is visible on the eth0 interface when the Mobility Router is in the voice path; in these cases, this option is not required. This option is disabled by default and is a global configuration, not determined by Group or User. In a High Availability (HA) environment, this option is available on the Master node only.

When Voice Recording Support is enabled, the following Mobility Router UDP port rules are used when forwarding to the eth0 interface:

- When the source UDP port is in the range of RAST server flow ports, the default range is 15000 to 24999.

- When the source UDP port is in the range of Media Server RTP Ports, the default range is 25370 to 31999.

For more information, refer to "Mobility Router Ports" on page 193.

To enable Voice Recording Support for voice traffic between two Secure Remote Voice clients:

1. Click **System > Networking > Remote Access**. Select the **Options** page.
2. In the **Voice Recording Support** area, select **Mirror Internal Interface**.
3. Click **Apply**.

Enabling Remote Access for Groups and Users

You can enable Secure Remote Voice and Secure Enterprise Services for a group or for individual users. If you enable Secure Enterprise Services, you can specify whether access is allowed from cellular packet-data networks or remote Wi-Fi networks when users are not in range of the enterprise network.

After you create a group, when new users are created (automatically during provisioning or added manually), those users inherit all group properties, including Secure Remote Voice and Secure Enterprise Services settings.

Enable Remote Access for Groups

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group for which you want to enable remote access. If have not yet created the group, see “Creating Groups” on page 145.
3. Click **Modify**.
4. Click the **User Options** tab.
5. In the **Call Routing** area, select the **Wi-Fi** check box to enable Secure Remote Voice.
6. In the **Data Services** area, select **Cellular Data** enable access to Secure Enterprise Services when users are outside the enterprise:
7. In the **Presence/IM area**, enable or disable Presence on the user devices in this group. By default, Presence is disabled.
   - Select the **Enable** box. When this is selected, options pop up that control whether Presence is available when the device is roaming:
     - **Cellular data** —Select to allow Presence to be shown in cellular packet-data networks.
     - **Cellular Data Roaming**—Select to allow presence and IM activity to be performed on the client while roaming.

Tip

The previous screen is an example configuration. Enable or disable the options as appropriate to the Group settings.

8. To save your changes, click **Apply**.

Enable Remote Access for Users

1. Click **Configuration > Groups and Users > Users**. The Users page displays.
2. Select the user for which you want to enable remote access. If have not yet created the user, see “Creating Users” on page 159.
3. Click **Modify**.
4. Click the **Options** tab.
5. In the **Call Routing** area, select **Wi-Fi** and **Cellular Data** to enable Secure Remote Voice.
6. In the **Presence/IM** area, enable or disable Presence on the user devices. By default, Presence is disabled. Select the box to enable Presence. When this is selected, options pop up that control whether Presence is available when the device is roaming:
   - **Cellular Data** —Select to allow Presence to be shown in cellular packet-data networks.
   - **Cellular Data Roaming**—Select to allow presence and IM activity to be performed on the client while roaming.

Tip

The previous screen is an example configuration. Enable or disable the options as appropriate to the User device.

Tip

Data Services for **Cellular Data** and **Cellular Data Roaming** are automatically enabled when **Presence/IM** is enabled for these two networks. When either of these networks are disabled for Presence/IM, they become active and can be configured in the **Data Services** area for configurations other than Presence/IM.

7. Click **Apply** to save your changes.

Note

Remote Access certificate verification is performed by default. If the configuration does not match, a warning is displayed.

Configuring Mobile Devices for Remote Access

Before end users can use Secure Remote Voice and Secure Enterprise Services, they must add a remote Wi-Fi access point (for example, home access point or Wi-Fi hotspot) as a preferred connection on the mobile device. Doing so allows users to get registered with the Mobility Router. After users are registered, they can place and receive calls and access remote enterprise services, such as directory query, while connected to the remote access point. End users can also access Secure Enterprise Services using a remote Wi-Fi or cellular packet-data network.

Monitoring Active Users

Use the Active Users monitoring page to get real-time information about remote user activity. To monitor active users:

1. Click **Monitor > Users > Active Users**.
2. Select the users that you want to monitor.
3. Click **User Monitoring**. The **Monitoring** page displays information for this user.

Monitoring Remote Users

Use the Active Remote Users monitoring page to get real-time information about remote user activity. To monitor remote users:

1. Click **Monitor > Users > Active Remote Users**.
2. On the user's mobile device, try to establish a Secure Remote Voice tunnel. Messages regarding the Secure Remote Voice session appear when the tunnel is established. You can monitor status of calls made while the user is using Secure Remote Voice and verify that the mobile device is authenticating and registering with the Mobility Router for the session.
3. On the user's mobile device, end the Secure Remote Voice connection. Messages regarding the Secure Remote Voice session appear when the tunnel is terminated.

Troubleshooting Remote Access

The following lists issues you might encounter after implementing remote access and how to verify your configuration.

- Users are not able to create a tunnel on the mobile device.
  - If you are using a firewall, verify that the appropriate ports and IP addresses are publicly accessible.
  - If you are using a firewall, verify that the firewall rule forwards traffic received on the external IP address to the eth1 IP address of the Mobility Router.
  - Click **Configuration > System > Networking > Remote Access**. verify that the IP addresses and ports used for remote access are configured properly.
  - Verify that Connect Platform has received the latest configuration information from the Mobility Router. Users can get the latest configuration when they connect their mobile devices to the enterprise Wi-Fi network.
  - Decrease the MTU size for the tunnel interface (**Configuration > System > Networking > Remote Access > General** tab).

- Users cannot hear the other parties while on calls using Secure Remote Voice.
  - Review user information about the Active Remote Users page (**Monitor > Users > Active Remote Users**). Find a user who is having the problem and check the data in the Rx Packets and Tx Packets columns. These counters should increase at the same pace. If they do not, there is configuration problem.
  - Verify that the default gateway has a route defined to forward packets sent to the client pool IP addresses to the eth0 interface of the Mobility Router.

- Users report poor voice quality for Secure Remote Voice calls.
  - Verify that the TLS or DTLS tunnel is established between the mobile device and the Mobility Router.
  - If the tunnel is using TLS, use DTLS for the tunnel.
  - Decrease the MTU for the TLS and DTLS protocols (**Configuration > Networking > Remote Access > Protocol** tab). If modify the MTU value, you or the user must exit, and restart Connect Platform on the mobile device being tested.
  - Consider enabling or raising the priority of a voice codec that handles packet loss better (for example, iLBC or G.729) if you are encountering packet loss on the remote Wi-Fi network.

CHAPTER

7

Managing Security

The mobility solution uses the following certificates to secure communications between the Mobility Router and mobile devices running Connect Platform (previously known as Mobility Client):

- Certificate authority (CA)—Certificate used by the Mobility Router to sign Mobility Router and client certificates.
- Mobility Router certificates—Certificates used by the Mobility Router to identify itself to its clients.
- Client certificate—Certificate issued by the Mobility Router to the client applications that is used to verify the client's identity to the Mobility Router. Connect Platform applications include the Connect Platform and Mobility Calibrate.

You can generate certificates on the Mobility Router, import self-signed certificates, or certificates from other certificate authorities.

This chapter contains the following sections:

Certificate Authority

The certificate authority (CA) in the Mobility Router is used to sign certificates generated by the Mobility Router. The Mobility Router generates and signs a client certificate for every client that is provisioned. The Mobility Router can also generate and sign the Mobility Router certificates if you choose to use a generated certificate instead of an imported certificate.

You must either generate or import a CA because there is no preinstalled factory-default CA. Without a generated or imported CA, users cannot be provisioned, and Mobility Router certificates cannot be generated.

Generating a Certificate Authority

To generate a certificate authority:

1. Click **Configuration > System > Certificate > Certificate Authority**. The **Certificate Authority** page displays.
2. Click **Generate**. The **Generate Certificate** page displays.
3. In the **Country Name** field, type the two-letter country code for the country where the Mobility Router is located. The default is US.
4. In the **State or Province**, field, type the state or province where the Mobility Router is located.
5. In the **Locality** field, type the locality where the Mobility Router is located. Typically, this is the name of a city.
6. In the **Organization** field, type the name of the organization. Typically, this is the name of the company.

7. In the **Organization Unit** field, type the name of the organization unit (or example, enter the name of a department within the organization).
8. In the **Common Name** field, type the domain name for the Mobility Router. The default value is the domain name on the Express Setup page and can be changed as needed.
9. Click **Generate**. A warning message displays:

```
Generating Client Certificate Authority certificate invalidates provisioning status
of existing client applications. All provisioned clients will stop working until
they are reprovisioned. Generate the certificate?
```

10. To generate the certificate, click **OK**.

Note

The generated certificate displays in a separate window. The Last Generated Date field updates to the current date and time. Verify that the certificate was created correctly by checking the status line at the top of the certificate.

11. Click Close to close the certificate window.
12. A restart prompt displays. Do one of the following:
    - Click **OK** to restart the mobility service and activate the newly generated certificate.
    - If you do not want to restart the Mobility Router, click **Cancel**. The newly generated certificate will be activated on next restart.

Importing a Certificate Authority

You can import a Certificate Authority (CA) certificate to the Mobility Router.

Note

An imported certificate must be in unencrypted Privacy Enhanced Mail (PEM) format and contain the X.509 certificate and the RSA key. Make sure the certificate contains Beginning and End lines within the certificate file.

To import a certificate authority:

1. Click **Configuration > System > Certificate > Certificate Authority**. The **Certificate Authority** page displays.
2. Click **Import**. The **Import Certificate** page displays.
3. Paste the certificate and private text key into the text box on the **Import Certificate** page.
4. Click **Import**. A warning message displays as follows:

```
Warning: Importing Certificate Authority certificate invalidates provisioning status
of existing client applications. All provisioned clients will stop working until
```

```
they are reprovisioned. Press OK if you want to import the certificate. Press Cancel
otherwise.
```

If the certificate is valid, a Restart prompt displays. If the certificate is not valid, an Error prompt displays. In the case of an error, generate a valid certificate or obtain a new certificate to paste in the field.

Note

Optionally, click Verify to view if the certificate is valid.

5. Restart the mobility service and activate the newly generated certificate, click **OK**.

Note

If you do not want to restart the Mobility Router, click Cancel. The newly generated certificate is stored on the Mobility Router until the next restart.

The **Last Generated Date** field updates to the current date and time. Verify the certificate was created correctly by checking the status line at the top of the certificate. The following is an example of an imported certificate authority:

```
-----BEGIN CERTIFICATE-----
MIIDgjCCAuugAwIBAgIET3ISpjANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU3Vubnl2YWxlMREwDwYD
VQQKEwhTaG9yZVRlbDEUMBIGA1UECxMLRW5naW5lZXJpbmcxFDASBgNVBAMTC3Jh
bXItZGV2MTAuMB4XDTEyMDMyNjE5MTkwMloXDTMyMDMyMjE5MTkwMlowdTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEjAQBgNVBAcTCVN1bm55dmFs
ZTERMA8GA1UEChMIU2hvcmVUZWwxFDASBgNVBAsTC0VuZ2luZWVyaW5nMRQwEgYD
VQQDEwtyYW1yLWRldjEwLjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtCOH
5MkPjSM+8w93QGat5TmfR3M2DuhQjI9YwUqZrVAHOA23WqFG5MqQEUi8CRFwfvvC
QYLnqlZW5w9GBCOAlRRH1/Gu4fLLZsKAt4AZvZ+dE8qmgQ5+tJh/7sb6t+P265qv
e+zsw3ZfbJgYpKjVZ0M4PLd0VaX8a9g8sU+S/IMCAwEAAaOCAR0wggEZMAwGA1Ud
EwQFMAMBAf8wEQYJYIZIAYb4QgEBBAQDAgTwMDIGCWCGSAGG+EIBDQQlFiNSQSBN
b2JpbGl0eSBSb3V0ZXIgUm9vdCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUEkJGzl4q
Gw4oDPi6UGA11oTS7pwwgaIGA1UdIwSBmjCBl4AUEkJGzl4qGw4oDPi6UGA11oTS
7pyheaR3MHUxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYD
VQQHEwlTdW5ueXZhbGUxETAPBgNVBAoTCFNob3JlVGVCMRQwEgYDVQQLEwtFbmdp
bmVlcmluZzEUMBIGA1UEAxMLcmFtci1kZXYxMC6CBE9yEqYwDQYJKoZIhvcNAQEF
BQADgYEAgi6+yrZdyU6PD3uYkEU39QXLGRfipt96WzYBDjttTb+LttoitcwUDoCD
S47/1FiBWrt+I9eqRxLoQQYrWy/n60qmwHUz9HC4YzY78FB8gwwsgdKBNvhHzqs+
hnYvBrsaZS5KPOZVNusrLwkEKopLvxujKGSq/vi64rqKrF+AvS0=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,520383B070CB9EDA

gyk/BTHISosifGwnl5Kfl1QQRki9ynZVZAsV7UtVEcMpMNyjC+sC1Ofa+MMHHNkg
KMJTOY+O+hxmqavvTEn05kvWxMrwks5Q/6WUUaCFmgSf1usOmnb2kuchwo+cE8yZ
FjEyXij61JUKKVxTj+TPlerhEiJtqgn7TmUvvTcbbYSEirHtiUvz/ef5HXBymc16
1p9CT0OsLseu26Lq6WThR7pyebcNxPk+uwjlsZlzMTbt+rL4CMFNhh4sBteUJU2n
h3yc6n7Xw6FedpfEbjQFn8UkTktxnHYAv8Ea4JycYXJ1XBR3F+vHE0d+9CCYyxX1
```

```
N7iiNGnWfAEwLXdycR/WzYQIER92Pgf5CRbtyDfH3P3340IpNntokrMPoY9CuZPl
FGN8OtTqBix45ls14StCkdUQugWrt6eQFi8BNdxXR7HofPDS6v9on+8XFqeDtvlD
zAuF8UQENcjbK75Vn3SjlQcwFrHifL/+NhSZUvrtHsGh9BsNS/DBxkiwbncRnr4Y
aTQMNtJizlxkGaTmgt92ZoVevR0ZRleVHnpnGjp7EQaLHz3d9oJEhjMyAzOfAsGn
Qx5vbHg08CLGKw1y78lyxrvSHWBJJzPnjqAasW6Qp7zlxgBcV9lCYlsVL0+yQnkJ
Uv+dEKEBxKnV4uNAOYWo2OTJM6ngCqmFkInaSrVJhUhmKskHHP254/BQDAc/JQCT
OqYSlas/jIm0DF2zmADSICQyj1ZJ7TS281XekRfK1gdot98Q4IzrvJ+lZjFd19zI
CA4pT+Ubxw69cTdZLB3ObRibBjJlNb84eqhhJu1hW5gsqWcgkehuRA==
-----END RSA PRIVATE KEY-----
```

Mobility Router Certificates

There are four Mobility Router certificates which establish secure sessions during client provisioning and create HTTPS sessions to the Mobility Router. In addition, these certificates establish mutually authenticated secure remote connections when the clients are outside of the enterprise.

WARNING!

Before proceeding with the following steps to generate a Mobility Router Certificate, first install the Certificate Authority (CA). See “Certificate Authority” on page 60.

The Mobility Router presents different certificates when a client initiates a connection from local or remote interfaces.

Generate a Mobility Router virtual certificate only if you are creating a redundancy cluster to provide stateful high availability for the mobility solution. This is the certificate used by the virtual IP address that manages the redundancy cluster. When the Mobility Router runs in redundancy mode, both nodes must use the same virtual certificates. For information about redundancy clusters, see “Managing Redundancy Clusters” on page 181.

The following local, remote, and virtual certificates are supported:

- **Local Access**—internal connections over the LAN interface in a standalone configuration inside the enterprise.
- **Remote Access**—connections using Secure Remote Access with Connect Platform in standalone configuration.
- **Local Access (Virtual)**—internal connections over the LAN interface in cluster configurations inside the enterprise and synced across all cluster nodes.
- **Remote Access (Virtual)**—connections using Secure Remote Access with Connect Platform in cluster configurations.

WARNING!

When generating or importing a virtual certificate on the master node, the certificate is automatically synced to the standby node. All services on all nodes must be restarted for the new certificate to be valid

Locally Generated Certificates

You can create a locally generated certificate on the Mobility Router. This is a convenient option for enterprises that have not already purchased a certificate. The certificate is signed by the certificate authority on the Mobility Router.

Certificate Signing Request

Administrators can generate a Certificate Signing Request (CSR) for all Mobility Router Certificates. The Mobility Router stores only one set of CSRs and corresponding private keys per type of certificate, and automatically syncs them to the standby node, if applicable.

Generating a Mobility Router Certificate

WARNING!

Before proceeding with the following steps to generate a Mobility Router Certificate, first install the Certificate Authority (CA). See "Certificate Authority" on page 60.

The Mobility Router Certificate page displays the date and time that the last certificate was generated.

1. Click **Configuration > System > Certificate > Mobility Router**, and then do one of the following:
   - If you are running a Mobility Router in a standalone environment, select **Standalone** to generate a Local Access or Remote Access certificate.
   - If you are running a Mobility Router in a clustered configuration, select **Clustered** to generate a Local Access or Remote Access certificate.

Note

The following example generates a standalone Remote Access certificate.

2. Click **Generate**. If the remote access configuration does not match the certificate, a warning message displays as follows:

```
Warning: Certificate Subject CN <> does not match Remote Access configuration <>.
```

3. In the **Country Name** field, type the two-letter country code for the country where the Mobility Router is located. The default is US.
4. In the **State or Province**, field, type the state or province where the Mobility Router is located.
5. In the **Locality** field, type the locality where the Mobility Router is located. Typically, this is the name of a city.
6. In the **Organization** field, type the name of the organization. Typically, this is the name of the company.
7. In the **Organization Unit** field, type the name of the organization unit (for example, enter the name of a department within the organization).

8. In the **Common Name** field, type the FQDN, hostname or IP Address for the Mobility Router.

Note

When generating a Local Access certificate, the default value is the local FQDN of the Mobility Router. When generating a Remote Access certificate, the default value is the external FQDN of the Mobility Router if configured in **System > Network > Remote Access > Remote Access FQDN**. See "Configuring General Settings" on page 47.

9. Select the strength of the private key from the **Key Length** pulldown menu. The longer the number, the stronger the security of the key. The default is 1024.

10. Select any combination of the default **Alternative Names** displayed or add your own by entering it in the **Other Alternative Names** field. (Click **Add** if entering an address in this field.) These additional addresses will be added to the locally generated certificate or CSR and display in the **Subject Alternative Names** field as they are selected.

11. Click **Generate** to generate a certificate signed by the certificate authority installed on the Mobility Router or click Generate CSR to generate a certificate signing request (CSR) to be sent to a third-party certificate signing authority.

WARNING!

When generating a CSR, the Mobility Router outputs both a certificate request as well as an RSA private key. Save the RSA private key in a secure location for future use. This information is necessary when importing the signed certificate.

Note

The private key of the CSR is stored in the Mobility Router.

12. If generating a CSR in the previous step, submit the CSR to a trusted certificate signing authority and save the RSA private key.

13. If a restart prompt displays, do one of the following:

    - Click **OK** to restart the mobility service and activate the newly generated certificate.
    - If you do not want to restart the server, click **Cancel**. The newly generated certificate will not take effect until the next restart.

14. Refresh the browser to regain access, then log in.

Importing a Certificate to the Mobility Router

You can also import a purchased or self-signed certificate for any of the four Mobility Router certificates. For example, if you purchased a certificate from VeriSign, that certificate can be imported and used by the Mobility Router. You can also import wildcard certificates for any of the four Mobility Router certificates.

Note

A wildcard certificate only supports the same level of sub-domains. For example, “*.acme.com” will secure “mobility.acme.com” and “vpn.acme.com”, but not “vpn.mobility.acme.com”.

Note

The Mobility Router's local access certificate is used for the secure connections initiated from the internal network; the remote access certificate is used for the secure connection initiated from the external networks such as homes and hotspots. Mitel recommends use of FQDN rather than IP address for imported remote access certificates.

1. Click **Configuration > System > Certificate > Mobility Router**, and then do one of the following:
   - If you are running a Mobility Router in a standalone environment, select **Standalone**.
   - If you are running a Mobility Router in a clustered configuration, select **Clustered**.

Note

The following example generates a clustered Remote Access certificate.

2. Click **Import**. The **Import Certificate** window displays.
3. Paste the Mobility Router certificate issued by the trusted certificate authority, RSA private key, and the intermediate and root certificates you may have received from the certificate signing authority. Be sure to include both “BEGIN” and “END” statements for all information in the following order:
   - Mobility Router signed certificate
   - RSA private key
   - Any certificate chain/bundle that may have been included from the certificate authority

Note

The text in the following window displays an example of section of a certificate, beginning with a portion of the Mobility Router signed certificate, the RSA private key, and a portion of the bundle the certificate authority included for the Mobility Router certificate. Be sure to use unencrypted certificates and the private key in unencrypted PEM format. In addition, be sure to add an empty line (press Enter) between the line “END RSA PRIVATE KEY” and “BEGIN CERTIFICATE”, as shown.

4. Click **Import**. If the certificate is valid, a Restart prompt displays. If the certificate is not valid, an Error prompt displays. In the case of an error, generate a valid certificate or obtain a new certificate to paste in the field.

Note

Optionally, click Verify to view if the certificate is valid.

5. Restart the mobility service and activate the newly generated certificate, click **OK**. If you do not want to restart the Mobility Router, click **Cancel**. The newly generated certificate is stored on the Mobility Router until the next restart.

6. Refresh the browser to regain access, then log in.

Connect Platform Certificates

Connect Platform certificates are generated by the Mobility Router. The client certificate is signed by the CA on the Mobility Router and sent to the client during provisioning. This is automatic, and no administration is required.

Managing the Permit List

The permit list is a list of valid client certificates issued by the Mobility Router. When an end user provisions the Connect Platform on the mobile device, the client's certificate is automatically entered in the permit list.

Reviewing the Permit List

Click **Configuration > System > Certificate > Permit List**. The **Permit List** page displays. The following information is displayed:

- **Serial Number**— Unique number used to identify each certificate. The Certificate Authority assigns a unique number to each certificate it generates and signs.
- **Active**—Indicates that the certificate is active.
- **Application**—Specifies whether Connect Platform or Calibrate is using the certificate.
- **User ID**—User name of the end user on the Mobility Router.
- **Device Type**—Type of mobile device using the certificate. This information matches the information about the **Mobile Device** tab of the **User** page.
- **IMEI**—Displays the International Mobile Equipment Identity (IMEI) of the client mobile device. This information is provided automatically during client provisioning. The IMEI is a number unique to every GSM and UMTS mobile phone.

Note

The permit list entries for Mobility Calibrate do not display details about User ID, Device Type, or IMEI.

Deleting an Entry from the Permit List

You can delete an entry from the permit list to revoke an application for a specific user. Delete an entry from the permit list if a mobile device is lost or you no longer want the user to have access to certain applications.

To delete an entry from the Permit List:

1. Click **Configuration > System > Certificate > Permit List**.
2. Select the entry to be deleted.
3. To select multiple contiguous items, hold the Shift key while selecting the items. To select multiple non-contiguous items, hold the Ctrl key while selecting the items.
4. Click **Delete**.
5. When prompted to confirm the deletion, click **OK**.

CHAPTER

8

Configuring Authentication

There are three options for user authentication available with the mobility solution, one of which uses AAA (authentication, authorization and accounting) functionality:

- Local user's authentication database
- Directory Authentication

In addition to specifying the authentication method, you can also specify the order in which authentication methods are attempted.

This chapter contains the following sections:

Directory Authentication/ Trusted Admin App

You can specify a Directory to be used for authentication as needed. Defining a Directory is mandatory for users with PBX for Connect.

The following procedure configures a Directory server.

1. Run cd “C:\Program Files (x86)\Shoreline Communications\ShoreWare Director\App\bin” pki.bat -S SMRAdminApp in a Command Prompt window on the HQ server

   To generate the certificate for the CMR they are in the Shoreline Data\keystore\certs directory and copy the contents of the following cert and key files:
   SMRAdminApp.crt - located in cert folder within the above root directory
   SMRAdminApp.key - located in private key folder within above root directory

   Set Up Trusted Server Applications for the CMR
   Complete the following steps to set up trusted server applications for the CMR:

2. Log in to Mitel Connect Director and navigate to System > Security >Trusted Server Application.

3. Click New, and complete the following steps to create a new trusted server application for the Mobility 9.x SMR:

4. Specify the Trusted account name. This should be a descriptive name that conveys the location and use of the SMR. This information is for reference only.

5. Browse to Shoreline Data\keystore\certs and select the SMRAdminApp file.

6. Select Client Application Service in Application Type and select Enabled.

7. In Property Type, select admin-cas in Available, and then click to move it to Selected.

8. Click Save

   Navigate to the Mobility Router:

9. Click **Configuration > System > Authentication > Directory**.

10. Click **Add**.

11. Select **Mitel Directory** from the Server Type drop-down list.

12. Enter a **Name**.

13. Click **Apply** to advance to the Add New Directory Group parameters page.

14. Enter a fully qualified domain name (FQDN) or IP address of the HQ server or local DVS server (if you have installed CMR for remote site) in **Server Address** field.

15. In the **Server Port** field, use the default port number, or enter an appropriate port number if your server uses a different port.

16. Select the **Server Certificate Verification** box if **TLS** is used for a secure session using STARTTLS method. TLS provides more secured authentication. Hence, it is recommended. Click the **Manage Certificate** link.
17. Click **Import.** Copy and paste the appropriate hq_ca Certificate. The hq_ca.crt is stored in C:\Shoreline Data\keystore\certs.
18. Select Trusted Admin App, and then click the Manage App Certificate link to launch the Directory Server Certificate page.
19. Click Import and paste the contents of the cert and key files you copied in step 1 of this section.
20. Click Import again, and then cancel the prompt to reboot.
21. In the **Bind Timeout** field, use the default timeout number 5 or enter another appropriate timeout value.
22. In the **Search Timeout** field, enter the number of seconds to wait for a search response from the server.
23. In the **Max Search Entries Returned** field, enter the maximum number of displayed search responses.
24. Choose TLS from the **Security Type** drop-down list.
25. Use the default **Secure Port** value or enter an appropriate port number if your server uses a different port.
26. Click **Apply**.
27. Click **Verify** to verify the server configuration is correct.

Note

If verification is not successful, select **Security Type "None"** to make sure other parameters are correct, then retry the selected security type.

28. Select **Query** to perform the Directory search. The Query screen displays.
    a. Enter a search string such as a user name in the **Search For** field. Refer to Directory Query on page 214 for more information about this field.
    b. By default, the **Search In** drop down menu displays the currently configured Directory server. Select the specific Directory server to complete a search. Refer to Directory Query on page 214 for more information about this field.
29. Click **Sync ABC Keys** to exchange the authenticator public keys with HQ and DVS servers.
30. When you add or remove DVS server, you click **Sync ABC Keys** again.

Adding a Directory Group

The following procedure configures a Directory server.

1. Click **Configuration > System > Authentication > Directory**.
2. Select **Add**.
3. Select **Mitel Directory**.
4. Enter a **Name**.
5. Select **Apply** to advance to the Directory Group parameters page.
6. Select an **Interface**. By default, the IP address associated with the primary interface is chosen. This interface is used by the Mobility Router for communicating with HQ and DVS servers.

Note

This option is only configurable when used in conjunction with Connect and multi-tenant system.

7. Enter a fully qualified domain name (FQDN) or IP address of the Directory server in **Server Address** field.
8. In the **Server Port** field, use port number 5447 or enter another appropriate port number.
9. In the **Bind User** field, type the credentials used for authenticating with the Directory Server.
10. In the **Bind Password** field, enter the Bind DN password to bind to the Directory Server. This password must be available for the Mobility Router to make an authentication request.
11. In the **Bind Timeout** field, use the default timeout number 5 or enter another appropriate timeout value.
12. In the **Search Timeout** field, enter the number of seconds to wait for a search response from the server.
13. In the **Max Search Entries Returned** field, enter the maximum number of displayed search responses.
14. Click **Apply**.
15. Select **Query** to perform the Directory search. The Query screen displays.
    a. Enter a search string such as a user name in the **Search For** field. Refer to “Directory Query” on page 214 for more information about this field.
    b. By default, the **Search In** drop down menu displays the currently configured Directory server. Select the specific Directory server to complete a search. Refer to “Directory Query” on page 214 for more information about this field.
16. Click **Verify** to verify the server configuration is correct.

Managing Local User Authentication

There are three types of users who require authentication on the Mobility Router:

- Administrator—Authenticates to the Mobility Router to administer the mobility solution. Users with Administrator access have root level permissions on the server.
- Monitor—Authenticates to the Mobility Router to monitor the mobility solution.
- End user—Authenticates to the Mobility Router to provision and use the Connect Platform application.

Any user defined in Mobility Router's built-in database server with the "Admin" or "monitor" role can administer and monitor the Mobility Router.

Note

Local users with end-user privileges are created in the Add Groups or Add Users pages. For information about adding local end users, see Managing Groups on page 144 and Managing Users on page 158.

Adding Local Users

To add a local user:

1. Click **Configuration > System > Authentication > Local Users**. The **Local Users** page displays.
2. Click **Add** to view the **Add User** page.
3. In the **User ID** field, type the name of the user. This field is case sensitive.
4. In the **Password** field, type the password for the user. This field is case sensitive.
5. In the **Capability** list, select the type of account.
   - For SIP Local Users, select from the following:
     - admin
     - monitor
     - user
   - For non-SIP Local Users, select from the following:
     - admin
     - monitor
6. To enable the user, select the **Enabled** check box.
7. To save your changes, click **Apply**.

Modifying Local Users

Note

For the admin and monitor default user accounts, you can change only the password. Passwords should not be left at default and must meet the customers password security policy such as complexity, length and so on.

To modify a local user:

1. Click **Configuration > System > Authentication > Local Users**. The **Local Users** page displays.
2. Select the user to be modified and click **Modify**. The **Modify User** page displays.
3. Modify the values as needed.
4. To save your changes, click **Apply**.

Deleting Local Users

The default Monitor and Admin users cannot be deleted. Other users with the capability of Monitor or Admin can be deleted. Customers must maintain Local Users accounts and ensure that when a user leaves the company that their account is also deleted.

Local end users on SIP cannot be deleted on this page. For information about deleting users, see Managing Groups on page 144 and Managing Users on page 158.

To delete a local user:

1. Click **Configuration > System > Authentication > Local Users**. The Local Users page displays.
2. Select the local user to be deleted.
3. Click **Delete**. The user is deleted.

Managing Order of Authentication

After defining local authentication or adding authentication servers, specify the order in which the Mobility Router performs authentication against the established databases. The order determines the search order that the Mobility Router uses when attempting authentication. The order of authentication can be defined separately for Admin users and for End Users: Admin privilege users logged in to the Mobility Router using the Web UI, Connect Platform Administrator provisioning, and so on, use the Admin Authentication Ordering; End users logged in to the Mobility Router for Connect Platform provisioning use the User Authentication Ordering.

By default, the first metho
d of authentication attempted is authentication with the local user database on the Mobility Router. We recommend that you keep the default for the first method.

After successful authentication, the Mobility Router discontinues searching. If the Mobility Router is unsuccessful in authenticating using the first method specified, the search order defined is used to continue the search.

To set the order of authentication:

1. Click **Configuration > System > Authentication > Ordering**.

   The Ordering page displays.

2. In the **First** list, select the authentication method to be used first:

   - local—Uses the Mobility Router local user database pulling from the trusted admin application connection

   The Mobility Router first attempts authentication with the option specified in this field.

3. If you defined more than one method of authentication, set the **Second** field to an option different than the one selected for the **First** field. The Mobility Router attempts to authenticate with this setting if it cannot authenticate with the option specified in the **First** field.

4. If you have three options for authentication, set the **Third** field to an option different than the one selected for the **First** or **Second** fields. The Mobility Router attempts to authenticate with this setting if it cannot authenticate with the option specified in the **First** or **Second** fields.

Note

One of the Authentication mechanisms for both Admin and User Authentication must be local and is recommended as the First authentication.

Note

If you have only one authentication option, set the Second and Third field to the same value as the First field. If you have only two authentication options, set the Third field to the same value as the First or Second field.

Note

The Admin authentication ordering is different than the End User authentication order.

1. Click **Apply**.

CHAPTER

9

Managing Mobility

An enterprise location provides the framework in which you can configure and monitor your mobility network. In an enterprise location, you define the physical representation of the network, consisting of one or more campuses, one or more buildings, and all floors where the mobility solution is to be deployed.

After creating the enterprise location, you can define Route Points, which are the locations within the campus where the Mobility Router hands overactive calls between Wi-Fi and cellular networks. You define Route Points based on where Wi-Fi coverage is typically weakening. Common Route Points include the entry/exit points of a building, elevator entrances, or stairwell entrances. You can define Route Points using the Mobility Router or the Mobility Calibrate application on your mobile device.

Depending on the WLAN controllers used in your network and how you have configured them, you can configure the Mobility Router to get location information directly from the WLAN controller. This saves you from having to manually define the enterprise location. Depending on the WLAN controller, the Mobility Router can also get SSID, BSSID, and transmit power information, allowing you to have a more accurate representation of your network.

In addition to the previous methods for defining location, the Mobility Router gathers location information from Connect Platform on the mobile devices as users roam from access points known by the Mobility Router to unknown access points. If the mobile device roams from a known access point to an unknown access point, Connect Platform sends a query to the Mobility Router with the unknown access point's information. The Mobility Router adds this access point to its list of known access points.

This chapter contains the following sections:

Establishing Default Mobility Settings

Default mobility settings are applied to locations where a calibrated Route Point is not specified or not needed. In this case, the default settings trigger the handover as needed. The default mobility settings and enterprise-location specific settings combine to support seamless roaming between the Wi-Fi and cellular network, which ensures that the mobility solution optimizes the available Wi-Fi network and reduces use of the cellular network while inside the enterprise.

The Mobility Router uses default mobility values for voice call quality. These default values can be used for two purposes:

- To establish initial mobility values when creating new enterprise locations. You can adjust the default mobility settings per floor when creating Route Points, or you can use the default settings. Per-floor settings apply only if Route Points exist.
- To determine when a handover should take place in locations where no Route Points are established, or Route Points are not needed. These settings apply only if no Route Points are present.

In addition to specifying default mobility settings for the enterprise, you can also specify default mobility settings for home locations for users. These default mobility settings apply to all home locations unless you override these settings by modifying them for specific home locations for users. For information about modifying mobility settings for user home locations, see Modifying Home Location General Settings on page 169.

You can review or change the default mobility settings to meet your network requirements.

Enterprise Default Settings

To review or change Enterprise default mobility settings:

1. Click **Configuration > Mobility > Default Settings**. The **Enterprise** tab is active.
2. In the **Min Wi-Fi to Cellular Roam RSSI** field, type the minimum Wi-Fi received signal strength indication (RSSI) threshold below which a call is handed over from Wi-Fi to cellular.

   This value represents the minimum threshold for weak coverage areas in the network. It can be used as a backup if a Route Point is missed or for areas that have weak coverage but do not yet have a Route Point specified.

   The default value is -80. The recommended value is between -95 and -40.

3. In the **Min Cellular to Wi-Fi Roam RSSI** field, type the minimum Wi-Fi RSSI threshold that must be available for a call to be handed over from cellular to Wi-Fi. The default value is -65. The recommended value is between -95 and -40.

   This value applies only in cases where the handover is not triggered by a Route Point. This value should represent an RSSI that is typically available only within the building so handover to Wi-Fi does not occur outside. This value is also used as a backup for handing over to Wi-Fi if the user misses connecting with a Route Point when entering the building.

   If a Route Point is present, the handover is triggered based on the Route Point specific settings, even if they are different than the Min Cellular to Wi-Fi Roam RSSI value.

4. In the **Min Voice RSSI** field, type the minimum RSSI threshold for incoming and outgoing voice calls.

   This value represents the minimum RSSI allowed for initiating a voice call. If this value is not met or exceeded, then Wi-Fi is not available.

   The default value is -72. The recommended value is between -95 and -40.

5. In the **Max Packet Loss %** field, type the maximum average percentage of voice packet loss allowed before the call is handed over to cellular. The default value is 10%. If average packet loss exceeds this value, the call is handed over to the cellular network if the cellular network is available.

6. To enable use of multiple BSSIDs in your network, select the **Multiple BSSID** check box. To disable this option, clear the **Multiple BSSID** check box. By default, this option is selected. We recommend that you leave this option enabled. If the Multiple BSSID option is selected, you can take calibration data from one WLAN, and that data can support all WLANs at that location. If this option is not selected, each WLAN must be calibrated individually.

7. To save your changes, click **Apply**.

8. Table 4 displays the client-preferred PBX and Enterprise Codecs priority listing. The following table displays each Codec's supported packet size and default packet size.

Table 4: Supported Codecs

Codec name	Supported Packet Size	Default Packet Size
G.711 µ-Law	20/30/40/60	20
G.711 A-Law	20/30/40/60	20
G.729 Annex- B	20/30/40/60	20
AMR	20/40/60	20
iLBC 30	30/60	30

Use the Up or Down buttons to select the highest priority Codec supported by both ends. Move the Codecs into their appropriately ranked order for usage, the top Codec being the highest priority.

Default Home Settings

To review or change home-location default mobility settings:

1. Click **Configuration > Mobility > Default Settings**.
2. Click the **Home** tab.
3. In the **Min Wi-Fi to Cellular Roam RSSI** field, type the minimum Wi-Fi received signal strength indication (RSSI) threshold below which a call is handed over from Wi-Fi to cellular. The default value is -76. The recommended value is between -95 and -40.
4. In the **Min Cellular to Wi-Fi Roam RSSI** field, type the minimum Wi-Fi RSSI threshold that must be available for a call to be handed over from cellular to Wi-Fi. The default value is -70. The recommended value is between -95 and -40.
5. In the **Min Voice RSSI** field, type the minimum RSSI threshold for incoming and outgoing voice calls. This value represents the minimum RSSI allowed for initiating a voice call. If this value is not met or exceeded, then Wi-Fi is not available. The default value is -72. The recommended value is between -95 and -40.
6. In the **Max Packet Loss%** field, type the maximum average percentage of voice packet loss allowed before the call is handed over to cellular. The default value is 10%. If average packet loss exceeds this value, the call is handed over to the cellular network if the cellular network is available.
7. Click **Apply** to save changes.
8. The applicable Codecs display in the table. Use the Up or Down buttons to select the highest priority codec supported by both ends. Move the codecs into their appropriately ranked order for usage, the top codec being the highest priority.

Default Cell Data Settings

To review or change cell-data default mobility settings:

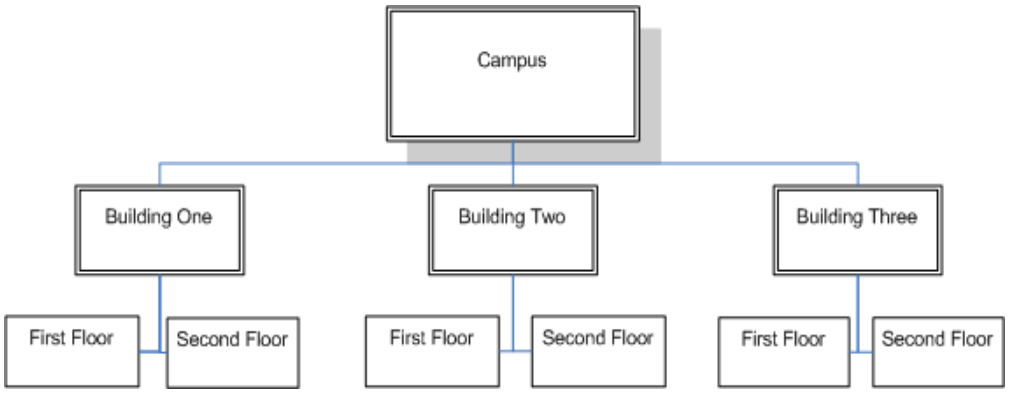
1. Click **Configuration > Mobility > Default Settings**.
2. Click the **Cell Data** tab.
3. The applicable Codecs display in the table. Use the Up or Down buttons to select the highest priority codec supported by both ends. Move the codecs into their appropriately ranked order for usage, the top codec being the highest priority.
4. Click **Apply** to save changes and return to the main screen.

Enterprise Locations

About Enterprise Locations

An enterprise location consists of a campus, a series of buildings, and all the floors where the mobility solution is deployed. Figure 7 shows an example of an enterprise location. In this example, the campus has three buildings, and each building has two floors. The campus layout is entered as an enterprise location in the Mobility Router. For information about creating enterprise locations, see Creating Campuses on page 89.

Figure 7: Sample Enterprise Location Layout



About Route Points

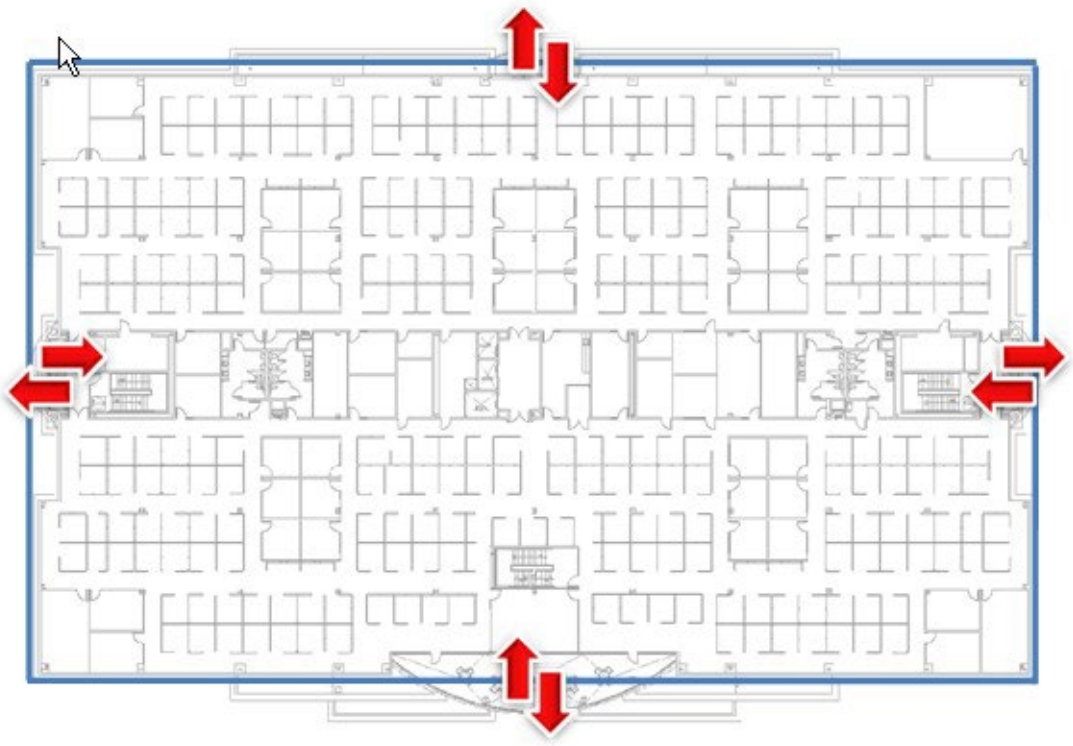
A Route Point is a specific location within the campus where you want to handover between Wi-Fi and cellular. Some common route points include the entry/exit points of a building, at the entrance to an elevator, or at the entrance to a stairwell. If a building has a unique shape, Wi-Fi coverage might not reach to some remote corners of the floor.

Areas where the Wi-Fi signal has a received signal strength indication (RSSI) threshold below the level acceptable for voice calls should be marked as Route Points. If there are no locations on a given floor of a building where a handover needs to take place, you do not need to create Route Points on the Mobility Router for that floor.

Route Points can be predefined or created during the calibration process. Calibrate Route Points by taking readings of Wi-Fi signal strength.

Figure 8 shows the first floor of Building One. There are four places where Route Points could be created. These places are entered the Enterprise Location menu as Route Points for this specific building and floor. For information about adding Route Points, see “Creating Route Points for a Floor” on page 91.

Figure 8: Example of Route Points on the First Floor of a Building



Understanding the Relationship Between Route Points and Default Handover Settings

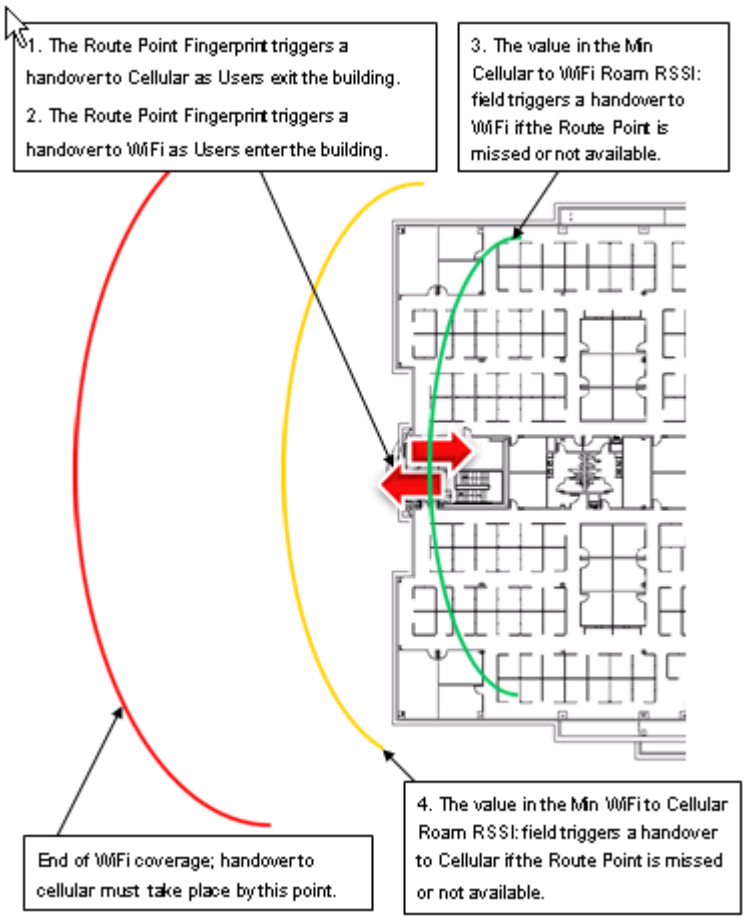
The Min Wi-Fi to Cellular Roam RSSI value specifies the minimum Wi-Fi received signal strength indication (RSSI) threshold below which a call is handed over from Wi-Fi to cellular. This value represents the minimum threshold for weak coverage areas in the network. It can also be used as a backup in case a Route Point is missed or for areas that have weak coverage but do not yet have a Route Point specified.

The Min Cellular to Wi-Fi Roam RSSI value specifies the minimum Wi-Fi RSSI threshold that must be available for a call to be handed over from cellular to Wi-Fi. This value applies only in cases where the handover is not triggered by a Route Point. This value should represent an RSSI that is typically only available within the building so handover to Wi-Fi does not occur outside. This value is also used as a backup for handing over to Wi-Fi if the user misses connecting with a Route Point when entering the building.

If a Route Point is present, the handover is triggered based on the Route Point-specific settings, even if they are different than the values in these fields.

Figure 9 shows the relationship between Route Points and default handover settings at an entry point of a building.

Figure 9: Example of the Relationship Between Route Points and Default Handover Settings



A handover can take place for any of the following reasons:

- A Route Point triggers a handover to cellular as the user exits the building.
- A Route Point triggers a handover to Wi-Fi when the user enters the building.
- When the value specified in the Min Cellular to Wi-Fi Roam RSSI field is a match and the Route Point is missed or not available, a handover to Wi-Fi occurs.
- When the value specified in the Min Wi-Fi to Cellular Roam RSSI field is a match and the Route Point is missed or not available, a handover to cellular occurs.

Using WLAN Controllers to Retrieve Location Information

Currently, the mobility solution supports integration of enterprise location information for WLAN controllers from the following vendors:

- Aruba Networks
- Cisco Systems
- Meru Networks

By default, when you integrate a WLAN controller with the Mobility Router, it sends SNMP queries to the WLAN controller for information.

Optionally, you can configure the Mobility Router to receive SNMP trap information about transmit power from the WLAN controller. If you choose to do this, you need to define the Mobility Router as a trap receiver on the WLAN controller.

Optionally, if you have enterprise location information configured for any of these WLAN controllers, you can enable the integration of this information with the Mobility Router. When you integrate location information, the Mobility Router gets the following information from the WLAN controller:

- Basic service set identifier (BSSID) list
- Service set identifier (SSID) list
- Location information (for example, campus, building, floor, and so on) (not supported for Cisco controllers)

Transmit power (not supported for Meru controllers)

Note

If you have location information configured for your controller, we recommend that you synchronize this information with the Mobility Router.

The Mobility Router uses the WLAN controller information in conjunction with fingerprints that you create, and location information received from mobile devices as users roam within the enterprise to maintain and update location information.

How the Mobility Router Dynamically Learns Location Information from the Connect Platform

The Mobility Router learns location information from the Connect Platform on the mobile devices as users roam from known access points to unknown access points.

If the Connect Platform does not know an access point, the Connect Platform sends a location query to the Mobility Router with the following data:

- Wi-Fi information—MAC address, IP address, BSSID, and SSID
- GSM information—Cellular ID, LAC, MNC, and MCC

The Mobility Router compares this information with its known access point list and adds the access point as a known access point. The Mobility Router also sends fingerprints, a list of known cellular networks, and a list of known access points to the Connect Platform.

If the Connect Platform finds that its list of known access points are missing fingerprints, the Connect Platform sends the BSSID to the Mobility Router. The Mobility Router sends the Connect Platform fingerprints.

If the Connect Platform already has location and access point information from what the Mobility Router previously has sent, the Connect Platform sends a movement update to the Mobility Router. The Mobility Router uses this information to keep track of the mobile device and does not send any information to the Connect Platform.

Mobility Configuration Task List

Depending on your wireless network, the tasks that you complete to establish mobility settings can differ.

The major steps in establishing mobility settings are:

1. Establish the enterprise location.
   - If your WLAN controller supports and you have configured location information, you can integrate the controller with the Mobility Router.
   - You can also manually create the enterprise location:
     - Define the campus.
     - Associate buildings with the campus.
     - Specify floors for each building.
2. Specify Route Points as needed for the enterprise location.
3. Take calibration measurements at each Route Point

Note

If you have Meru access points and have enabled Virtual Cell, you cannot take fingerprints for these access points. This is because fingerprinting is based on a BSSID for an access point. Because Virtual Cell uses one BSSID for all access points, fingerprinting is not possible.

CHAPTER

10

Managing IP-PBX Integration

The Mobility Router communicates with an enterprise IP-PBX over line-side and trunk-side interfaces.

The Mobility Router uses the line-side interface to register all Connect Platform to the respective IP-PBXs. This allows the Mobility Router to send and receive calls to and from the Connect Platform using the line-side interface. The Mobility Router uses the trunk-side interface to send and receive calls from the Connect Platform when the devices are in the cellular network.

If the line-side interface is not enabled, the trunk-side interface is used to send and receive calls to and from the Connect Platform.

This chapter contains the following sections:

Adding an IP-PBX

Add an IP-PBX on the Mobility Router for each enterprise IP-PBX with which the Mobility Router communicates.

Configuring IP-PBX General Settings

To configure IP-PBX general settings:

1. Click **Configuration > Voice > IP-PBXs**.
2. Click **Add** to view the **General** page.
3. In the **Name** field, type the name for the IP-PBX. The name can be up to 50 alphanumeric characters long and cannot contain special characters except for spaces, hyphens (-), and underscores (_).
4. In the **Type** list, select the IP-PBX type from the list of supported PBXs.
5. To enable the use of registration on the IP-PBX, select the **Line-Side Support** check box. By default, this option is selected. To disable line-side support, clear the **Line-Side Support** check box. Disable this option only if the IP-PBX does not support Line Side Interface. If you disable this option, go to Step Configuring SIP Trunk Settings on page 99.
   a. In the **FQDN or IP Address** field, type the fully qualified domain name (FQDN) or IP address of the IP-PBX.
   b. In the **Port** field, type the port number of the SIP listening port on the IP-PBX that the Mobility Router uses for access. The port number can be between 1024 through 49151, and the default value is 5060.
   c. In the **SIP Transport** list, select the protocol used for SIP transport:
      - UDP
      - TCP
      - TLS

      If you select TLS as the protocol for SIP transport, do the following:

      1. Click **Import** next to the **Certificate** field.
      2. **Enter the SRTP Certificate ID**.
      3. Enter the hq_ca.crt in the HQ CA Root Certificate area (hq_ca.crt is stored in C:\Shoreline Data\keystore\certs).
      4. Enter the SRTP TLS Certificate in the SRTP TLS Certificate area (SRTP TLS Certificate is stored in C:\Shoreline Data\keystore\certs).
      5. Enter the SRTP TLS Private Key in the SRTP TLS Private Key area (SRTP TLS Private Key is stored in (C:\Shoreline Data\keystore\private).
      6. Click **Import**.

d. In the **SIP Domain Name** field, enter a domain name of the appropriate/logical group for this PBX, for example marketing.Mitel.com. Refer to your PBX Configuration Guide for more information.

e. In the **Keep Alive Time** field, type the interval at which the Mobility Router sends registration keepalive messages to the PBX.

f. Select the **Mitel Connect Features** check box to enable Connect features. Click **Add Mitel Directory Server** link. The **Add Mitel Directory Server** page opens. For information about how to add a Directory Server, see Directory Authentication on page 78.

6. Click **Next** to configure SIP Trunk parameters.

Configuring SIP Trunk Settings

To configure SIP trunk settings:

1. In the **Name** field, type the name of the trunk. By default, a name is provided. It is the name you specified on the General tab, with -trunk appended to the name. The name can be up to 50 alphanumeric characters and can contain spaces, hyphens (-), and underscores (-).

2. In the **Description** field, type a description for the trunk. By default, a name is provided. It is based on the name that you specified on the General tab, with trunk appended to the name.

3. In the **Local SIP End Points** area:

   a. Verify the value of the eth0 **Interface**, as shown on the Interfaces page. This IP address is also entered as the destination IP address when you configure the SIP trunk on the IP-PBX.

   b. Select **Use Alternate IP Address** if your network topology requires you to use a different IP address for the trunk connection than the interface default address. For most deployments, this is left cleared.

   c. In the **Port** field, type the port number of the trunk-side port on the Mobility Router. Use the same port number as the destination port in the IP-PBX SIP trunk configuration. The default is 5068.

   d. In the **SIP Domain Name** field, type the appropriate local domain name.

4. In the **Remote SIP End Point** area:

   a. In the FQDN or IP Address field, type the fully qualified domain name (FQDN) or IP Address of the primary SIP trunk switch.

   b. In the FQDN or IP Address Alternative field, type the IP Address of the secondary or alternative SIP trunk switch. When the capacity on the primary SIP trunk is reached, Mobility Router receives an error message “503 service not available” and tries the alternative or secondary SIP trunk for this call. If primary SIP trunk is down or Mobility Router receives a 503- e r r o r message for any new call, Mobility Router switches to the secondary or alternative SIP trunk. If both SIP trunks are down and the secondary SIP trunk reaches at full capacity for any new call, call fails. All the existing calls continues to utilize their respective trunks.

5. In the **Port** field, type the remote port number of the IP-PBX. This is the trunk-side port on the IP-PBX. The port number needs to match with the corresponding SIP listening port on your IP-PBX. The default value of this field is 5068.
6. In the **Transport** list, select UDP or TCP. The Mobility Router accepts either UDP or TCP transport on a SIP trunk, but it initiates the session using the transport protocol that you select here. The default value is UDP.
7. In the **SIP Domain Name** field, type the appropriate remote domain name.
8. Select a **Security** type. Select **None** or **Digest**. The digest user value must match the owner user ID and password.

Note

The Cisco Call Manager does not allow same port to be entered for both the line-side and trunk-side interfaces.

9. Click **Next**. The **Numbering Plan** tab displays.

Configuring Numbering Plan Settings

A numbering plan allocates telephone number ranges to countries, regions, areas, and exchanges. A numbering plan can also allocate telephone numbers to mobile device networks.

A closed numbering plan uses area codes and local phone numbers of fixed lengths (for example, the United States uses a closed numbering plan). An open numbering plan uses area codes and local phone numbers of varying lengths (for example, Australia uses an open numbering plan). The Mobility Router supports closed and open numbering plans and provides predefined numbering plan templates for various countries. Using a template as a base, you can customize a numbering plan to accommodate your network. In addition, the Connect Platform uses numbering plan tables to identify special service numbers (emergency and network numbers) and enterprise extensions.

- Numbering plan parameters—Define traditional dial plan settings, such as area codes, country codes, access codes, and combinations of digits that are dialed. Each numbering plan template defines default numbering plan parameters, based on the country for the template. You can modify the default numbering plan parameters and also add new parameters to accommodate your network. Refer to Numbering Plan Parameter Sets on page 102.
- Numbering plan tables—Lists of patterns that the Mobility Router uses to identify whether a mobile device is dialing an access number, formats caller ID numbers sent to the Connect Platform, and constructs phone numbers for outgoing calls from the Connect Platform. Refer to Adding an Individual Parameter (Column) on page 104.

On the Mobility Router, the Numbering Plan tab for an IP-PBX consists of two pages: **Basic** and **Advanced**.

You can apply one of the predefined numbering plans to the IP-PBX to start over with a set of default numbering plan values. If the country in which the Mobility Router changes, you can apply a template for the new country to the IP-PBX. After you apply a numbering plan template to an IP-PBX, any

changes that you made to the previous numbering plan are lost, and the numbering plan uses the default settings from the template until you modify the numbering plan. Use this mode to add or modify the following:

- Anonymous Caller ID (ACI)—Phone number the Mobility Router uses as the caller ID when it forwards an anonymous call to the mobile device when it is on the cellular network. The anonymous caller ID must be a valid PSTN number and match the route pattern of the SIP trunk configured on the IP-PBX. This ensures that the Connect Platform can receive this caller ID when the mobile device is on the cellular network. The anonymous caller ID can include digits and plus signs (+). For example, if you specify +16505555555 as the anonymous caller ID parameter, the Mobility Router sends the number as the caller ID of the call. The Connect Platform interprets the number as the anonymous number and displays “unnamed” on the mobile device.

- International Access Code (IAC)—The number that is prepended to phone numbers when end users place calls to phone numbers outside of the country in which the Mobility Router is located. A default value for the IAC is applied to a numbering plan when it is first added. Verify that the IAC value is correct for the country in which the Mobility Router is located. Modify the IAC value if necessary. The default value depends on the numbering plan template that you chose when you added the IP-PBX. For example, the default value for the North America template is 011, and the default value for the United Kingdom template is 00.

- Local Country Code (LCC)—Country code of the country in which the Mobility Router is located. A default value for the local country code (LCC) is applied to a numbering plan when it is first added. Verify that the LCC value is correct for the country in which the Mobility Router is located. Modify the LCC value if necessary. The default value depends on the numbering plan template that you chose when you added the IP-PBX. For example, the default value for the North America template is 1, and the default value for the United Kingdom template is 44.

- National Number Code (NNC)—Number that is prepended to phone numbers when end users place calls to phone numbers within the country and outside of the area code in which the Mobility Router is located. A default value for the national number code (NNC) is applied to a numbering plan when it is first added. Verify that the NNC value is correct for country in which the Mobility Router is located. Modify the NNC value if necessary. Type the number that is prepended to phone numbers when end users place calls to phone numbers within the country and outside the area code in which the Mobility Router is located. The default value depends on the numbering plan template that you chose when you added the IP-PBX. For example, the value for the North America template is 1, and the value for the United Kingdom template is 0.

Refer to Numbering Plan Parameter Sets on page 102 for details on numbering plan sets.

Refer to Numbering Plan Table Patterns on page 105 for details on numbering plan table patterns.

Each pattern consists of a combination of pattern elements. Each numbering plan table consists of entries of patterns which you can modify. You can create new entries for the numbering plan tables as well. The default patterns in the entries for each numbering plan table differ, depending on the country of the numbering plan template. This page allows you to Apply, Reset, and Reload a Numbering Plan template, manage numbering plan pattern tables, and use the test panel to verify the numbering plan tables. Use this mode to add or modify:

- Enterprise Country Code (ECC) — (“North America Generic” selection only)

- Enterprise extension pattern (EEP)—Pattern that defines a range of extensions within the enterprise. For example, if you chose the United Kingdom numbering plan template when adding an IP-PBX, the default value for the EEP is XXXX. This pattern defines any four-digit number as an

enterprise extension. If the range of extensions in your enterprise is 6000 through 6999, you can modify the EEP to 6XXX. This pattern identifies any four-digit number starting with 6 as an enterprise extension. If your enterprise extensions are four-digit numbers, you would need to modify the EEP to accommodate your extensions. For example, any four-digit number starting with 70, 71, or 73 as an enterprise extension should be written as 7[013]XX.

- Enterprise Full Number Patter (EFP) — ("North America Generic" selection only - includes LAC and LEC).
- Local area code (LAC)—Area code in which the Mobility Router is located. LAC is not defined in some numbering plan templates (for example, France). A default value for the local area code (LAC) is applied to a numbering plan when it is first added. You must modify the LAC so that it is valid for your enterprise. For example, if you chose the North America numbering plan template when adding an IP-PBX, the default LAC value is 408. If the area code for the region in which the Mobility Router is located, change the LAC value to the appropriate area code. In some countries, the local area code might also be known as city or dialing code.
- Local exchange code (LEC)— The local exchange code (LEC) is the prefix that is prepended to the enterprise extension pattern (EEP) to form a valid phone number. For example, for the phone number 9198000, the LEC is 919. A default value for the LEC is applied to a numbering plan when it is first added. Verify that the LEC value is correct for the area in which the Mobility Router is located. Modify the LEC value if necessary.
- Land Line Numbers (LLN) — ("North America Generic" selection only) Includes NPA and NPL.
- Mobile GSM Numbers (MGN) — ("North America Generic" selection only) Includes NPA and NPL.
- Numbering Plan Area Code (NPA)—First set of 3 digits, combined with the NPL (seven digits), that directs telephone calls to region. For example, in the North American template, the NPA first digit must not include a 0 or 1 as this causes confusion with directing a call outside the country. The second digit must not include a 9. For example, 212 is valid, however 121 is not. Some numbering plan templates may not use this value, such as UK.
- Numbering Plan Local Number (NPL)—Second set of seven digits, combined with the NPA (three digits) that directs telephone calls to a region. For example, in the North American template, the NPL first digit must not include a 0 or 1 as this causes confusion with directing a call outside the country. For example, 2345678 is a valid telephone number, however 1234567 is not. Some numbering plan templates may not use this value, such as UK.
- Outside line access code (OLC)—Number that is prepended to phone numbers when end users place calls to phone numbers outside of the enterprise. This is also known as trunk access code. The default value for the OLC is 9. Modify this value if is not the number that your enterprise uses to place calls outside of the enterprise.

Numbering Plan Parameter Sets

A parameter set consists of all parameters needed to complete the numbering plan, for example LEC+LAC+EEP. You may also define additional sets of parameters for the existing numbering plan.

Adding a Numbering Plan Parameter Set (Row)

To add a new row of a numbering plan parameter set:

1. On the Mobility Router, click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX to which you want to add a numbering plan.
3. On the **Basic** screen, click the **Add** button. This function may also be performed on the Advanced page.
4. The **Add Parameter Set** page displays.

Tip

To use a shortcut to add a row in this table, select an existing row and right click. Select Duplicate Row. Modify the new row as needed.

5. The following are format examples.
   - EEP Format: X[XXXX]XX
   - LAC Format: XXX (area code)
   - LEC Format: XXX (exchange code)
   - NPA Format: [2-9][0-8]X
   - NPL Format: [2-9]XXXXXX
   - OLC Format: X (outside line)
6. To save your changes, click **Apply**. The table is populated with the new information.

Note

Expand or reduce the number of visible Numbering Plan Parameters Sets on the Advanced page.

Duplicating a Row

You can modify a numbering plan parameter set on the Basic or Advanced page. To modify a numbering plan parameter:

1. On the Mobility Router, click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX to which you want to modify a numbering plan.

Modifying a Numbering Plan Parameter Set (Row)

You can modify a numbering plan parameter set on the Basic or Advanced page. To modify a numbering plan parameter:

1. On the Mobility Router, click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX to which you want to modify a numbering plan.

3. On the Basic screen, click the **Modify** button. This function may also be performed on the **Advanced** page.
4. The Modify Parameter Set page displays.
5. Modify the appropriate parameters and click Apply to save changes. The table is populated with the new information.

Deleting a Numbering Plan Parameter Set (Row)

You can delete a numbering plan parameter set from the **Basic** or **Advanced** page. The default numbering plan set cannot be deleted (note the **Delete** option is unavailable for this parameter set).

To delete a numbering plan parameter:

1. On the Mobility Router, click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX of which you want to delete a numbering plan, then select the Numbering Plan tab.
3. On the **Basic** screen, click the **Delete** button. A prompt asking to confirm the deletion displays. This function may also be performed on the **Advanced** page.
4. Click **OK** to delete the parameter set or **Cancel** to return to the Numbering Plan page without saving changes.

Adding an Individual Parameter (Column)

You can augment a Numbering Plan set by adding a column of customized parameters. To add a Numbering Plan Column:

1. On the Mobility Router, click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX of which you want to delete a numbering plan, then select the **Numbering Plan** tab. A Cisco Call Manager is used in this example.
3. Select the **Advanced** page.
4. Click **Add Column**.
5. The **Add Column** popup displays.
6. Enter a **Description** for the numbering plan.
7. Enter a **Key**. The key is three-letter code that is used to identify the numbering plan parameter when constructing numbering plan table patterns. You cannot change any keys, and the value entered must not be already used in other parameters (IAC, NNC, and so on.).
8. Enter a **Default Value**. Depending on the parameter, the literal value or pattern used by the Mobility Router and the Connect Platform.
9. Click **Apply** to continue or **Cancel** to return to the Numbering Plan window without saving changes. If applied, the new column is added in alphabetical order.

Deleting an Individual Parameter (Column)

To delete a Numbering Plan Column:

1. On the Mobility Router, click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX of which you want to delete a numbering plan, then select the **Numbering Plan** tab. A Cisco Call Manager is used in this example.
3. Select the **Advanced** page.
4. Click **Delete** Column.
5. Select the column you want to delete from the dropdown window. Click **Apply** to continue or **Cancel** to return to the Numbering Plan window without saving changes.

Numbering Plan Table Patterns

Numbering plan tables consist of entries that are composed of patterns.

Each numbering plan template consists of the numbering plan tables that the Mobility Router and the Connect Platform use for caller ID, dialing calls, and identification of different types of calls.

Overview of Numbering Plan Table Patterns

Numbering Plan Table Patterns are added, modified or deleted using the Advanced page of the Numbering Plan tab. To access the patterns:

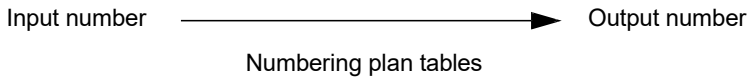
1. Click **Configuration > Voice > IP-PBXs**.
2. Double-click the IP-PBX of which you want to add, modify or delete a pattern. Select the **Numbering Plan** tab and click **Advanced**.
3. Locate the **Numbering Plan Table** at the bottom of the page.
4. The numbering plan tables map input numbers to output numbers:

For detailed information about each Numbering Plan Table menu item, refer to Overview of Numbering Plan Table Patterns on page 105.

This pattern is constructed by combining numbering plan parameters. In this case, the pattern consists of a plus sign preceding the local country code (LCC), local area code (LAC), local exchange code (LEC), and enterprise extension pattern (EEP). Using the default values for the numbering plan parameters from the North American numbering template, the pattern expands to +14089198XXX. Any numbers starting with +1408919 and ending with 4 digits that start with 8 would match this pattern (for example, +14089198000).

When the Mobility Router receives a dialed number from the Connect Platform (for example, a local extension or phone number), the number is matched against the Outgoing Called Number Mapping table patterns.

The following figure shows how a number that the Mobility Router receives is mapped to an appropriate output number.



Showing Values and Keys of Numbering Plan Parameters

By default, if numbering plan parameter keys are used in patterns, the keys are shown in the patterns. For example, the default pattern for the Enterprise Extension Pattern table, which has a default value of 8XXX. To see the value of the (EEP) key in the pattern, you can use the Show Values/Show Keys button. The pattern then uses 8XXX in the pattern rather than (EEP).

To review numbering plan table patterns as values:

1. Click **Configuration > Voice > IP-PBXs**.
2. Click the **Numbering Plan** tab.
3. Select **Advanced**.
4. In the **Table** list, select the numbering plan table pattern that you want to review.
5. Click **Show Values**. The values of the patterns are listed.
6. To switch back to reviewing patterns as parameter keys, click **Show Keys**.

The following lists the “Key” entries for the VoIP Caller ID Mapping table:

Table 5: Key Number Mapping Example

Original Caller ID	Caller ID for RA Client
(EEP)	(LAC)(LEC)(EEP)
(NPL)	(LAC)(NPL)
(IAC)(LCC)(NPA)(NPL)	(NPA)(NPL)
+(LCC)(NPA)(NPL)	(NPA)(NPL)
+*	(IAC)*

The following lists the “Values” entries for the VoIP Caller ID Mapping table:

Table 6: Values Number mapping example

Original Caller ID	Caller ID for RA Client
8[0138]XX	4089198[0138]XX
[2-9]XXXXXX	408[2-9]XXXXXX
0111[2-9][0-8]X[2-9]XXXXXX	[2-9][0-8]X[2-9]XXXXXX
+1[2-9][0-8]X[2-9]XXXXXX	[2-9][0-8]X[2-9]XXXXXX
+*	011*

If the Mobility Router receives a caller ID from a calling party of 9198000, the number is matched against patterns of the entries of the VoIP Caller ID Mapping table. The patterns that match the number are assigned weights, based on how well the number matches the pattern. In this case, 9198000 matches the pattern [2-9]XXXXXX. The output number is defined to show the local area code preceding the phone number. The output number is 4089198000.

Table 7 lists the allowed pattern elements that you can use when configuring numbering plan parameters and numbering plan tables.

Table 7: Allowed Pattern Elements for Numbering Plan Parameters and Numbering Plan Tables

Valid and Active States	Description
digit	Actual digit (for example, 5)
X	Specifies a single digit in the range 0 through 9 or +. For example, if you type 408555120X, the pattern matches all phone numbers starting with 4085551200, up to 4085551209.
+	Plus sign.
[*list*]	Specifies a single digit within *list*, where *list* is one or more digits. For example, if you type 408555120[123], the pattern matches the following phone numbers: 4085551201, 4085551202, 4085551203.
[*digit1*–*digit2*]	Specifies a single digit in a range from *digit1* through *digit2*. For example, if you type 408555120[0–7], the pattern matches *only* the following phone numbers: 4085551200, 4085551201, 4085551202, 4085551203, 4085551204, 4085551205, 4085551206, and 4085551207.
[**list*]	Specifies zero or more digits from the list. For example, if you type 408555[*123]444, the following are some of the numbers for which the calling rule is applied: 4085551444, 4085552444.
[**digit1*–*digit2*]	Specifies zero or more digits in a range from *digit1* through *digit2*. For example, if you type 408555120[*0–7], the following are some of the number for which the calling rule is applied: 4085551201, and 4085551202, 4085551203.
*	Specifies zero or more of any digits. Pattern cannot have “*” as its only element. To match any number, use “X*” as a pattern. For example, if you type 408555*123*, the pattern matches phone numbers that start with 408555 and include the pattern 123.

Table 7: Allowed Pattern Elements for Numbering Plan Parameters and Numbering Plan Tables

Valid and Active States	Description
U	Specifies a special pattern—Type U to apply if the caller ID is unknown.
(*key*)	Numbering plan parameter key, which is a three-letter code and surrounded by parentheses, used in numbering plan table patterns. When specifying a numbering plan parameter key in a numbering plan pattern table, make sure to include parentheses. Specifying only the three-letter code is not valid. Only use parentheses in conjunction with a key; parentheses used in any other context are not valid in a pattern. The default numbering plan parameter keys are as follows: ■ EEP—Enterprise extension pattern ■ LAC—Local area code ■ LEC—Local exchange code ■ NPA—Numbering plan area code ■ NPL—Numbering plan local ■ OLC—Outside line access code For example, to include the national number code parameter in a numbering plan table pattern, specify (NNC) as part of the pattern. Note the special bracket type for this parameter is ( ). In addition to the default numbering plan parameter keys listed above, the following built-in variables are automatically expanded with the appropriate value at run-time: ■ EEN - User's Enterprise Extension Number ■ EFN - User's Enterprise Full Number ■ CNM - User's Cellular Number Built-in variables are enclosed in curly braces "{}". For example, {EEN} expands to the Enterprise Extension Number of the user in call.

Numbering Plan Tables

The following sections discuss each table. Refer to Table 7 for a description of how to configure each table:

Access Call Number Mapping

The Access Call Number Mapping table defines the rules to modify both the incoming called number and caller ID for any call received on a trunk line to a standard normalized format. If the mobile device is on a cellular network when a user places a call, the Connect Platform dials the cellular access number to communicate with the Mobility Router. The cellular access number should be configured as a valid PSTN number.

Because the access number dialed on an incoming access call might not exactly match the format of the cellular access number configured on the Mobility Router, access call number patterns are used to normalize called and calling numbers on the incoming access calls. The Mobility Router also normalizes the configured access numbers as well as the cellular phone numbers. Comparing these normalized numbers, mobility can determine whether the incoming call is an access call and whether the calling party is a known mobile device on the cellular network.

For example, if the cellular access number is configured to +14089198000 and the called number on an incoming access call is 8000, the incoming number is mapped to +14089198000 so that it matches the format of the cellular access number.

Access Call Number Mapping:

- Incoming Number — the pattern for the possible phone numbers that the Mobility Router receives when communicating with the Connect Platform.
- Normalized Number — the pattern that maps the incoming number to the normalized format for cellular access number and device cell number.

VoIP Caller ID Mapping

The Mobility Router formats the caller ID for VoIP calls so that the Connect Platform can display the appropriate name and number for incoming calls. VoIP caller ID patterns are used to map the caller ID sent to the Mobility Router from the calling party to the caller ID that is sent to the Connect Platform and shown on the mobile device.

For example, if the caller ID sent to the Mobility Router is 4545, that number gets mapped to 4085554545. This mapped number is sent to the Connect Platform, and this is the caller ID that the user sees on the mobile device.

VoIP Caller ID mapping:

- Original Caller ID — the pattern for the caller ID sent to the Mobility Router from the calling party.
- Caller ID for RA Client — the pattern for the caller ID information sent to the Connect Platform for VoIP calls.

Cellular Caller ID Mapping

The Mobility Router changes the caller ID format of calls routed to the Connect Platform while connected to the cellular network for the following reasons:

- Caller ID is not blocked by public switched telephone networks (PSTNs) or public land mobile networks (PLMNs).
- Connect Platform can recognize anchored calls.
- Connect Platform can display the appropriate name and number for incoming calls. For

example, if the caller ID sent to the Mobility Router is 4545, that number gets mapped to 4085554545. This mapped number is sent to the Connect Platform, and this is the caller ID that the user sees on the mobile device.

For an anonymous incoming call, the Mobility Router sends the anonymous caller ID (ACI) numbering plan parameter to the Connect Platform. The Connect Platform recognizes the ACI and presents the call as an anonymous call.

- Original Caller ID — the pattern for the caller ID sent to the Mobility Router from the calling party.
- Cellular Caller ID for RA Client — the pattern for the caller Client ID information sent to the Connect Platform for cellular calls. If “Use Numbering Plan Enterprise Full Number Pattern Table” is selected for Enterprise Cellular Call Indicator in the PBX Options, you must configure this table to ensure the outgoing cellular caller ID for RA Client matches an entry in the Enterprise Full Number Pattern Table.

Outgoing Called Number Mapping

The Mobility Router uses outgoing called number patterns to format phone numbers of outgoing calls so that calls are efficiently routed to the intended destinations. Outgoing called number patterns are also used when calling Mobility users when their mobile devices are on the cellular network.

For example, if a user dials 4085554242, the Mobility Router adds the outside line access code (OLC) and national number code (NNC) to the phone number (914085554242) so that the enterprise PBX can place the call.

If a user dials 14085551234, and the number is identified as an enterprise full normalized number and the last four digits make an enterprise extension, the Mobility Router dials 1234 so that the routing of the call is more efficient.

- Original Called Number — the pattern for the phone number originally dialed.
- Converted Called Number — the pattern for the mapped phone number that is used to place the call.

Emergency Number Pattern

Patterns in this table identify emergency numbers (for example, 911). By default, country-specific main emergency number patterns are automatically added to this table. Add additional patterns or modify existing pattern to accurately identify all emergency numbers in your country. Phone numbers covered by patterns in this table are dialed directly over cellular network when there is cellular coverage. Depending on the configuration of Emergency Call Routing in **Configuration > Groups and Users > Groups > Options**, emergency numbers might optionally be routed over Wi-Fi network. See Emergency Call Routing on page 151 for more information. It is the responsibility of the Administrator of the system to ensure the proper emergency number(s) configuration in this table to ensure calls are routed to the correct destination. Mitel is not liable for any resulting error or delay due to misconfiguration of this table.

- Pattern — the pattern for special service numbers.

Cellular Direct Number Pattern

Patterns in this table specify numbers to be routed directly over cellular network and should include cellular networks special service numbers such as 411 and 511. Add other patterns that are to be routed directly over the cellular networks.

- Pattern — the pattern for special service numbers.

Enterprise Extension Pattern

The Dynamic Anchoring feature on the Mobility Router provides a mechanism to only route calls through the enterprise if an enterprise extension is dialed. If configuring outgoing calls to enterprise extensions while on the cellular network, the Connect Platform must know whether an outgoing call placed by a user is an enterprise extension.

- Pattern — the pattern for enterprise extension.

Enterprise Full Number Pattern

The Enterprise Full Number Pattern Table is used if the selection for Enterprise Cellular Call Indicator for the PBX is “Use Numbering Plan Enterprise Full Number Pattern Table”. This table should cover all the phone numbers your enterprise can send as caller ID on outgoing PSTN calls.

- Pattern — the pattern for full enterprise number. You can add multiple entries to the table.

Note

The parameters *(LAC)(LEC)(EEP) are listed in this table by default, and cover most of your enterprise numbers. Add these parameters to the table if they are not displayed (this may be the case if you have upgraded your Mobility Router from version 3.1 or older).

Adding Numbering Plan Table Patterns

For any of the numbering plan tables, you can add new patterns to accommodate your requirements. Adding an extremely large number of new patterns (more than 1,000) might slow Mobility Router performance. To test new numbering plan table patterns, you can use the test panel to verify patterns. For more information, see Using the Test Panel on page 113.

To add a numbering plan table pattern:

1. Click **Configuration > Voice > IP-PBXs**.
2. Select the IP-PBX to which you want to apply a numbering plan template and click **Modify**.
3. Click the **Numbering Plan** tab and select **Advanced**.
4. In the **Table** list, select the numbering plan table to which you want to add a pattern.
5. Click the **Add** button for the numbering plan tables. The **Add Table Entry** page displays.
6. Fill in the fields for the **Add Table Entry** page. The fields available depend on the numbering plan table that you selected. For more information, see Overview of Numbering Plan Table Patterns on page 105.
7. To save your changes, click **Apply**.

Changing the Order of Patterns for a Numbering Plan Table

When an extension or phone number is compared to numbering plan table patterns, the pattern that best matches the number is used. If there are two patterns that match with the same weight, the first pattern in the pattern list is used. You can move patterns up and down in the pattern list for a numbering plan table.

To move a pattern up or down in the pattern list:

1. Click **Configuration > Voice > IP-PBXs**.
2. Click the **Numbering Plan** tab.
3. Select **Advanced**.
4. In the **Table** list, select the numbering plan table pattern that you want to move.
5. Do one of the following:
   - To move the pattern up in the list, click **Up**.
   - To move the pattern down in the list, click **Down**.

Modifying Numbering Plan Table Patterns

For any of the numbering plan tables, you can modify patterns to accommodate your requirements.

Note

When on the Show Value page, Numbering Plan Table Patterns cannot be modified.

To modify a numbering plan table pattern:

1. Click **Configuration > Voice > IP-PBXs**.
2. Click the **Modify** button for the numbering plan tables. The **Modify Table Entry** page displays. The fields available depend on the numbering plan table that you selected. For more information, see Overview of Numbering Plan Table Patterns on page 105.
3. To save your changes, click **Apply**.

Deleting Numbering Plan Table Patterns

To delete a numbering plan table pattern:

1. Click **Configuration > Voice > IP-PBXs**.
2. Click the **Numbering Plan** tab.
3. Select **Advanced**.
4. In the **Table** list, select the numbering plan table pattern that you want to delete.
5. When prompted to delete the table entries, click **OK**.

Using the Test Panel

You can test new or existing numbering plan pattern tables with the test panel to see which pattern a phone extension or number matches. After creating or modifying a pattern for a numbering plan table, you can verify that the pattern works correctly by providing an input number, which gets matched against the list of patterns to map to the output number that the Mobility Router uses.

When an extension or phone number is compared to numbering plan table patterns, the pattern that best matches the number is used. In the test panel, the patterns that best match the input number are assigned weights. The pattern with the highest weight is the best match that is used to map the input number. If there are two patterns that match with the same weight, the first pattern in the pattern list is used.

In the following example, an input number of 8000 is specified for the default Outgoing Called Numbers numbering plan table patterns from the North American numbering plan template. The input number matched three patterns, and the pattern with the highest weight of 1 is used for mapping.

To use the test panel:

1. Click **Configuration > Voice > IP-PBXs**.
2. Select the IP-PBX numbering plan table you want to test and click Modify.
3. Click the **Numbering Plan** tab and select **Advanced**.
4. Select the **Test** check box. The test panel displays.
5. Type the desired User ID into the **User ID** field.
6. In the **Table** list, select the numbering plan table pattern you want to test.
7. In the **Input Number** field, type an extension or phone number that will match a pattern that you created or an existing pattern to produce a mapped number.
8. Click **Test**.

The input number is mapped to the output number, which displays in the Output Number field. The Details box lists the patterns available for the numbering plan table and which pattern was used to map the input number.

Configuring Media Settings

Use the **Media** tab to configure RTP media related settings:

- Select **Inband DTMF Detection** to enable the inband DTMF detection on the Mobility Router. The preferred setting is disabled as the DTMF detection is typically performed on the PBX or Gateway. However, if your PBX or gateway does not support RFC 2833 based DTMF relay, enable this option.
- Select **Ringback Detection** to enable ringback tone detection. Some PBXs (for example, Mitel) connect a call immediately and provide in-band tones for call progress indication. Select this option if your PBX is set up to answer a call immediately.
- Select **Initial Invite requires SDP** for PBXs which require SDP to be sent in the Initial Invite request message. If this option is selected, the Mobility Router always includes SDP when it sends the initial invite request to the PBX. In some cases, that might require bridging RTP media through the Mobility Router. If this option is not selected, the SDP is included in the initial invite only if it is available at the invite time, otherwise it will be included in the ACK message.
- Select **Re-Invite requires SDP** for PBXs which require SDP to be sent in the re-invite request message. If this option is selected, the Mobility Router always includes SDP when it sends re-invite request to the PBX. In some cases, that might require bridging RTP media bridging through the Mobility Router. If this option is not selected, SDP is included in the re-invite only if it is available when the Mobility Router generates re-invite message, otherwise the SDP will be included in the ACK message.
- In the **Default Payload (RFC 2833)** field, type a value from 96 through 127. The default value is 101.

- Select the **Voice Prompt Profile Name** as created in **Configuration > Voice > Advanced > Voice Prompt Profiles**. All users configured on this PBX will hear these prompts on their clients/ devices. The default profile type is default, which consists of factory default settings/prompts.
- **Voice Activity Detection (VAD)**, also known as speech activity detection, enables speech processing when the presence or absence of human speech is detected. The main uses of VAD are in speech coding and speech recognition. The VAD can avoid unnecessary coding/ transmission of silence packets, thus saving on computation and network bandwidth.

Note

VAD is disabled when using IP-PBX configuration.

- Select **Force RTP Bridging through the Mitel Connect Mobility Router** to bridge RTP media streams through the Mobility Router. This option is disabled by default.

Note

Bridging media through the Mobility Router increases the CPU and network load on the Mobility Router and reduces scalability.

Note

This option may be used in combination with Mobility Router Transcoding. See below in Mobility Router Transcoding for more information about these Media Operation Modes, and how the Mobility Router's performance may be affected by the various combinations of these Modes.

WARNING!

For IP-PBX releases 11.x and older, confirm that **Force RTP Bridging** is disabled (not selected); In this release, this is enabled(selected) by default.

- Check **Mitel Connect Mobility Router Transcoding** if transcoding between codecs is necessary in the network. This option is enabled by default for IP-PBXs. Used in combination with **Force RTP Bridging** (see above for more information about this option), the following Media Operation Modes occur:
  - RTP Bridging Off/Transcoding On (Default for IP-PBXs): Disable **Force RTP Bridging through the Mitel Connect Mobility Router** and enable **Mitel Connect Mobility Router Transcoding** to place the Mobility Router in the media path for the first few seconds of the call. During this initial period, the Mobility Router assesses if it needs to continue to stay in the media path or if it can "jump out" based on Codec agreement on both sides. If there is no shared common Codec on both sides, the Mobility Router re-enters the media path and provides the necessary transcoding.
  - RTP Bridging On/Transcoding On: always Enable both Force RTP Bridging through the Mitel Connect Mobility Router and Mitel Connect Mobility Router Transcoding to place the Mobility Router in the media path and perform media transcoding if necessary. In this mode, the Mobility Router replaces the incoming Session Description Protocol (SDP) with the Mobility Router's SDP. The list of Mobility Router-supported Codecs is forwarded to other side and is reordered according to incoming SDP Codec list. Codecs that are not present in the incoming SDP but enabled on the Mobility Router (Refer to step n) are inserted at end of

the list. This mode allows the Mobility Router to be interoperate with the most PBXs, but it could significantly increase the Mobility Router's resource (CPU, networking and memory) requirement.

- RTP Bridging On/Transcoding Off: Enable **Force RTP Bridging through the Mitel Connect Mobility Router** and disable **Mitel Connect Mobility Router Transcoding** to place with Mobility Router in the media path without transcoding. In this mode, the Mobility Router replaces the incoming Session Description Protocol (SDP) with the Mobility Router's SDP. The list of Codecs that is forwarded to other side is limited and in the same order as in incoming SDP. Additionally, Codecs which are not supported by the Mobility Router are excluded from the list. RTP packets flow through Mobility Router, but no transcoding is performed.
- RTP Bridging Off/Transcoding Off: Disable both **Force RTP Bridging through the Mitel Connect Mobility Router** and **Mitel Connect Mobility Router Transcoding** to keep the Mobility Router transparent during SDP negotiations. In this mode, the Mobility Router does not inspect the SDP, and simply forwards it to the other side. Except for special cases (for example, Access calls), RTP packets do not pass through Mobility Router. This mode is most desirable when transcoding and media bridging are not necessary.

- The Mobility-Router preferred Codecs display in the table in the following priority list.
  - G.711 μ-law
  - G.711 a-law
  - G.729 Annex-B
  - iLBC 30
  - AMR

  a. Use the Up or Down buttons to select the highest priority codec supported by both ends. Move the codecs into their appropriately ranked order for usage, the top codec being the highest priority. To modify the packet duration of a codec:

  b. Select the codec from the table.

  c. Click **Modify**.

  d. Modify the packet duration.

  e. Click **Apply** to save changes and return to the main screen.

Configuring PBX Options

PBX Trunk-side and Line-side options can be configured using the **Configuration > Voice > IP-PBXs > Options** tab.

Line side support provides registration of the user to the PBX and routes all the call feature requests on the Line side IP and Port.

Trunk side support does not register the user to the PBX. Trunk side support routes all the call feature requests on the Trunk side IP and Port.

Options include:

- **Caller ID Preferences** (Trunk side only) —selects either Enterprise Extension or Enterprise Full Number as the caller ID for outgoing calls.
- **SIP User ID** (Line side only) —selects either Enterprise Extension or Mobility User ID in the User ID field of SIP messages.
- **Call Forward**—configures call forwarding features, including PBX-based call forwarding and local call forwarding.
- **Call Transfer**—enables call transfer features, including PBX call transfer, local call transfer, and consultation and blind transfer options when transferring to a desk phone.
- **Default Enterprise Cellular Call Indicator**— selects the option to Prepend Digits to Caller ID, Map Used to Unused Area Codes in North America, Use Numbering Plan Enterprise Full Number Pattern, or None.
- **Voice Mail**—configures voice mail routing.
- **No Answer Ring Duration** (Trunk side only)—configures the length of time that ringing occurs before ringing discontinues.
- **Forced Ringback Start Timer**—configures the time the Mobility Router waits for a receive SIP Ringing message from the Called party before sending the SIP Ringing message to the Calling Party.
- **SIP Session Timer**—Configures the session interval for a SIP session. It is placed only in 'invite' or 'update' requests, as well as in any 2xx response to an 'invite' or 'update'.

To configure PBX options:

1. If the IP-PBX configuration page is not active, click **Configuration > Voice > IP-PBXs**. Select the IP-PBX you want to change and click Modify.
2. Click the **Options** tab.
3. In the **SIP User ID (Line Side)** or **Caller ID Preferences (Trunk side)** area, select one of the following:
   - **Enterprise Extension** — the abbreviated number assigned to the user within the enterprise. The User ID matches the Client user name within Director.
   - **User ID** — the Client user name within Director.
4. In the **Call Forwarding** area, select one of the following:
   - **PBX-based Call Forwarding** - check this field to forward the call to a new number. This function is recommended if PBX supports SIP "302" response. This is the default.

- **Local Call Forwarding** - select this option to allow the Mobility Router (not the PBX) to forwarding the call.

WARNING!

For IP-PBX releases 11.x and older, confirm that **Call Forwarding > Local Call Forwarding** is enabled/selected; **Local Call Forwarding** may not be the default in these releases.

5. In the **Call Transfer** area, select **Use PBX Transfer Feature** to enable SIP referral. Otherwise select **Local Transfer**.

   - When Mobility users are members of a conference call on their mobile devices, they have the option to transfer the call to their desk phones. (Note that a Mobility user who originates a conference call cannot transfer to desk.) When a member of the conference call transfers the call to the desk phone, the other members of the conference call can hear the desk phone ringing until the user answers the desk phone if a blind transfer is used. This is **Blind Transfer**.

   - To prevent conference call members from hearing the desk phone ringing if a Mobility user transfers the call to the desk phone, the Mobility Router select **Consultation Transfer**. We recommend keeping this default value, unless your PBX does not support consultation transfers. See your PBX documentation for information about transfer support.

6. In the **Voice Mail redirection** area, select one of the following:

   - **Busy Redirection** - PBX routes the call to voice mail on busy response. Selecting this option is recommended if the PBX forwards the call to voice mail after receiving a SIP “486” response.

   - **Server** - Microsoft Exchange® server information for retrieving voice mail. Enter the hostname IP address, port number and transport protocol.

   - **Pilot Number** - the number used to forward to voice mail. Select this option to enter the number in the field. DTMF sequence includes three parts: pre-digits; voice mail ID; post-digits. If the voice mail server requires DTMF sequence to identify the voice mailbox, select the following.

     - Pre-Digits field- Enter the pre-digit of the sequence. Valid characters are 0-9, A-D, “*”, “,” and “#”. Use the “,” to add a one second delay in the sequence.

     - Voicemail Box Number - Select the appropriate voice mail ID used in your system from the dropdown menu. The dropdown menu displays:

       - None — Only pre-digit and post-digit numbers are used.

       - Additional Number — The User’s additionally configured number is used between the pre-digit and post-digit numbers. Refer to Configuring Additional Devices on page 163 for more information.

       - Enterprise Extension — The User’s enterprise extension is used.

       - Enterprise Full Number — The User’s enterprise full number is used.

- Post-Digits fields - Enter the pre-digit of the sequence. Valid characters are 0-9, A-D, “*”, “,” and “#”. Use the “,” to add a one second delay in the sequence. An example of DTMF sequence: “,8027#2”, where “,” is the pre-digit, “8027” is the Enterprise Extension used as the voice mail ID, and “#2” is the post-digit.
- **Explicit MWI Subscription Required** - Check this box if your PBX requires an explicit subscription for receiving a message waiting indicator.

7. In the **No Answer Ring Duration** (Trunk side only) field, enter the length of time that ringing occurs before ringing discontinues. The default is 24 seconds. The range is 5-180 seconds.
8. Enter the number of seconds in the **Forced Ringback Start Timer** field to control the maximum time the Mobility Router waits for a SIP Ringing message from the Called party before sending the SIP Ringing message to the Calling Party. The default value is 8 seconds.
9. Enable or disable the **SIP Session Timer**. If enabled, enter the session refresh interval. The valid range is 90-65535 seconds and is enabled by default.
10. Check or uncheck the **Play Music on Hold** check box. If checked, the music on hold is played when the user/client places somebody on hold.
11. To save your changes, click **Apply**.

Modifying an IP-PBX

You can change the details of an IP-PBX, but any changes should be made carefully so as not to disrupt end-user services.

To modify an IP-PBX:

1. Click **Configuration > Voice > IP-PBXs**. The IP-PBXs page displays.
2. Select the IP-PBX that you want to modify.
3. Click **Modify**.
4. Make changes as necessary on the **General** tab. You cannot modify the IP-PBX name.
5. To save your changes, click **Apply**.
6. Make changes as necessary on the **SIP Trunk, Numbering Plan, Device Mobility** and **Options** tabs.
7. To save your changes, click **Apply** on each tab.

Deleting an IP-PBX

If an IP-PBX is assigned to a group, you must first change the group setting to a different PBX before deleting a PBX.

To delete an IP-PBX:

1. Click **Configuration > Voice > IP-PBXs**.

   The IP-PBXs page displays.

2. Select the IP-PBX that you want to delete.
3. Click **Delete**. The IP-PBX is deleted.

Copying a PBX

When creating or modifying a PBX, you can copy the PBX to another PBX template.

To copy a PBX:

1. Select **Configuration > Voice > IP-PBXs**. The **IP-PBXs** page displays.
2. Select the PBX that you want to copy.
3. Select **Copy**.
4. A new IP-PBXs template is created and displays **Copy <Name>** at the top of the window.
5. Fill in the fields as described in Adding an IP-PBX on page 98 or Modifying an IP-PBX on page 120 and save. Once the changes are saved, the name displayed for this IP-PBX changes from “Copy <Name>” to the saved name.

CHAPTER

11

Configuring Voice Settings

Voice settings are established to allow the Mobility Router to communicate with an enterprise IP-PBX. You must add an IP-PBX on the Mobility Router so that the Mobility Router can communicate with the PBX. You must also specify access numbers, which are phone numbers that allow users to make and receive calls on their mobile devices while using the Connect Platform.

This chapter contains the following sections:

Managing Access Numbers

Access Numbers are a collection of numbers used by the Mobility Router to provide identifiers and access to various services on the Mobility Router. Multiple sets of Access Numbers can optionally be defined on a per country basis if required. Access Numbers are needed to support the following services on the Mobility Router:

- Handover between Wi-Fi and cellular networks
- Enterprise dialing while operating on the cellular network
- Enterprise voice mail access while on the cellular network
- Reverse dial services

Adding Access Numbers

To Add access numbers:

1. Click **Configuration > Voice > Access Numbers**. The **Access Numbers** page displays.
2. Click **Add**.
3. In the **Name** field, type the name for the access number. The name can be up to 50 alphanumeric characters long and cannot contain special characters except for spaces, hyphens (-), and underscores (_).
4. (Optional) In the **Description** field, type a description for the access number.
5. In the **VoIP Handover Number** field, type the access number that the Connect Platform uses to hand over an active call from the cellular network to the Wi-Fi network. The Connect Platform dials the VoIP handover number when an active call needs to be handed over to a VoIP network.

Make sure that the phone number you specify is a unique phone number, with a valid area code, in your enterprise network. Using a unique phone number ensures that the Mobility Router can identify that an active call needs to be handed over from a cellular network to a Wi-Fi network.

The phone number must also use the appropriate numbering format for the country in which the Mobility Router is located. The Mobility Router uses this phone number as the caller ID when the Mobility Router calls the mobile device to deliver enterprise voice mail notification when the device is on the cellular network. If the phone number is not formatted correctly, the PSTN or cellular network might not deliver the caller ID correctly to the Connect Platform.

The phone number cannot contain spaces, hyphens (-), or parentheses [()].

An example of a VoIP handover number for a Mobility Router located in the United States is +4089198000.

1. In the **Voice Mail Access Number** field, type the extension number of the pilot number of the voice mail system, which is the enterprise extension that is dialed for users to access their voice mail.

2. Use the **Mobile to Fixed Reverse Call Indicator** field to enforce the Reverse Dial Number as Caller ID in the reverse call. When None is selected, a Connect Platform accepts any call as reverse call when it is waiting for a reverse dial call. When Reverse Dial Number as Caller ID is selected, the client must receive a call with Reverse Dial Number as caller ID in order to accept the call as the reverse dial call.

Note

Mobile to Fixed Reverse Dial is supported on iPhone and Android devices when the Connect Platform has Wi-Fi or Cellular Data connection with Mobility Router.

3. In the **Default Cellular Access Numbers** area, enter the following information:

   - **Country**— Select a country from the dropdown menu to define the access number.
   - Enterprise gateways and IP-PBXs need to be configured such that calls made to this number are delivered to the Mobility Router.
   - **Access Number**— the phone number that the Connect Platform uses to access the Mobility Router from the cellular network. Use the international dialing format, which includes a plus sign (+) before the phone number. The international dialing format does not work for some CDMA mobile devices. For users with these devices, add a separate cellular access number without the plus sign (+) and assign this number to a group that contains only users with CDMA mobile devices. Include the local country code and local area code in the cellular access number. The Connect Platform application uses this phone number to access the Mobility Router from the cellular network. This number can be used for such services as originating call from the cellular network or configuring various call features. This number must be a valid PSTN number and match the route pattern of the SIP trunk configured on the IP-PBX.
   - **Reverse Dial Number**— used in the following cases:

Note

Mobile to Fixed Reverse Dial is supported when the Connect Platform has Wi-Fi or Cellular Data connection with Mobility Router. This feature is supported on iPhone and Android devices only.

     - The Mobility Router uses this number as caller ID on a Mobile to Fixed Reverse Call or Reverse Wi-Fi to Cellular handover call, and the Connect Platform users the Caller ID to differentiate a Reverse call from other calls.
     - The Connect Platform calls this number to establish a Fixed to Mobile Reverse Dial Call.

   - **Handover Number**—Phone number that the Mobility Router calls to hand overactive VoIP calls to the cellular network.

     Mitel recommends that the cellular handover number be a different phone number than the cellular access number so that access call requests can be unambiguously distinguished from handover requests. If you have a limited number of available Direct Inward Dialing (DID) numbers, you can specify the same phone number for the cellular access number and cellular handover number.

The phone number cannot contain spaces, hyphens (-), or parentheses [()]. In general, follow these guidelines when specifying the cellular access number:

Use the international dialing format, which includes a plus sign (+) before the phone number. If this format does not work for some CDMA mobile devices, add a separate cellular access number without the plus sign and assign this number to a group that contains only users with CDMA mobile devices. Include the local country code and local area code in the cellular access number.

Enterprise gateways and IP-PBXs need to be configured such that calls made to these numbers are delivered to the Mobility Router.

4. Click **Apply**. The Country Specific Access Numbers area is enabled.
5. In the **Country Specific Cellular Access Numbers** area, click **Add**. Entries are only required in this table if you have access numbers in multiple countries, where you want to route calls through these numbers, when users are roaming. Using this feature minimizes costs. The information entered in these fields take precedence over the fields in the previous screen. If these fields are not filled in, the fields in the previous steps are the default:
   - Country
   - Access Number
   - Reverse Dial Number
   - Handover Number
6. Multiple access numbers may be added per country. To add more numbers, repeat these steps and click **Apply**. All Country Specific Cellular Access Numbers are added at the top-level Access Numbers screen in a folder.
7. To save your changes, click **Apply**.

Modifying Access Numbers

To modify an access number:

1. Click **Configuration > Voice > Access Numbers**. The **Access Numbers** page displays.
2. Select the access number to be changed.
3. Click **Modify**. The **Modify Access Numbers** page displays.
4. Change any options as necessary. You cannot change the name when modifying an access number. For information about the options that you can change, see “Adding Access Numbers” on page 123.

Note

Country Specific Access Numbers may not be modified at the top-level Access Numbers screen. Select the access number or the folder in the Access Number row and click Modify. Select the Country Specific Access Number to be changed and click **Modify**.

5. To save your changes, click **Apply**.

Deleting Access Numbers

To delete an access number:

1. Click **Configuration > Voice > Access Numbers**. The Access Numbers page displays.
2. Select the access number that you want to delete.
3. Click **Delete**. The access number is deleted.

Note

Country Specific Access Numbers may not be deleted from the top-level Access Numbers screen. Select the access number or the folder in the Access Number row and click Modify. Select the Country Specific Access Number to be changed and click Delete.

Viewing Table Rows

Note

Refer to Copying a Selection on page 20 for information about how to copy a selection on a page.

Expand All

1. Click in the Access Numbers Summary page.
2. Right-click to **Select All Rows**.
3. Right-click to **Expand All**.

Collapse All

1. Click in the Access Numbers Summary page.
2. Right-click to **Select All Rows**.
3. Right-click to **Collapse All**.

Importing/Exporting Numbering Plan Templates

Numbering plans can be imported and added to the Numbering Plan template and exported as a binary file. Numbering plans can also be deleted from the Mobility Router.

Importing a Numbering Plan

To import a Numbering Plan:

1. Click **Configuration > Voice > Numbering Plan Templates**. The **Numbering Plan** page displays.
2. Click **Select Import File (Requires IE)** to locate the numbering plan template to import. After selecting the appropriate numbering plan, click **OK**.
3. The new numbering plan is populated in the Numbering Plan page. If a file is added with the same name as an existing plan, the original plan is not overwritten. The new plan's name is appended to show distinction.

Exporting a Numbering Plan

To export a Numbering Plan:

1. Click **Configuration > Voice > Numbering Plan Templates.** The **Numbering Plan** page displays.
2. Select a Numbering Plan to be exported.
3. Click **Export** to send a numbering plan to a specified location. A directory popup displays. Browse to the appropriate location to save the file, optionally rename the file with a name that represents this numbering plan or country.
4. Click **OK** to save the file in this location.

Deleting a Numbering Plan

Note

Default plans are noted as such and cannot be deleted.

1. To delete a Numbering Plan:
2. Click **Configuration > Voice > Numbering Plan Templates**. The Numbering Plan page displays.
3. Select a numbering plan from the list.
4. Click **Delete**. You will be prompted with a confirmation. Click **OK** to proceed or Cancel to return to the main screen without saving changes.

Configuring Advanced Voice Settings

The Voice menu includes Advanced settings used to verify SIP server settings, Media Server settings, remote access settings, tune cellular operator information, and display a list of supported mobile devices.

The following are Advanced voice settings:

Configuring SIP Server Settings

SIP Server Settings are used to control SIP communications between the Mobility Router and the Connect Platform. When you set up the Mobility Router with the Initial Configuration Wizard, you provided the IP address of the Mobility Router, which is what the SIP server settings are based on.

You typically do not need to modify the SIP server settings. An example of when you might need to modify SIP server settings is if you need to change the port numbers on which the Mobility Router listens to UDP, TCP, or TLS traffic.

To configure SIP server settings:

1. Click **Configuration > Voice > Advanced > SIP Server**. The **SIP Server** page displays.
2. In the **UDP Port** field, type the port number on which the Mobility Router listens for UDP traffic. The UDP port can be between 1024 through 49151. The default UDP port is 5060.
3. In the **TCP Port** field, type the TCP port number on which the Mobility Router listens for TCP traffic. The TCP port can be between 1024 through 49151. The default TCP port is 5060.
4. In the **TLS Port** field, type the TLS port number on which the Mobility Router listens for TLS traffic. The TLS port can be between 1024 through 49151. The default TLS port is 5061.
5. In the **Registration Refresh Interval on Wi-Fi** field, type the interval at which the client on Wi-Fi refreshes its registration with Mobility Router. The default is 240 seconds.
6. In the **Registration Refresh Interval on Cell-Data** field, type the interval at which the client on the cellular data network refreshes its registration with Mobility Router. The default is 480 seconds.
7. In the **SIP Initial Retransmit Timer (T1) For Local Wi-Fi** field, type the time at which the Mobility Router retransmits the SIP request messages towards the client when it is in local Wi-Fi network. The default is 750 ms.
8. In the **SIP Initial Retransmit Timer (T1) For Remote Wi-Fi** field, type the time at which the Mobility Router retransmits the SIP request messages towards the client when it is in remote (SRV) Wi-Fi network. The default is 1000 ms.
9. In the **SIP Initial Retransmit Timer (T1) For Cellular Data** field, type the time at which the Mobility Router retransmits the SIP request messages towards the client when it is in cellular data network. The default is 2500 ms.
10. To save your changes, click **Apply**.

If you make any changes on this page, restart the SIP service.

Managing Voice Prompts

The Voice Prompt Profile feature allows the Admin to replace the system default audio for ringback, no answer, not found, busy, comfort noise, and music on hold. These profiles can be assigned to a PBX, enabling all users assigned to this PBX to use the voice prompts from this profile. All profiles are initially assigned with the factory default voice prompts. After creating the profile, any of the voice prompts can be modified. The following prompts can be selected:

- Ringback - the tone the calling party hears when the called party's device starts ringing.
- No Answer - the tone or announcement the calling party hears if the called party does not answer the call.
- Not Found - the tone or announcement the calling party hears if the called number is not a valid number.
- Busy - the calling party hears this prompt when the called party device is busy.
- Comfort Noise - this sound is played to avoid the uncomfortable "dead" silence that might make caller think that there is something wrong with connection.
- Music on Hold - this is played when the user/client puts somebody on hold.

Note

All prompts except Music on Hold are played to the Connect Platform when the user places outgoing calls from the cellular network. When on Wi-Fi, the client plays local voice prompts. Music on Hold is played when the user on Wi-Fi places the remote party on hold. When on the cellular network, the cellular network hold feature is used, which may produce a different result.

Adding a Voice Prompt Profile

To create a profile:

1. Click **Configuration > Voice > Advanced > Voice Prompt Profiles**. The **Voice Prompt Profile** page displays with the default profile.
2. Click **Add**.
3. Enter a name and description for the new profile.
4. Click **Apply**.
5. The new profile is added. The default Voice Prompts are associated with the new profile.

Modifying Voice Prompts

You can change any of the user-created profile Voice Prompts by importing a new prompt/sound. Internet Explorer is required. The audio file you are uploading must meet the following requirements:

- .wav file
- Sampling rate = 8000
- 1 channel (mono)
- 8-bit sample A-law and U-law or 8- or 16-bit sample for PCM

Note

The Default Voice Prompt Profile cannot be modified.

To modify a voice prompt:

1. Click **Configuration > Voice > Advanced > Voice Prompt Profiles**. The **Voice Prompt Profile** page displays.
2. Select the profile you want to modify. The profile's list of prompts displays in the screen below.
3. Select the voice prompt you want to modify and click **Change File (Requires IE).**
4. Select the appropriate.wav file and click **Open**.
5. The imported file is now used for the selected prompt.
6. To remove the new prompt and revert to the default setting, select **Restore Default**.

Deleting Voice Prompt Profiles

Before deleting voice prompt profile, make sure that no users are provisioned to that profile.

Note

The Default Voice Prompt Profile cannot be modified.

To delete a profile:

1. Click **Configuration > Voice > Advanced > Voice Prompt Profiles**. The **Voice Prompt Profile** page displays.
2. Select the profile that you want to delete and click **Delete**.

CHAPTER

12

Managing Calling Rules

Calling rules direct calls to specified destinations based on user requirements. Calling rule criteria can include a range of days, days of the week, time of day, calling party telephone number, and user location. Based on the calling rule, incoming calls are routed to the specified destination, such as an office telephone, mobile device, or voice mail system.

Calling rules based on the day of the week, time of day, and calling party number offer an efficient method of processing incoming calls. Calling rules that also consider the user location provide additional flexibility and convenience when users are out of the office and require fewer changes, even when schedules vary.

For example, if the user is at home between 7 p.m. and 8 a.m., all calls are routed to enterprise voice mail. However, if the user is still in the office during this time, calls continue to be routed to the desk phone.

A table of country-specific numbers may be imported or exported using the Numbering Plan feature. Use the Connect Platform to configure individual phone features, such as ringback tones. Refer to the Connect Platform User's Guide for more information.

A default set of country numbering plans can be selected when adding a new PBX. Administrators can also create and configure custom dial plans.

This chapter contains the following sections:

Calling Rules

Create calling rules at the global level by using the **Configuration > Policies > Calling Rules** page and then assign them to groups and users. Calling rules created this way are not active until they are assigned to groups or users. For more information, see “Assigning Calling Rules to a Group” on page 155 and “Assigning Calling Rules to Users” on page 165.

You can also add a calling rule when creating or modifying a group or user, which automatically assigns the rule to that group or user. Group calling rules apply to all users in the group. See “Managing Groups” on page 144 and “Managing Users” on page 158 for details about adding calling rules using the Groups and Users pages.

The following describes calling rules with location-based constraints that you might create:

- From 8:00 a.m. to 6:00 p.m., a user receives all calls at the desk phone when in the office. If the user leaves the office between 8:00 a.m. to 6:00 p.m., all calls are routed to the mobile device, allowing the user to continue to be responsive while out of the office.
- At all hours, all calls from a specific phone number (for example, a manager) are routed to the desk phone or mobile device, based on location, allowing the manager to reach users regardless of location.
- When a user is out of the office between 6:00 p.m. to 7:00 p.m., all calls are routed to the mobile device, allowing the user to receive calls during the commute. If the user is still in the office during this time, calls continue to be routed to the desk phone.

Creating a Calling Rule

To create a calling rule:

1. Click **Configuration > Policies > Calling Rules**. The **Calling Rules** page displays.
2. Click **Add**.
3. In the **Name** field, type a name for the calling rule.

The name can be up to 50 characters long and can contain letters and numbers. Do not use any special characters, including spaces, except for hyphens (-) and underscores (_).

Calling rule names are case-sensitive. For example, Commute is not the same as commute.

4. To activate the calling rule, select the **Active** check box.

To disable the calling rule, clear the **Active** check box. By default, the Active check box is selected.

5. (Optional) In the **Description** field, type a description for the calling rule. The name can be up to 50 characters long and can contain letters, numbers, and spaces. Do not use any special characters except for hyphens (-) and underscores (_).
6. In the **From** field, type one or more phone numbers for which the calling rule applies.

Keep the following in mind when filling in the **From** field:

- If you specify a 7- or 10-digit number, the calling rule is effective only if the designated IP-PBX has a numbering plan that includes entries that maps the short and long version of numbers within the numbering plan. For more information, see "Configuring Numbering Plan Settings" on page 100.
- Do not use hyphens when specifying phone numbers. For example, type `4085554442`.
- If typing more than one phone number, separate the phone numbers with commas (for example, `4085551732, 4085554356`).
- You can type up to 50 characters in the **From** box. If you use commas to separate phone numbers, the commas count toward the 50-character limit.
- If you leave this box empty, the calling rule applies to all phone numbers. If you do not specify any phone numbers in this field, you must specify a time constraint, as described in Step step 2.

Table 8 lists patterns that you can use in the **From** field to specify a range of phone numbers rather than individually specifying phone numbers.

Table 8: Allowed Patterns for Phone Numbers

Valid and Active States	Description
`X`	Specifies a single digit in the range 0 through 9. For example, if you type `408555120X`, the calling rule applies for all phone numbers starting with 408555120, up to 4085551209.
`[`*list*`]`	Specifies a single digit within *list*, where *list* is one or more digits. For example, if you type `408555120[123]`, the calling rule applies for the following phone numbers: 4085551201, 4085551202, 4085551203.
`[`*digit1*`-`*digit2*`]`	Specifies a single digit in a range from *digit1* through *digit2*. For example, if you type `408555120[0-7]`, the calling rule applies *only* for the following phone numbers: 4085551200, 4085551201, 4085551202, 4085551203, 4085551204, 4085551205, 4085551206, and 4085551207.
`[*`*list*`]`	Specifies zero or more digits from the list. For example, if you type `408555[*123]444`, the following are some of the numbers for which the calling rule is applied: 4085551444, 4085552444.
[*digit1-digit2]	Specifies zero or more digits in a range from *digit1* through *digit2*. For example, if you type `408555120[*0-7]`, the following are some of the number for which the calling rule is applied: 4085551201, and 4085551202, 4085551203.

Table 8: Allowed Patterns for Phone Numbers

Valid and Active States	Description
*	Specifies zero or more of any digits. For example, if you type `408555*123*`, the calling rule applies to phone numbers that start with 408555 and include the pattern 123.
U	Specifies a special pattern—Type `U` for the calling rule to apply if the caller ID is unknown.

1. In the **Time Zone** list, select the time zone for the calling rule.
2. In the **Time Constraint** field, define one or more of the following time constraints for the calling rule:
   - **Date**—To specify the calling rule for a range of dates, click the first Date field to select the starting date from the calendar that displays. Then click the second Date field to select the ending date from the calendar.
   - To clear the date field, click the Date field to access the calendar, and select the date that is in the Date field. The Date field is now empty.
   - **Day**—To specify the calling rule for certain days of the week, select the check boxes for the days.
   - Clear the check boxes for the days for which you do not want the calling rule to apply. If you clear the check boxes for all days, the calling rule applies every day. By default, all workdays (Monday through Friday) are selected.
   - **Time**—To specify the calling rule for a timeframe, select the starting hour and minute values and the ending hour and minute values from the Time lists.

     Click **Add** for each time constraint you create.

     To modify a time constraint, select it, and click **Modify**. To delete a time constraint, select it, and click **Delete**.
3. To take the user's location into account for the calling rule, select the **Location Aware Policy** check box.

   Select one of the following:
   - **In the Office**—Calling rule applies only when the user is in the office.
   - **At Home**—Calling rule applies only when the user is at home.
   - **On the Road**—Calling rule applies when the user is out of range of the office or home network.

Note

o take location into account for the calling rule, you or the user must create a home location. For more information, see "Managing Home Locations" on page 167.

To have the calling rule apply to all locations, clear the Location Aware Policy check box. By default, the Location Aware Policy check box is not selected.

4. In the **Action** list, select one of the following actions that is taken if an incoming call matches the criteria of this calling rule:
   - **Do not ring any device**—Incoming calls are routed to the user's enterprise desk phone, if available. If the enterprise desk phone is not available, calls are immediately directed to the user's enterprise voice mail.
   - **Forward to Voicemail**—Calls are immediately directed to the user's enterprise voice mail.
   - **Ring all devices**—Ring all appropriately configured devices.

Note

Refer to the Mobility User Portal to specify a device to ring using the Ring Specified Device option. Contact your IT department for more information about accessing the Mobility User Portal.

5. To save your changes, click **Apply**.

Modifying a Calling Rule

After creating calling rules, you can modify them to change the criteria you previously defined. You can also modify calling rules that users created.

To modify a calling rule:

1. Click **Configuration > Policies > Calling Rules**. The **Calling Rules** page displays.
2. Select the calling rule to be modified.
3. Click **Modify**.
4. Make changes to the calling rule as appropriate.
5. You cannot change the name of the calling rule. For information about changing the properties of a calling rule, see "Creating a Calling Rule" on page 139.
6. To save your changes, click **Apply**.

Deleting a Calling Rule

You can delete calling rules that have not been assigned to a group or user.

Note

If a calling rule is assigned to a group or user, you must first unassign the calling rule before you can delete it. For more information, see "Unassigning Calling Rules for a Group" on page 155 or "Unassigning Calling Rules for Users" on page 165.

To delete a calling rule:

1. Click **Configuration > Policies > Calling Rules**. The **Calling Rules** page displays.
2. Select the calling rule that you want to delete. You can select multiple calling rules (contiguous or non-contiguous) to delete. Select multiple calling rules as you would select multiple items for your operating system.
3. Click **Delete**. The calling rule is deleted.

Assigning a Calling Rule

Calling rules created in the Policies page are not active until they are assigned to groups or users.

To assign a calling rule to a group or user:

1. Click **Configuration > Policies > Calling Rules**. The **Calling Rules** page displays.
2. Select the calling rule to be assigned.
3. Click **Assign**. The **Assign Calling Rule** page displays.
4. To assign this rule to a group, select the group and then click >> to add the group to the **Assigned** column. Refer to “Assigning Calling Rules to a Group” on page 155 for more information.
5. To assign this rule to users, select the users and then click >> to add the users to the **Assigned** column. Refer to “Assigning Calling Rules to Users” on page 165 for more information.
6. Click **Apply**. The calling rules are assigned, and the screen returns to the list of available calling rules.

CHAPTER

13

Managing Groups

Creating groups on the Mobility Router allows you to set up logical categories of users based on criteria such as department, geographical location, or any other separation that you choose. You can also use groups to apply policies, such as calling rules, balance loads on an IP-PBX, or apply access numbers.

This chapter contains the following sections:

Creating Groups

To create a group on the Mobility Router, configure general settings, security settings, remote access and calling rules before adding users.

Configuring General Settings

To configure general group settings:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Click **Add**. The **Add Group page** displays, with the **General** tab active.
3. In the **Name** field, type the name of the group. The group name can be up to 50 characters long and cannot contain special characters except for spaces, hyphens (-), and underscores (_).
4. In the **IP-PBX** list, select the IP-PBX that supports the group. If you have not previously added an IP-PBX, click **Add**. The Add IP-PBX page displays. For information about adding an IP-PBX, see “Adding an IP-PBX” on page 98. After you have added the IP-PBX, the **Add Group** page displays so that you can continue adding the group.
5. Select a **Directory Search Group** or create a new group by clicking **Add.** This is the company directory by which the Mobility Router will search for an individual.
6. In the **Access Numbers** list, select the access number that users in this group use to access Mobility Router services. If you have not previously added an access number, click **Add**. The **Add Access Numbers** page displays. For information about adding an access number, see “Adding Access Numbers” on page 123. After you have added the access number, the **Add Group** page displays so that you can continue adding the group.
7. Choose External User Authentication/Authorization from the drop-down list.
8. Choose Directory to map the Mobility Router group to a Directory. Choose the appropriate one from the drop-down list.

Configuring Security Settings

Click the **Configuration > Groups and Users > Groups >Groupname > Security** tab to define the following security settings for the group:

- “PBX-Side Security” on page 147—SIP security used for communication between the Mobility Router and the PBX:
  - No authentication is used between the Mobility Router and the PBX.
  - Mitel recommends using digest authentication (user name and password) between the Mobility Router and the PBX.
- “Client-Side Security (Wi-Fi)” on page 147—Specifies whether certificate-based SIP-TLS is used for SIP communication between the Mobility Router and mobile devices. Mitel recommends using this Client-Side Security for Wi-Fi.
- “Client-Side Security (Cellular)” on page 147—Specifies whether a personal identification number (PIN) is used to authenticate access requests received from the Connect Platform when

the mobile device is in the cellular network. Mitel recommends using this Client-Side Security for Cellular.

PBX-Side Security

To configure PBX-side security:

1. Do one of the following:
   - Click **None** if you do not want PBX-side security enabled.
   - Click **Digest** to specify that digest authentication is used.
2. In the **User ID** area, select one of the following:
   - **Same as RA User ID**—Specifies that the digest user name for an end-user matches the Mobility user ID.

Tip

Use the same User ID as the Mobility user ID.

   - **Same as RA User Enterprise Extension**—Specifies that the digest user name for an end- user matches the Enterprise Extension number.
   - **Default**—Specifies that a default digest user name is used for all users in the group.
3. In the **Password** field, type the default password that is used for all users in the group.

Client-Side Security (Wi-Fi)

To configure client-side security:

1. In the **Client-Side Security (Wi-Fi)** area, select one of the following:
   - None
   - Certificate

Client-Side Security (Cellular)

To configure client-side security:

1. In the **Client-Side Security (Cellular)** area, select one of the following:
   - **None**—No PIN is used between the Mobility Router and mobile devices.
   - **Generate random pin per user**—The Mobility Router automatically selects a random PIN for each mobile device, and the PIN is securely sent to the device during provisioning.
   - **Default Pin**—A default PIN is used for all mobile devices. If you select this option, type the default PIN in the box that displays.
2. To save your changes, click **Apply**. To apply these security settings to all existing users in the group, select **Apply to all existing users in this group** check box and then click **Apply**.

Configuring User Options

Click the **Configuration > Groups and Users > Groups > User Options** tab to configure the following user options:

Call Routing

To configure Call Routing for audio calls:

1. Select **Wi-Fi** to allow users in this group to access voice services over Wi-Fi. Click the **Remote Access link** to go to the **Remote Access** page to configure Remote settings including protocols and options. Refer to "Managing Remote Access" on page 40 for details.
2. Select **Cellular Data** to allow users in this group to access voice services from cellular packet-data networks.
3. Select **Cellular Voice** to allow users in this group to access voice services from cellular networks.
4. Select **Cellular Data Roaming**—Select to allow access to voice services from cellular packet-data networks when the mobile device is roaming.
5. Select **Cellular Voice Roaming**—Select to allow access to voice services from the cellular network when the mobile device is roaming.

Note

Some mobile devices, such as Apple iOS devices, cannot detect when the device is roaming. Enabling/Disabling Cellular Data Roaming and Cellular Voice Roaming will not be recognized by these devices. Instead, the administrator may need to set those users into a special Group with the desired settings for those devices.

Data Services

In the **Data Services** area, specify whether users in the group can access secure enterprise services from cellular packet-data networks and remote Wi-Fi networks.

1. **Cellular Data** —Select to allow users in this group to access secure enterprise services from cellular packet-data networks.
2. **Cellular Data Roaming**—Select to allow access to data services from cellular data networks when the mobile device is roaming.

By default, these options are not enabled. You can enable one or both options.

Note

Some mobile devices, such as Apple iOS devices, cannot detect when the device is roaming. Enabling/Disabling Cellular Data Roaming will not be recognized by these devices. Instead, the administrator may need to set those users into a special Group with the desired settings for those devices.

Presence/IM

Enable or disable Presence on the user devices in this group. By default, **Presence/IM** is disabled. If Presence is enabled, options pop up to control whether Presence/IM is available when the device is roaming:

1. **Cellular Data**—Select to allow Presence/IM information to utilize the cellular data networks.
2. **Cellular Data Roaming**—Select to allow Presence/IM information to utilize the cellular data networks when the mobile device is roaming.

Note

Some mobile devices, such as Apple iOS devices, cannot detect when the device is roaming. Enabling/Disabling Cellular Data Roaming will not be recognized by these devices. Instead, the administrator may need to set those users into a special Group with the desired settings for those devices.

Enterprise Cellular Call Routing

To configure Enterprise Cellular Call Routing, specify how direct cellular calls are routed.

1. Select **Mobile to Fixed Reverse Dial** to enable Mobile to Fixed Reverse Dial for the users in this group. This enables a client from a cellular network to request the Mobility Router (the “fixed” location in the system) place an outgoing call on the client’s behalf, either through cellular data service or through a call on the Reverse Dial Access Number. When the Mobility Router receives Mobile to Fixed Reverse Dial request, it first calls the client's cell number to establish a voice path to the client, then calls the remote party to connect with the client. In this case, the original call, which would have been dialed from Mobile device (Client) to the Fixed network (Mobility Router), is now being dialed from the Fixed network (Mobility Router) to the Mobile device (Client).

a. If **Mobile to Fixed Reverse Dial** is selected, the **Initial Call Settings** display. Select **Auto, On** or **Off**. The initial setting determines the Reverse Dial Mode upon provisioning. Once the client is provisioned, the user can change the mode from client's call settings menu. Select **On** to force the Reverse Dial on all future calls. Select **Off** to turn off the Reverse Dial feature. Select **Auto** to dynamically determine if an outgoing call should be reverse dialed.

Note

Changing the Initial Call Setting after provisioning does not change the client running the configuration.

If the **Mobile to Fixed Reverse Dial Mode** is set to **Auto**, reverse dial is automatically triggered when the following conditions are met:

- A non-U.S.-based SIM is roaming. For example, if a user with a United Kingdom SIM card is travelling outside the country.
- A non-U.S.-based SIM is not roaming and is without a country-specific access number available. For example, if a user with a United Kingdom SIM is in the UK, but there is no local UK access number.

2. Select **Fixed to Mobile Reverse Dial** to enable the Mobility Router (the “fixed” location in the system) to notify a device using the Connect Platform (in the cellular network) of an incoming call through cellular packet data service. The Client calls the Mobility Router’s Reverse Dial Access Number to pick up the call. In this case, the original call, which would have been dialed from Fixed network (Mobility Router) to the Mobile device (Client), is now being dialed from the Mobile device (Client) to the Fixed network (Mobility Router).

   a. If **Fixed to Mobile Reverse Dial, s**elect a **Fallback Option** in the event the Fixed to Mobile Reverse Dial call does not connect in time:

   - **Forward Dial** - the Mobility Router tries to connect the call by directly calling the Connect Platform cellular number. If this Fallback Option is selected but the call does not connect, the Mobility Router connects the remote party to the user’s enterprise voice mail.
   - **Voice Mail** - the Mobility Router connects the remote party to the user's enterprise voice mail.

3. Select one of the following to specify how outgoing cellular calls are routed:

   a. **Route all outgoing calls through the enterprise**—Select to route all outgoing cellular calls through the enterprise. By default, this option is selected.

   b. **Route all outgoing calls directly over cellular**—Select to route all outgoing cellular calls directly over the cellular network (not routed through the enterprise).

   c. **Route all outgoing calls directly over cellular except**—Select to route certain cellular calls through the enterprise. If you select this option, the following options are available:

   - **From nearby home or office location**—Select to route calls made when close to a home location or an enterprise Wi-Fi network through the enterprise. Clear this option to route these calls directly through the cellular network. By default, this option is selected.

- **Enterprise extensions**—Select to route calls to enterprise extensions through the enterprise. By default, this option is selected.

WARNING!

If you clear the Enterprise extensions option, users cannot dial only the extension when calling enterprise phone numbers. Users would need to dial the Enterprise Full Number.

- **International numbers**—Select to route outgoing international calls through the enterprise. Clear this option to have international calls go directly over the cellular network. By default, this option is selected.

Emergency Call Routing

1. Select **Allow Emergency Calls on VoIP** to enable emergency calls to be placed over VoIP. By default, this option is disabled (recommended). Emergency calls are routed directly over the cellular network when cellular coverage is available regardless of the setting of this option. When **Allow Emergency Calls on VoIP** is not selected and cellular coverage is not available, emergency calls will fail as they are not routed over VoIP.

   a. If **Allow Emergency Calls on VoIP** is selected, the option to **Block Remote VoIP Calls if Cell Coverage Is Not Available** is displayed.

   - If **Block Remote VoIP Calls if Cell Coverage Is Not Available** is selected, all remote VoIP calls (emergency and non-emergency) are blocked in the absence of cell coverage.
   - If **Block Remote VoIP Calls if Cell Coverage Is Not Available** is not selected, the system attempts to route emergency calls over VoIP when cellular coverage is not available, but Wi-Fi coverage is available, and if the phone is registered to the Mobility Router. Softphone technology utilized by this application may not provide accurate or timely location information data; calls may be misdirected to the wrong emergency response center or the emergency response center may make errors when determining your location. Mitel is not liable for any resulting error or delay.

For more information about configuring emergency number patterns, refer to “Emergency Number Pattern” on page 111.

Cellular Voice Mail Indicator

Select the **Cellular Voice Mail Indicator** check box to enable the enterprise voice mail message indicator on the mobile device when it is on the cellular network. By default, this option is enabled. If you do not select this option and users receive enterprise voice mail while on the cellular network, no voice mail indicator displays on the mobile device.

Note

If the Connect Platform is registered with the Mobility Router via cellular data (not on Wi-Fi), the Mobility Router sends the MWI notification when the client is on the cellular network. In this case, enabling the Cellular Voice Mail Indicator check box is not required.

Call Ignore

Select **Ignore call on all shared line devices** to ensure the mobile device and all other devices that share the same line immediately stop ringing when a user selects to ignore an incoming call on the mobile device. If this option is not selected and the user chooses to ignore an incoming call on the mobile device, the other devices sharing the same line continue to ring until the maximum ring time configured on the PBX is reached. If none of the other devices answers the call within the maximum ring time, the call is then forwarded to voice mail.

Note

Call Ignore is available on VoIP calls only.

Note

Configure voice mail on the IP-PBX for this option to be effective. If voice mail is not configured on the IP-PBX, the call is not sent to voice mail.

Client Privilege

Assign a **Client Privilege** to this device. Select **Full** to show all menus and enable exiting.

Provisioning

Select **Prevent users from changing devices by re-provisioning** to disallow users in this group from provisioning with their credentials on another phone. The default is unchecked (disabled).

Applying Changes

Click **Apply** to save your changes, to apply these security settings to all existing users in the group, first select **Apply to all existing users in this group** and then click **Apply**.

WARNING!

If **Apply to all existing users in this group** is not checked before **Apply** is clicked, the selected options will not apply to the existing users in the group but will apply to any new users added to this group.

Configuring Device Options

Click the **Configuration > Groups and Users > Groups > Device Options** tab to configure the following device options:

Maximum Number of Devices

Select the maximum number of devices per user. The maximum is 5. The default is 1. The Maximum Number of Devices per user setting in the Users page takes precedence over this setting. Refer to "Configuring the Connect Platform Device" on page 161 for more information.

DTMF Error Correction

Enable **DTMF Forward Error Correction** to improve reliability of DTMF digit delivery on calls placed on the cellular network. The default is **Disabled**. Note that when changing the operational functionality between **Enabled** and **Disabled**, the client may take some time to sync with the change.

Caller ID via DTMF

Enable **Caller ID via DTMF** is to view options **Always, Never** or only when **Roaming**. Some cellular operators block Caller ID for cellular calls.

- The default for this option is **Roaming**, where the client uses DTMF for presenting its caller ID when in a roaming network.
- Select **Always** when the cellular operator in this area is known to block Caller ID.
- Select **Never** when the cellular operator in this area does not block Caller ID.

Cellular Call Answer Confirmation

The **Cellular Call Answer Confirmation** feature helps the enterprise user to properly route the call to enterprise voice mail.

- When on the cellular network, and this feature is set to **None**, the Mobility Router does not distinguish between the user answering the call or the cellular voice mail. Select **None** to send enterprise voice messages to the personal cellular mailbox.

- If this feature is set to **DTMF**, the Mobility Router distinguishes between the user answering using a DTMF tone and cellular voice mail answering. In this case, the Mobility Router identifies the user's cellular voice mail, and routes the call to the enterprise voice mail.

WARNING!

Android and iPhone devices do not send the DTMF digit "#". Select **IVR** for these devices to route the call to enterprise voice mail.

Applying Changes

To save your changes, click **Apply**. To apply these security settings to all existing users in the group, first select **Apply to all existing users and devices in this group** and then click **Apply**.

WARNING!

If **Apply to all existing users and devices in this group** is not checked before **Apply** is clicked, the selected options will not apply to the existing devices of the users in the group but will apply to any new devices associated with users added to this group.

Managing Calling Rules for Groups

You can create calling rules to direct calls to specified destinations based on individual user requirements. Calling rule criteria can include a range of days, days of the week, time of day, calling party telephone number, and user location. Based on the calling rule, incoming calls are routed to a specified destination, such as an office telephone, mobile telephone, or the user's voice mail system.

Calling rules based on the day of the week, time of day, and calling party number provide efficient processing of incoming calls. Calling rules that also consider the user's location provide the user with additional flexibility and convenience when out of the office and require fewer changes, even as the user's schedule changes.

You can manage calling rules while creating or modifying groups. You can also perform these tasks by using the **Configuration > Policies > Calling Rules** page. For more information, see "Creating a Calling Rule" on page 139.

When creating or modifying a group, you can also add users to the group without having to switch to the Users page.

Adding Calling Rules

When you add a calling rule as part of creating a group, the calling rule is automatically assigned to the group. You can also later assign the calling rule to other groups or users. For more information, see "Assigning a Calling Rule" on page 143.

To create a calling rule:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group to which you want to add a calling rule.
3. Click **Add**. The **Add Calling Rule** page displays.

4. Specify the details of the calling rule. For information about adding a calling rule, see “Creating a Calling Rule” on page 139.

Modifying Calling Rules

To modify a calling rule:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group to which the calling rule is assigned.
3. Click **Modify**. The **Modify Group** page displays.
4. Click the **Calling Rules** tab.
5. Click **Modify**. The **Modify Calling Rule** page displays.
6. Make changes to the calling rule as needed. For information about modifying calling rules, see “Modifying a Calling Rule” on page 142.

Assigning Calling Rules to a Group

To assign a calling rule to a group:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group to which you want to assign the calling rule.
3. Click **Modify**. The **Modify Group** page displays.
4. Click the **Calling Rules** tab.
5. Click **Assign**. The **Assign Calling Rule** page displays.
6. Select the calling rule to assign to the group.
7. Click **Apply**. The page returns to the **Calling Rules** tab and shows the calling rules assigned to the group.

Unassigning Calling Rules for a Group

To unassign a calling rule for a group:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group for which you want to unassign the calling rule.
3. Click **Modify**.
4. Click the **Calling Rules** tab.
5. Select the calling rule to unassign from the group.
6. Click **Unassign**. The calling rule is removed from the list of calling rules assigned to the group.

Setting Priority for Calling Rules for a Group

For a group, calling rules are checked in the order in which they appear in the Calling Rules tab. You can move a calling rule up or down to promote or demote the priority of the calling rule.

To set the priority for a calling rule:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group assigned to the calling rule you want to change.
3. Click **Modify**. The **Modify Group** page displays.
4. Click the **Calling Rules** tab.
5. Select the calling rule to promote or demote from the group.
6. Click **Move Up** or **Move Down** to change the priority of the rule. The rule moves within the list as the Move Up or Move Down option is selected.

Adding Users to a Group

To add users to a group:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group to which you want to add a user.
3. Click **Modify**. The group displays with the General tab selected.
4. Click the **Users** tab.
5. Click **Add**. The **Add User** page displays.
6. To complete the **Add User** pages, see “Creating Users” on page 159.

Modifying Groups

To modify a group:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select the group associated with the user you want to change.
3. Click **Modify**. The group displays, with the **General** tab active.
4. Make changes to each page as required.
5. To save changes. click **Apply** on each page.

Deleting Groups

You can delete groups from the Mobility Router. A group cannot be deleted if there are any users in the group. To delete a group that has users in it, you must first move the users to another group or delete all the users from the group.

To delete a group:

1. Click **Configuration > Groups and Users > Groups**. The **Groups** page displays.
2. Select one or more groups you want to delete.
3. Verify that the group has no users in it.
4. Click **Delete**.
5. When prompted to confirm the deletion, click **OK**.

CHAPTER

14

Managing Users

Each user on the Mobility Router must have a user profile on the Mobility Router. You can create a user profile locally, or the profile can be automatically added when authorized end users perform over-the-air provisioning using their mobile devices. For end-user provisioning to succeed, the user entry must exist within Director

This chapter contains the following sections:

Creating Users

End users can be in one of the following states on the Mobility Router:

Table 9: User Status

States	Description
Provisioning Status	**Authorized**—User exists on the Mobility Router but has not completed over-the-air provisioning. **Provisioned**—User exists on the Mobility Router and has also completed over-the-air self-provisioning. The user can be enabled or disabled.
PBX Registration Status	The PBX Registration Status is updated only after a device is registered to a user. Possible values are as follows: **Registered**— User has successfully registered to PBX. **Rejected**—PBX has rejected the registration request (for example, authentication was denied). **Unknown**—User is disabled. **NA**—User does not have a device registered in the PBX.

Configuring General Settings

To configure general settings:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Click **Add**. The **Add User** page displays.
3. In the **Group** list, select the group to which the user belongs.

Note

When a user is created, it inherits all the properties of the group. Any subsequent user customization overrides the group settings. You can override remote-access and call routing options and security settings made for a user by using the “Apply to all existing users in this group” option on the Security and Options tabs for a group. For more information, see “Configuring Security Settings” on page 146 and “Configuring User Options” on page 148.

4. In the **User ID** field, type the user name of the user and it must match with the client user name within Director (The client user name created on Director(PBX) includes apostrophes).
5. In the **Full Name** field, type the name of the user.

6. To enable the user, select the **Enabled** check box. If you do not select Enabled, the user is not active on the Mobility Router.
7. Click **Next**. The **Line** tab is active.

Configuring Line Settings

The user line settings are inherited from three sources:

- User's group settings
- Settings retrieved from the directory server
- Information provided by the user during Connect Platform provisioning. To

change line settings for a user:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user for which you want to change line settings.
3. Click **Modify**. The **Modify User** page displays.
4. Click the **Line** tab.
5. In the **Enterprise Extension** field, type the short dial number assigned to the user within the enterprise. This number must match the enterprise extension assigned for that user on the IP-PBX.

Note

An enterprise extension must contain a minimum of four digits and can be up to 15 digits long.

6. In the **Enterprise Full Number** field, type in the complete DID number in canonical format assigned to the User in the enterprise (for example, +612… for a number in Sydney, Australia, +1408… for a number in the south bay area, California, and so on.). This field is required.

Note

When adding a user, you must specify the complete 10-digit telephone number assigned to the user.

7. In the **Forwarding Number** field, type the number to which all calls to this User's extension will be forwarded. Valid length is between 3 and 15 digits. Clear this field to disable call forwarding. Users manage call forwarding from their mobile devices or by accessing the User Portal. An Administrator can enable call forwarding for users by setting the call forwarding number on the user's **Line** tab. Contact your IT department for more information about using the Mobility User Portal.

Note

Mobility Router call forwarding is unconditional: If call forwarding is enabled, all incoming calls are forwarded to the configured number. The feature is enabled when the forwarding number field is not empty. If the field is empty, the call proceeds to the mobile device.

8. In the **PBX-Side Security** area, select **None** or **Digest**. If Digest is selected, you must specify a user ID and password. When the user entry is created, it inherits the group's PBX-Side security settings. The digest user ID password must match the entry in the Digest Credentials field on the IP-PBX.
9. In the **Client-Side Security (Wi-Fi)** area, select **None** or **Certificate**.
10. In the **Client-Side Security (Cellular)** area, select **None** or **PIN**. If you select PIN, you must specify the PIN.
11. To save your changes, click **Apply**.

Configuring Devices

The Mobility Router supports two types of devices: **Connect Platform** and **Additional Device**. Use the **Devices** tab to add, modify, delete and configure devices.

The Connect Platform is the typically your main mobile device. Refer to "Configuring the Connect Platform Device" on page 161 for more information.

You have the option to configure additional devices. Refer to "Configuring Additional Devices" on page 163 for more information.

Note

After Connect Platform is installed on the mobile device, some of the settings on the Mobile Device page are automatically populated after the information is sent to the Mobility Router.

Configuring the Connect Platform Device

1. Click **Configuration > Groups and Users > Users** > **Devices** tab.
2. Select the maximum number of devices allowed for this user. The maximum is 5. The default is 1.
3. Select **Apply**.
4. Click **Add** to add a new device. The **Add New Device** page displays.

Tip

Adding a new user device is optional. Devices are automatically added once the user completes the provisioning of a new device through the Connect Platform app.

Note

An incoming call to the user will be forked simultaneously to all the user's devices, based on each device's current call routing capability (Wi-Fi, cellular data or cellular voice). Similarly, outgoing calls may be placed at the same time from all the devices, but the maximum allowed simultaneous outgoing calls per user is limited to two from the Mobility Router and the PBX's configurations.

Note

If modifying an existing device's configuration, double-click the device in the User Devices table, or select the device then click **Modify**, then follow these instructions to add a device. Similarly, to delete a device, select **Delete** and follow the prompts.

5. Select the Device Type of the **Connect Platform**.
6. Optionally, enter a **Device Name**. If not specified, the Mobility Router generates a generic device name.
7. Select **Next**.
8. In the **Cellular Number** field, type the user's cellular telephone number.
9. In the **Cellular Operator** list, select the cellular provider for the mobile device, or select Add or Manage to modify these settings.
10. In the **Cellular Network Type** list, select the network service type for the mobile device.
11. Select an **Operation Mode.**
12. The **Cellular Call Answer Confirmation** feature helps the enterprise user to properly route the call to enterprise voice mail.

    When on the cellular network, and this feature is set to **None**, the Mobility Router does not distinguish between the user answering the call or the cellular voice mail. Select **None** to send enterprise voice messages to the personal cellular mailbox.

    If this feature is set to DTMF, the Mobility Router distinguishes between the user answering using a DTMF tone and cellular voice mail answering. In this case, the Mobility Router identifies the user's cellular voice mail, and routes the call to the enterprise voice mail.

    Some devices do not send the DTMF digit "#". Select **IVR** for these devices to route the call to enterprise voice mail.
13. Enable **DTMF Forward Error Correction** to improve reliability of DTMF digit delivery on calls placed on the cellular network. The default is **Disable**.

Note

The current Client Configuration for DTMF Error correction is displayed. The value of this field is automatically set when the configuration is downloaded to the client. When the value of DTMF Error Correction is changed on the Mobility Router, the change will not be operational until the client receives the new configuration from the Mobility Router. During that time, the value for DTMF Error Correction of the Mobility Router configuration and the client configuration may be different.

14. In the drop-down list, select when **Caller ID via DTMF** is enabled. The options are **Always, Never** or only when **Roaming**. Some Cellular Operators block Caller ID for cellular calls. The default for this option is **Roaming**, where the client uses DTMF for presenting its caller ID when in a roaming network. Select **Always** when the cellular operator in this area is known to block Caller ID. Select **Never** when the cellular operator in this area does not block Caller ID.

15. Click **Apply**. The device is added to the **User Devices** table. Click the device row to display the device's values in the Device Details table. After the device has been provisioned using the mobility solution, the provisioning information populates in this table.

Managing Calling Rules for a User

When you create or modify a user, you can also create calling rules. This allows you to create and automatically assign the calling rules to the user without first creating a calling rule using the **Configuration > Policies > Calling Rules** page.

You can create, change, assign, unassign, and change the priority of administrator-defined calling rules. You can also modify or delete user-defined calling rules. User-defined calling rules are created by end users with the User Portal. Contact your IT department for information about using the Mobility User Portal.

Creating Calling Rules

When you create a calling rule while creating or modifying a user, the calling rule is automatically assigned to the user. A calling rule is not active until it is assigned to a user or group. If you created a calling rule using the **Configuration > Policies > Calling Rules** page, you can use that page to assign the rule to groups or users.

To create a calling rule:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user to which you want to add calling rules.
3. Click **Modify**. The **Modify User** page displays.
4. Click the **Calling Rules** tab.
5. Click **Add**. The **Add Calling Rule** page displays.
6. Specify the details of the calling rule. For information about calling rules, see "Calling Rules" on page 139.

Modifying Calling Rules

To modify a calling rule:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user whose calling rule you want to change.
3. Select **Modify**. The **Modify User** page displays.
4. Click the **Calling Rules** tab.
5. Click **Modify**. The **Modify Calling Rule** page displays.
6. Make changes to the calling rule as needed.

Assigning Calling Rules to Users

To assign a calling rule to a user:

1. Click **Configuration > Groups and Users > User**. The **Users** page displays.
2. Select the user for which you want to assign the calling rule.
3. Click **Modify**. The **Modify User** page displays.
4. Click the **Calling Rules** tab.
5. Click **Assign**. The **Assign Calling Rule** page displays.
6. Select the calling rule to which you want to assign to the user.
7. Click **Apply**. The screen returns to the Calling Rules tab and shows the calling rules assigned to the user.

Unassigning Calling Rules for Users

To unassign a calling rule for a user:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user to which to unassign the calling rule.
3. Click **Modify**. The **Modify User** page displays.
4. Click the **Calling Rules** tab.
5. Select the calling rule to unassign from the user.
6. Click **Unassign**. The Calling Rule is removed from the list of calling rules assigned to the user.

Setting Priority for Calling Rules for Users

Calling rules are checked in the order the are listed within the user calling rules screens. You can move a calling rule up or down to promote or demote the priority of the calling rule.

Note

If a user has multiple devices, the calling rules apply to all devices. In addition, location-based calling rules apply to each device based on the device's location (for example, enterprise, home, on the road, and so on.).

To set the priority for a calling rule:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user to change the priority of the calling rule.
3. Click **Modify**. The **Modify User** displays.
4. Click the **Calling Rules** tab.
5. Select the calling rule whose priority you want to change.

6. Click **Move Up** or **Move Down** to change the priority of the rule. The rule moves within the list as the Move Up or Move Down option is selected.

Managing User-Defined Calling Rules

You can perform the following tasks to manage user-defined calling rules.

Reviewing User-Defined Calling Rules

To review user-defined calling rules:

1. Click **Configuration > Groups and Users > Users**. The Users page displays.
2. Select the user to view the user-defined calling rule.
3. Click **Modify**. The user displays with the General tab selected.
4. Click the **Calling Rules** tab.
5. Verify the user-defined calling rules as needed.

Modifying User-Defined Calling Rules

To modify user-defined calling rules:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user to view the user-defined calling rule.
3. Click **Modify**. The user displays with the General tab selected.
4. Click the **Calling Rules** tab.
5. In the **User Defined** area, select the calling rule that you want to modify.
6. Click **Modify**.
7. Make changes as necessary.
8. Verify the user-defined calling rules as needed.

Deleting User-Defined Calling Rules

To delete user-defined calling rules:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select the user to view the user-defined calling rule.
3. Click **Modify**. The user displays with the General tab selected.
4. Click the **Calling Rules** tab.
5. Verify the user-defined calling rules as needed.
6. In the **User Defined** area, select the calling rule that you want to modify.
7. Click **Delete**. The calling rule is deleted.

Managing Home Locations

A home location consists of information about a user's Wi-Fi network, as well as cellular network information. This information allows you to know their location if they are connected to the Wi-Fi network associated with the home location.

You can create home locations for users. You need only know the SSID of a user's Wi-Fi network. When the user's mobile device connects to the Wi-Fi network associated with the home location, the Connect Platform sends all the home and cellular network information to the Mobility Router.

Users can also create and manage home locations using the Connect Platform on their mobile devices. Users can also manage home locations using the User Portal. When you create, delete, or edit a home location or home-location information with the User Portal, these changes are reflected in the Connect Platform. Any changes to home-location information that you make with the Connect Platform are also reflected in the Mobility User Portal. Contact your IT department for information about using the Mobility User Portal.

Adding Home Locations

To add a home location, you need to know the service set identifier (SSID) of the access point at the home location.

You can optionally include the following information when adding a home location:

- Basic service set identifier (BSSID)
- Cellular service provider
- Location area code (LAC)
- Cellular identification number of your mobile device

If you do not include the SSID when adding a home location, the home location does not get sent to the Connect Platform on the mobile device.

To add a home location:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, click **Add**. The **Add Home Location** page displays.
4. In the **Name** field, type the name of the home location. The name can be up to 50 alphanumeric characters long and can contain spaces, apostrophes (‘), hyphens (-), and underscores (_).
5. In the **SSID** field, type the SSID of the access point of the home location. The SSID can be up to 50 alphanumeric characters long and can contain spaces, apostrophes (‘), hyphens (-), and underscores (_).
6. (Optional) In the **BSSID** field, type the BSSID of the access point.
7. (Optional) In the **Name** list, select your cellular service provider.
8. (Optional) In the **LAC** field, type the LAC of the mobile device.
9. (Optional) In the **Cell ID** field, type the identification number of your mobile device.
10. Click **Apply** to save your changes.

11. The applicable codecs display in the table. Use the Up or Down buttons to select the highest priority codec supported by both ends. Move the codecs into their appropriately ranked order for usage, the top codec being the highest priority. To modify the packet duration of a codec:

    a. Select the codec from the table.

    b. Click **Modify**.

    c. Modify the packet duration.

    d. Click **Apply** to save changes and return to the main screen.

12. A cellular home location may be added or deleted. To add a cellular home location, refer to "Adding Cellular Information to a Home Location" on page 170.
13. A Wi-Fi home location may be added or deleted. To add a cellular home location, refer to "Adding Wi-Fi Information to a Home Location" on page 171.

Modifying Home Location General Settings

A home location's general settings determine when handovers between Wi-Fi and cellular networks occur. General settings include the following values:

- Min Wi-Fi to Cellular Roam RSSI—Minimum Wi-Fi received signal strength indication (RSSI) threshold below which a call is handed over from Wi-Fi to cellular.
- Min Cellular to Wi-Fi Roam RSSI—Minimum Wi-Fi RSSI threshold that must be available for a call to be handed over from cellular to Wi-Fi.
- Min Voice RSSI—Minimum RSSI threshold for incoming and outgoing voice calls.
- Max Packet Loss %—Maximum average percentage of voice packet loss allowed before the call is handed over to the cellular network.

Note

The general settings for a home location are predefined when you create a home location.

To modify home location general settings:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, select the home location whose general settings you want to modify.
4. In the **General** area, you can modify the following values:

    - **Min Wi-Fi to Cellular Roam RSSI**—Minimum Wi-Fi received signal strength indication (RSSI) threshold below which a call is handed over from Wi-Fi to cellular. The valid value range is -95 through -40, and the default value is -76.
    - **Min Cellular to Wi-Fi Roam RSSI**—Minimum Wi-Fi RSSI threshold that must be available for a call to be handed over from cellular to Wi-Fi. The valid value range is -95 through -40, and the default value is -70.

- **Min Voice RSSI**—Minimum RSSI threshold for incoming and outgoing voice calls. This value represents the minimum RSSI allowed for initiating a voice call. If this value is not met or exceeded, then Wi-Fi is not available. The valid value range is -95 through -40, and the default value is -72.
- **Max Packet Loss %**—Maximum average percentage of voice packet loss allowed before the call is handed over to cellular. If average packet loss exceeds this value, the call is handed over to the cellular network if it is available. The valid value range is 0 through 100%, and the default value is 10%.

5. Click **Apply** to save your changes.

Deleting Home Locations

If you no longer want to include a home location as part of a user profile, you can delete the home location. If you have only one home location defined and delete it, any calling rules or call routing options that use a home location as criteria will no longer be activated when you are in proximity of the home location.

To delete a home location:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, select the home location that you want to delete.
4. Click **Delete**. The home location is deleted.

Adding Cellular Information to a Home Location

You can add the following cellular information to a home location:

- Cellular service provider
- Location area code (LAC)
- Cellular identification number

If you do not have easy access to the LAC and cellular identification number for the mobile device, the user can use the Connect Platform to manage the home locations.

To add home cellular information:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, select the home location to which you want to add the cellular information.
4. In the **Cellular** area, click Add. The Add Cellular Home Location page displays.
5. In the **Name** list, select the user's cellular service provider.
6. In the **LAC** field, type the LAC, which is a unique number that is assigned to a location area.
7. In the **Cell ID** field, type the identification number of the mobile device.
8. Click **Apply** to save your changes.

Deleting Cellular Information from a Home Location

You can delete the cellular information from the home location.

To delete home cellular information:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, select the home location for which you want to delete the cellular information.
4. In the **Cellular** area, click **Delete**. The cellular information is deleted.

Adding Wi-Fi Information to a Home Location

If a home location has multiple access points, you can add the SSID for each access point to the home location. You can optionally include BSSID information, but it is not required.

To add Wi-Fi information to a home location:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, select the home location to which you want to add the Wi-Fi information.
4. In the **Wi-Fi** area, click **Add**. The Add Wi-Fi Home Location page displays.
5. In the **SSID** field, type the SSID of the access point.
6. (Optional) In the **BSSID** field, type the BSSID of the access point.
7. Click **Apply** to save your changes.

Deleting Wi-Fi Information from a Home Location

If a home location no longer uses an access point that you defined for that location, you can remove it from the home location.

To delete home Wi-Fi information:

1. Click **Configuration > Groups and Users > Users**.
2. Click the **Home Locations** tab.
3. In the **Name** area, select the home location to which you want to add the Wi-Fi information.
4. In the **Wi-Fi** area, click **Delete**. The Wi-Fi information is deleted.

Configuring User Options

Click the **Configuration > Groups and Users > Users > Options** tab to configure the following user options:

Call Routing

To configure Call Routing:

1. Select **Wi-Fi** to allow users to utilize Wi-Fi networks for voice calls. Click the **Remote Access link** to go to the **Remote Access** page to configure Remote settings including protocols, and options. Refer to "Managing Remote Access" on page 40 for details.
2. Select **Cellular Data** to allow users to utilize cellular data networks for voice calls.
3. Select **Cellular Voice** to allow users to utilize the regular cellular network for voice calls.
4. Select **Cellular Data Roaming**—Select to users to utilize packet-data networks for voice when the mobile device is roaming.
5. Select **Cellular Voice Roaming**—Select to allow users to utilize the regular cellular network for voice calls when the mobile device is roaming.

Note

Some mobile devices, such as Apple iOS devices, cannot detect when the device is roaming. Enabling/Disabling Cellular Data Roaming and Cellular Voice Roaming will not be recognized by these devices. Instead, the administrator may need to enable or disable the regular Cellular Data and/or Cellular Voice networks for those users individually or move the user into a special Group with the desired settings for those devices.

Data Services

In the **Data Services** area, specify whether users in the group can access secure enterprise services from cellular packet-data networks and remote Wi-Fi networks.

1. **Cellular Data** —Select to allow users to access secure enterprise services from cellular packet-data networks.
2. **Cellular Data Roaming**—Select to access to data services from cellular data networks when the mobile device is roaming.

By default, these options are not enabled. You can enable one or both options.

Note

Some mobile devices, such as Apple iOS devices, cannot detect when the device is roaming. Enabling/Disabling Cellular Data Roaming and Cellular Voice Roaming will not be recognized by these devices. Instead, the administrator may need to enable or disable the regular Cellular Data and/or Cellular Voice networks for those users individually or move the user into a special Group with the desired settings for those devices.

Presence/IM

Enable or disable Presence on the user devices in this group. By default, **Presence/IM** is disabled. If Presence is enabled, options pop up to control whether Presence/IM is available when the device is roaming:

1. **Cellular Data**—Select to allow Presence/IM information to utilize the cellular data networks.
2. **Cellular Data Roaming**—Select to allow Presence/IM information to utilize the cellular data networks when the mobile device is roaming.

Note

Some mobile devices, such as Apple iOS devices, cannot detect when the device is roaming. Enabling/Disabling Cellular Data Roaming and Cellular Voice Roaming will not be recognized by these devices. Instead, the administrator may need to enable or disable the regular Cellular Data and/or Cellular Voice networks for those users individually or move the user into a special Group with the desired settings for those devices.

Enterprise Cellular Call Routing

1. To configure Enterprise Cellular Call Routing, specify how direct cellular calls are routed.
   - Select **Mobile to Fixed Reverse Dial** to enable Mobile to Fixed Reverse Dial for this user. This enables a client from a cellular network to request the Mobility Router (the “fixed” location in the system) to place an outgoing call on the client’s behalf. The client will either send the request using cellular data, or by calling the Reverse Dial Number. When the Mobility Router receives the request, it first calls the client's cell number to establish a voice path to the client, then calls the remote party to connect with the client. In this case, the original call, which would have been dialed from Mobile device (Client) to the Fixed network (Mobility Router), is now being dialed from the Fixed network (Mobility Router) to the Mobile device (Client).

Note

Changing the **Initial Call Setting** after provisioning does not change the client running the configuration.

Notes

If the **Mobile to Fixed Reverse Dial Mode** is set to **Auto**, reverse dial is automatically triggered when the following conditions are met:

- A non-U.S.-based SIM is roaming. For example, if a user with a United Kingdom SIM card is travelling outside the country.
- A Non-U.S.-based SIM is not roaming and is without a country-specific access number available. For example, if a user with a United Kingdom SIM is in the UK, but there is no local UK access number.

- Select **Fixed to Mobile Reverse Dial** to enable the Mobility Router (the "fixed" location in the system) to notify a device using the Connect Platform in the cellular network of an incoming call through cellular packet data service. The Client calls the Mobility Router's Reverse Dial Access Number to pick up the call. In this case, the original call, which would have been dialed from Fixed network (Mobility Router) to the Mobile device (Client), is now being dialed from the Mobile device (Client) to the Fixed network (Mobility Router).
- Select a **Fallback Option** in the event the Fixed to Mobile Reverse Dial call does not connect in time:
  - **Forward Dial** - the Mobility Router tries to connect the call by directly calling the Platform cellular number. If this Fallback Option is selected but the call does not connect, the Mobility Router connects the remote party to the user's enterprise voice mail.
  - **Voice Mail** - the Mobility Router connects the remote party to the user's enterprise voice mail.

2. Select one of the following to specify how outgoing cellular calls are routed:
   - **Route all outgoing calls through the enterprise**—Select to route all outgoing cellular calls through the enterprise. By default, this option is selected.
   - **Route all outgoing calls directly over cellular**—Select to route all outgoing cellular calls directly over the cellular network (not routed through the enterprise).
   - **Route all outgoing calls directly over cellular except**—Select to route certain cellular calls through the enterprise. If you select this option, the following sub options are available:
     - **From nearby home or office location**—Select to route calls made when close to a home location or an enterprise Wi-Fi network through the enterprise. Clear this option to route these calls directly through the cellular network. By default, this option is selected.

- **Enterprise extensions**—Select to route enterprise extensions through the enterprise. By default, this option is selected.

WARNING!

Clearing the Enterprise extensions option disables users from dialing just the extension when calling enterprise phone numbers. In this case, Users need to dial the 7- or 10-digit phone number.

- **International numbers**—Select to route outgoing international numbers through the enterprise. Clear this option to have international calls go directly over the cellular network. By default, this option is selected.

Enterprise Cellular Call Indicator

To specify an Enterprise Cellular Call Indicator, select one of the following:

- **None**—If you select this option, the Connect Platform cannot distinguish whether calls received while a mobile device is on the cellular network are enterprise calls or direct calls.
- **Prepend Digits to Caller ID** —Select this option to prepend a numeric prefix to the phone number that the Mobility Router sends to the Connect Platform for enterprise calls while the mobile device is on the cellular network.

  If you selected a numbering plan template other than North America in “Configuring IP-PBX General Settings” on page 98, the Use Prefix option is automatically selected.

  The prefix can be a number up to five digits long.
- **Map Used to Unused Area Codes (North America Only)** —Select this option to have the Mobility Router automatically map the phone number for enterprise calls sent to the Connect Platform when the mobile device is on the cellular network. This is the default option if you selected North America as the numbering plan template in “Configuring IP-PBX General Settings” on page 98.
- **Use Numbering Plan “Enterprise Full Number Pattern” Table** — Select this option to define the call. When enabled, the Mobility Router downloads the table of enterprise anchored number patterns to the clients, so that the Connect Platform can detect if a received call is anchored to the enterprise or is a personal/direct call. If using this option, the numbers used in Cellular Caller ID Mapping and Enterprise Full Number Pattern must match (Configuration > Voice > IP-PBX > Numbering Plan > Advanced page - refer to “Cellular Caller ID Mapping” on page 110 and “Enterprise Full Number Pattern” on page 111for configuration information).

Cellular Voice Mail Indicator

Select the **Cellular Voice Mail Indicator** check box to enable the enterprise voice mail message indicator on the mobile device when it is on the cellular network. By default, this option is enabled. If you do not select this option and users receive enterprise voice mail while on the cellular network, no voice mail indicator displays on the mobile device.

Note

If the Connect Platform is registered with the Mobility Router via cellular data (not on Wi-Fi), the Mobility Router sends the MWI notification when the client is on the cellular network. In this case, enabling the Cellular Voice Mail Indicator check box is not required.

Call Ignore

Select **Ignore call on all shared line devices** to ensure the mobile device and all other devices that share the same line immediately stop ringing when a user selects to ignore an incoming call on the mobile device. If this option is not selected and the user chooses to ignore an incoming call on the mobile device, the other devices sharing the same line continue to ring until the maximum ring time configured on the PBX is reached. If none of the other devices answers the call within the maximum ring time, the call is then forwarded to voice mail.

Note

The Call Ignore feature is available on VoIP calls only.

Note

When a user has multiple devices, the Call Ignore feature applies to all devices.

Note

Configure voice mail on the IP-PBX for this option to be effective. If voice mail is not configured on the IP-PBX, the call is not sent to voice mail.

Client Privilege

Assign a **Client Privilege** to this device. Select **Full** to show all menus and enable exiting.

Provisioning

In the Provisioning area, check the **Prevent users from changing devices by re-provisioning** box to disallow users from provisioning with their credentials on another phone. The default is read from the selection in the Groups area. In association with this feature, if the maximum number of devices per user has been reached, use **Configuration > Users > (select Modify)> Devices** tab to specify a device to delete. This allows the new device to be provisioned. For more information about deleting a device, refer to “Configuring Additional Devices” on page 163.

Applying Changes

Click **Apply** to save your changes.

Modifying Users

To modify a user:

1. Click **Configuration > Groups and Users > User**. The **User** page displays.
2. Select the user to be modified
3. Click **Modify**. The **Modify User** page displays.
4. Make any necessary changes. Click **Apply** on each tab to save the changes.

WARNING!

If you make changes to a user configuration, the user must restart the Connect Platform application before their service can continue. Any configuration change made to the user parameters affects calls being routed to the Connect Platform and the Client's handover behavior. If you change any user settings, the user must exit and restart the Connect Platform application to register to the Mobility Router again.

Enabling and Disabling Multiple Users

When creating or modifying a user, you can enable or disable the user. After you have created users (or they have been created by user provisioning), you can enable or disable multiple users without modifying each user individually.

To enable multiple users:

1. Click **Configuration > Groups and Users > User**. The **User** page displays.
2. Select the users that you want to enable.
3. Click **Enable**. The users that you selected are now enabled.

To disable multiple users:

1. Click **Configuration > Groups and Users > User**. The **User** page displays.
2. Select the users that you want to disable.
3. Click **Disable**. The users that you selected are now disabled.

Moving Multiple Users to a Group

When creating or modifying a user, you can move the user to another group. After you have created users (or they have been created by user provisioning), you can move multiple users to a different group without modifying each user individually. Before users can be moved to another group, they must be disabled, which you are prompted to confirm before moving the users.

To move multiple users to a group:

1. Click **Configuration > Groups and Users > User**. The **User** page displays.
2. Select the users that you want to move.
3. In the list that is next to the **Move** button, select the group to which you want to move the **users**.
4. Click Move.
5. When prompted to confirm whether users are disabled and moved to the selected group, click **OK**. The users are moved to the group that you selected.

Copying a User

When creating or modifying a user, you can copy the user to another User ID.

To copy a User:

1. Click **Configuration > Groups and Users > User**. The **User** page displays.
2. Select the user that you want to copy.
3. Select **Copy**.
4. A new User template is created and displays **Copy <User ID>** at the top of the window.
5. Fill in the fields as described in “Creating Users” on page 159 and save. Once the changes are saved, including a new User ID, the name displayed for this user changes from “Copy <User ID>” to the saved name.

Deleting Users

To delete a user:

1. Click **Configuration > Groups and Users > User**. The **User** page displays.
2. Select the user you want to delete.
3. Click **Delete**. The user is deleted.

Finding Users

Mobility Router users can be searched for and discovered based on multiple criteria.

To search for a user:

1. Click **Configuration > Groups and Users > User**. The User page displays.
2. In the **User ID** dropdown window, select the means by which to find the user. The options are **User ID, Device Name, Device ID, Client Version, Device Model, Enterprise Extension, Cellular Number, Group, Full Name, Enterprise Full Number, International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), Provisioning Status, or PBX**.
3. Select the criteria by which to find the user. The options are equal to or contains.
4. Type the appropriate string in the search field and press Enter. All rows containing the configured criteria display in the table.
5. You can click a column heading to alphabetically sort all pages by that criteria. For example, to sort by PBX type, click the PBX column heading to view an alphabetical listing of all PBXs.
6. The current page number displays at the bottom right. Select a new page number to begin with and the number of rows to follow using the Go to page field and the Retrieve pulldown on the bottom right. The valid values are 50, 100 and 500. For example, enter Go to row 101 and select Retrieve 50 to begin sorting the rows on number 101 and end on number 151.
7. Select **Prev** or **Next** to view the pages before or after the current page.
8. Use the **Move** button to move a user to a different group in the table.
9. Click **Clear** to return to the original table.

Viewing Table Rows

Note

Refer to “Copying a Selection” on page 20 for information about how to copy a selection on a page.

Select All Rows

Right-click to select all rows on a page.

Expand/Collapse All

1. Click in the User Summary page.
2. Right-click to **Select All Rows**.
3. Right-click to **Expand All or Collapse All**.

CHAPTER

15

Managing Redundancy Clusters

The Mobility Router provides stateful high availability by using redundancy clusters. A redundancy cluster consists of two Mobility Routers. One Mobility Router is the active (primary) node, and the other Mobility Router is the standby (secondary) node. The standby node becomes the active node if the original active node fails, ensuring that calls are not dropped. This chapter contains the following sections:

About Redundancy Clusters

A redundancy cluster consists of two Mobility Router 4000, 6000. Each redundancy cluster must have a unique cluster name.

Note

Clustering is not supported on Mobility Router 2000 Series appliances.

Failover occurs due to the following:

- The active node is powered off.
- The eth0 interface cable of the active node is removed or disconnected.
- SIP server, Mobility server, Remote Access server, Session Logger server or HMP server failure on the active node.

  In a redundancy cluster, a “heartbeat” packet is sent every two seconds from the active node to the standby node. If the standby node fails to receive five consecutive heartbeats, it becomes the active node, and a failover occurs.

  Redundancy clusters provide the following:

- Synchronization of configuration and state information between the active and standby nodes. The active node sends this information to the standby node. Synchronization occurs due to the following events:
  - A standby node joins the cluster.
  - The standby node becoming the active node.
  - The transition as an active node becomes a standby node.
- The following information is not synchronized:
  - Interface settings
  - Mobility Router certificate
  - Mobility Router logs
- Active calls are not dropped during a failover, including multiple separate calls and conference calls. Calls on hold remain on hold during failover.
  - To maintain media during a failover:
    - For Media bridging through CMR, audio must be removed when a user is registered on remote Wi-Fi.
    - For Media not bridging through CMR, audio must be retained when a user is registered on local Wi-Fi.

- Users retain their registration state after failover.
- CDR information is retained after failover.

Redundancy Cluster Prerequisites

Before you start configuring redundancy clusters, make sure you have the following:

- Two Mobility Router 4000, 6000. Both appliances must be of same model.
  - Each Mobility Router has a unique IP address and hostname.
  - Both Mobility Routers are running the same image of Mobility system software (Version 2.0 or later).
  - Both Mobility Routers are in the same subnet.
- Virtual IP address, which is a separate IP address that the two Mobility Routers share and is the management IP address for the two Mobility Routers
- (Secure Remote Voice and secure enterprise services only) Secure Remote Voice virtual IP address, which is a separate IP address that the two Mobility Routers share. This IP address is the IP address that mobile devices access if the address is publicly accessible. It can also be an internal IP address if you are using NAT on a firewall.
- Verify that the switch ports that are connected to the Mobility Routers meet one of the following requirements:
  - If Spanning Tree Protocol (STP) is enabled on the switch ports that are connected to the Mobility Routers, port fast must also be enabled.
  - STP is disabled on the switch ports that are connected to the Mobility Routers.

Redundancy Cluster Scenarios

How you configure a redundancy cluster depends on the scenario. The following are the scenarios in which a redundancy cluster can be formed:

- Two new or factory-default Mobility Routers that are to be configured as a redundancy cluster. (See “Creating a Cluster with Two New Mobility Routers” on page 184.)
- A Mobility Router has already been configured with users who are provisioned, and you want to add a new Mobility Router to form a cluster. (See “Creating a Redundancy Cluster with a Configured Mobility Router and a New Mobility Router” on page 187.)
- A Mobility Router that has already been configured with provisioned users and is configured for remote access (Secure Remote Voice or secure enterprise services).

Creating a Cluster with Two New Mobility Routers

If you have two new or factory-default Mobility Routers that you want to configure as a cluster, you perform the following tasks for each Mobility Router.

Configuring the First Mobility Router

To create a redundancy cluster, perform the following tasks for the first Mobility Router:

1. Initially configure the Mobility Router and establish it in your network using the Initial Configuration Wizard. For more information, see “Initially Configuring and Establishing Network Connectivity” on page 184.
2. Generate or import the following:
   - Certificate authority (CA)
   - Mobility Router certificate

   For more information, see “Configuring Certificates for the Mobility Router” on page 184.
3. Configure redundancy cluster settings and enable the cluster. For more information, see “Configuring Redundancy Cluster Settings” on page 185.
4. When prompted, restart the Mobility Router services.

   The first Mobility Router that you configure becomes the active node in the cluster.

Initially Configuring and Establishing Network Connectivity

Before you can join a redundancy cluster, you must initially configuring the first Mobility Router with the Initial Configuration Wizard, verify that the Mobility Router has network connectivity.

Configuring Certificates for the Mobility Router

Generate certificates in the following order:

1. Certificate authority—For more information, see “Importing a Certificate Authority” on page 61 or “Importing a Certificate Authority” on page 61.
2. Mobility Router certificate—For more information, see “Generating a Mobility Router Certificate” on page 64 and “Importing a Certificate to the Mobility Router” on page 66.

After generating these certificates, you must configure the redundancy cluster settings, as described in “Configuring Redundancy Cluster Settings” on page 185.

Configuring Redundancy Cluster Settings

To configure redundancy cluster settings:

1. Login to the first Mobility Router.
2. Click **Configuration > Clustering > Redundancy**. The Redundancy page displays.
3. Select the **Enabled** check box to enable redundancy on this Mobility Router.
4. In the **Name** field, type the name of the redundancy cluster. The name can be up to 50 characters long and cannot contain any special characters except for spaces, hyphens (-), and underscores (_).

   Make sure that the name for the redundancy cluster is unique for each cluster. If you already have a redundancy cluster and are creating another cluster, the name of the new cluster must be different from the existing cluster.
5. In the **Virtual IP Address** field for eth0 and eth1, type the shared IP address, and select the subnet mask from the list.

   This IP address is the management address you access when you need to configure the redundancy cluster. This is the IP address that mobile devices and the IP-PBX communicate with, rather than one of the individual physical IP addresses.
6. To save your changes, click **Apply**.
7. The **Services Restart** message displays. If selected, you are prompted with another message depending on Mobility Router joining or leaving the cluster. If joining, “Wait for Mitel Mobility Router to join the cluster” displays. If leaving the cluster, “Wait for Mitel Mobility Router to leave the cluster” displays. Mobility Router services automatically restart.

You can verify the state of the redundancy cluster by selecting **Monitor > Clustering > Redundancy**. The first Mobility Router is now the active node in the cluster.

Now that you have configured the first Mobility Router to create the redundancy cluster, you add the second Mobility Router to the cluster, as described in “Configuring the Second Mobility Router” on page 190.

Configuring the Second Mobility Router

After creating the redundancy cluster with the first Mobility Router, perform the following tasks on the second Mobility Router:

1. Initially configure the Mobility Router and establish it in your network using the Initial Configuration Wizard. For more information, see “Initially Configuring and Establishing Network Connectivity” on page 186.
2. Configure redundancy cluster settings and enable the cluster. For more information, see “Configuring Redundancy Cluster Settings” on page 185.
3. When prompted, restart the Mobility Router services.

Initially Configuring and Establishing Network Connectivity

Before you can create a redundancy cluster, you must initially configure the second Mobility Router with the Initial Configuration Wizard and verify that the Mobility Router has network connectivity.

Configuring Redundancy Cluster Settings

To configure redundancy cluster settings:

4. Login to the first Mobility Router.
5. Click **Configuration > Clustering > Redundancy**. The **Redundancy** page displays.
6. Select the **Enabled** check box to enable redundancy on this Mobility Router.
7. In the **Name** field, type the name of the redundancy cluster. The name can be up to 50 characters long and cannot contain any special characters except for spaces, hyphens (-), and underscores (_). Make sure that the name for the redundancy cluster is unique for each cluster. If you already have a redundancy cluster and are creating another cluster, the name of the new cluster must be different from the existing cluster.
8. In the **Virtual IP Address** field, type the shared IP address, and select the subnet mask from the list. This IP address is the management address you access when you need to configure the redundancy cluster. This is the IP address that mobile devices and the IP-PBX communicate with, rather than one of the individual physical IP addresses.
9. To save your changes, click **Apply**.
10. The **Services Restart** message displays. If selected, you are prompted with another message depending on Mobility Router joining or leaving the cluster. If joining, “Wait for Mitel Mobility Router to join the cluster” displays. If leaving the cluster, “Wait for Mitel Mobility Router to leave the cluster” displays. Mobility Router services automatically restart.

You can verify the state of the redundancy cluster by selecting **Monitor > Clustering > Redundancy**. The second Mobility Router is now the standby node in the cluster.

You can now make configuration changes to cluster nodes from the virtual IP address of the redundancy cluster. For more information, see “Managing Redundancy Clusters” on page 196.

Creating a Redundancy Cluster with a Configured Mobility Router and a New Mobility Router

If you have a Mobility Router that is already configured with users with mobile devices who are currently provisioned, you can preserve the configuration of that Mobility Router when creating a redundancy cluster. To preserve the existing configuration of the Mobility Router, you need to do the following:

- Disable all existing users on the Mobility Router.
- Change the eth0 IP address and hostname for the Mobility Router.
- Specify the existing eth0 IP address of the Mobility Router as the virtual IP address of the redundancy cluster.
- Specify the hostname of the Mobility Router as the redundancy cluster name.
- Use the certificate for the Mobility Router as the virtual certificate for the redundancy cluster.

If you do not follow the previous steps when creating the redundancy cluster, the existing configuration of the Mobility Router is lost, and you will need to recreate configuration of the Mobility Router. Any provisioned users no longer have access to Connect Platform features until you recreated the configuration on the Mobility Router.

Reconfiguring the Previously Configured Mobility Router

1. Perform the following tasks to reconfigure the previously configured Mobility Router in preparation of creating a redundancy cluster:
2. Disable all existing users on the Mobility Router. For more information, see “Disabling All Existing Users” on page 188.
3. Change the eth0 IP address and hostname for the Mobility Router. For more information, see “Changing the Hostname and IP Address of the Mobility Router” on page 188.
4. Copy the Mobility Router certificate and import it as the Mobility Router virtual certificate. For more information, see “Importing the Existing Mobility Router Certificate as the Virtual Certificate” on page 188.
5. Configure redundancy cluster settings and enable the cluster:
   - Specify the original hostname of the Mobility Router as the redundancy cluster name.
   - Specify the original Mobility Router IP address as the virtual IP address.
   - When prompted, restart the Mobility Router.

   For more information, see “Configuring Redundancy Cluster Settings” on page 185.
6. Enable all the existing users. For more information, see “Enabling Existing Users” on page 189.

Disabling All Existing Users

To preserve the existing user configurations after creating the redundancy cluster, you must disable all the existing users on the Mobility Router:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select all users.
3. Click **Disable**. All the users are disabled.

Note

If there are multiple pages of existing users, complete this action for each page.

Now you must change the IP address and hostname of the Mobility Router, as described in "Changing the Hostname and IP Address of the Mobility Router" on page 188.

Changing the Hostname and IP Address of the Mobility Router

To preserve the existing Mobility Router configuration and avoid having to reconfigure the Mobility Router after creating the redundancy cluster, you must change the hostname and eth0 IP address of the Mobility Router. Make sure that you note the original hostname and IP address, as you will need to specify them when configuring redundancy cluster settings.

To change the hostname and IP address of the Mobility Router:

1. Click **Configuration > System > Networking > Hostname/DNS**. The **Hostname/DNS** page displays.
2. In the **Hostname/DNS** field, type the new Mobility Router hostname. The hostname can be up to 64 alphanumeric characters long and can contain spaces, hyphens (-), and underscores (_).
3. Click **Apply**.
4. Click **Configuration > System > Networking > Interface**. The Interface page displays.
5. On the **eth0** tab, change the IP address of the eth0 interface, and select a subnet mask.
6. Click **Apply**.
7. If you have Secure Remote Voice and secure enterprise services configured, change the IP address of the eth1 interface on the **eth1** tab, and select a subnet mask.
8. To save your changes, click **Apply**.

Importing the Existing Mobility Router Certificate as the Virtual Certificate

You must copy the existing Mobility Router certificate and import it as the Mobility Router virtual certificate:

1. Click **Configuration > System > Certificate > Mobility Router > Clustered.** The **Mobility Router** page displays.
2. If a certificate was imported for **Mobility Router > Standalone > Local Access**, the same procedure is followed. If a certificate was not imported, create a new certificate under **Mobility Router > Clustered, as** shown in “Generating a Mobility Router Certificate” on page 64.
3. Restart the Mobility service and activate the newly generated certificate.
4. Refresh the browser to regain access, then log in.

You now need to configure the redundancy cluster settings, as described in “Configuring Redundancy Cluster Settings” on page 185.

Configuring Redundancy Cluster Settings

After importing the Mobility Router virtual certificate, configure the redundancy cluster settings:

1. Click **Configuration > Clustering > Redundancy**. The Redundancy page displays.
2. Select the **Enabled** check box to enable redundancy on this Mobility Router.
3. In the **Name** field, type the original hostname of the Mobility Router.
4. In the **Virtual IP Address** field, type the original IP address of the Mobility Router, and select the subnet mask from the list.

   This IP address is the management address you access when you need to configure the redundancy cluster. This is the IP address that mobile devices and the IP-PBX communicate with, rather than one of the individual physical IP addresses. By using the original IP address of the Mobility Router, you do not need to make any changes on the IP-PBX or reprovision mobile devices.
5. Click **Apply** to save your changes. The **Services Restart** message displays. If selected, you are prompted with another message depending on Mobility Router joining or leaving the cluster. If joining, “Wait for Mitel Mobility Router to join the cluster” displays. If leaving the cluster, “Wait for Mitel Mobility Router to leave the cluster” displays. Mobility Router services automatically restart.

   You can verify the state of the redundancy cluster by selecting **Monitor > Clustering > Redundancy**. The first Mobility Router is now the active node in the cluster.

   Now that you have configured the first Mobility Router to create the redundancy cluster, you need to enable the users again, as described in “Enabling Existing Users” on page 189.

Enabling Existing Users

To enable users:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select all users.

3. Click **Enable**. All the users are enabled.

After enabling existing users, you now need to configure the second Mobility Router, as described in “Configuring the Second Mobility Router” on page 190.

Configuring the Second Mobility Router

After configuring the first Mobility Router of the redundancy cluster, perform the following tasks on the second Mobility Router:

1. Initially configure the Mobility Router and establish it in your network using the Initial Configuration Wizard. For more information, see “Initially Configuring and Establishing Network Connectivity” on page 184.
2. Configure redundancy cluster settings and enable the cluster. For more information, see “Configuring Redundancy Cluster Settings” on page 185.
3. When prompted, restart the Mobility Router services. For more information, see “Initially Configuring and Establishing Network Connectivity” on page 184.

Initially Configuring and Establishing Network Connectivity

Before you can create a redundancy cluster, you must initially configure the second Mobility Router with the Initial Configuration Wizard and verify that the Mobility Router has network connectivity. For information about initially configuring the Mobility Router, see the *Mobility Router Hardware Installation Guide*.

Configuring Redundancy Cluster Settings

To configure redundancy cluster settings:

1. Log in to the first Mobility Router.
2. Click **Configuration > Clustering > Redundancy**. The **Redundancy** page displays.
3. Select the **Enabled** check box to enable redundancy on this Mobility Router.
4. In the **Name** field, type the name of the redundancy cluster. The name can be up to 50 characters long and cannot contain any special characters except for spaces, hyphens (-), and underscores (_).
5. Make sure that the name for the redundancy cluster is unique for each cluster. If you already have a redundancy cluster and are creating another cluster, the name of the new cluster must be different from the existing cluster.
6. In the **Virtual IP Address** field, type the shared IP address, and select the subnet mask from the list.
7. This IP address is the management address you access when you need to configure the redundancy cluster. This is the IP address that mobile devices and the IP-PBX communicate with, rather than one of the individual physical IP addresses.

8. To save your changes, click **Apply**.
9. The **Services Restart** message displays. If selected, you are prompted with another message depending on Mobility Router joining or leaving the cluster. If joining, “Wait for Mitel Connect Mobility Router to join the cluster” displays. If leaving the cluster, “Wait for Mitel Connect Mobility Router to leave the cluster” displays. Mobility Router services automatically restart.

   You can verify the state of the redundancy cluster by selecting **Monitor > Clustering > Redundancy**. The second Mobility Router is now the standby node in the cluster.

   You can now make configuration changes to the virtual IP address of the redundancy cluster. For more information, see “Managing Redundancy Clusters” on page 196.

Creating a Redundancy Cluster with a Configured Mobility Router with Remote Access and a New Mobility Router

If you have a Mobility Router that is already configured with users with mobile devices who are currently provisioned, you can preserve the configuration of that Mobility Router when creating a redundancy cluster. To preserve the existing configuration of the Mobility Router, you need to do the following:

- Disable all existing users on the Mobility Router.
- Change the eth0 IP address and hostname for the Mobility Router.
- If the Mobility Router has Secure Remote Voice and secure enterprise services configured using the eth1 interface, change the IP address of the eth1 interface.
- Specify the existing eth0 IP address of the Mobility Router as the virtual IP address of the redundancy cluster.
- Specify the hostname of the Mobility Router as the redundancy cluster name.
- Use the certificate for the Mobility Router as the virtual certificate for the redundancy cluster.
- If the Mobility Router has Secure Remote Voice and secure enterprise services configured using the eth1 interface, specify the original eth1 IP address as the remote access virtual IP address. For information about setting the remote access virtual IP address, see “Configuring General Settings” on page 47.

If you do not follow the previous steps when creating the redundancy cluster, the existing configuration of the Mobility Router is lost, and you will need to recreate configuration of the Mobility Router. Any provisioned users no longer have access to Connect Platform features until you recreated the configuration on the Mobility Router.

Initially Configuring the New Mobility Router

After configuring the first Mobility Router of the redundancy cluster, configure the Mobility Router and establish it in your network using the Initial Configuration Wizard. For more information, see “Initially Configuring and Establishing Network Connectivity” on page 186.

Establishing Network Connectivity

Before you can create a redundancy cluster, you must initially configure the second Mobility Router with the Initial Configuration Wizard and verify that the Mobility Router has network connectivity. For information about initially configuring the Mobility Router, see the *Mobility Router Hardware Installation Guide*.

Reconfiguring the Previously Configured Mobility Router

Perform the following tasks to reconfigure the previously configured Mobility Router in preparation of creating a redundancy cluster:

1. Disable all existing users on the Mobility Router. For more information, see “Disabling All Existing Users” on page 188.
2. Change the eth0 IP address and hostname for the Mobility Router. If you are using Secure Remote Voice and secure enterprise services, you also need to change the eth1 IP address. For more information, see “Changing the Hostname and IP Address of the Mobility Router” on page 188.
3. Import the Mobility Router virtual certificate as described in “Importing the Existing Mobility Router Certificate as the Virtual Certificate” on page 188.
4. Configure redundancy cluster settings and enable the cluster:
   - Specify the original hostname of the Mobility Router as the redundancy cluster name.
   - Specify the original Mobility Router IP address as the virtual IP address.
   - When prompted, restart the Mobility Router.

   For more information, see “Configuring Redundancy Cluster Settings” on page 185.
5. Enable all the existing users. For more information, see “Enabling Existing Users” on page 189.

Disabling All Existing Users

To preserve the existing user configurations after creating the redundancy cluster, you must disable all the existing users on the Mobility Router:

1. Click **Configuration > Groups and Users > Users**. The **Users** page displays.
2. Select all users.
3. Click **Disable**. All the users are disabled.

Now you must change the IP address and hostname of the Mobility Router, as described in “Changing the Hostname and IP Address of the Mobility Router” on page 188.

Changing the Hostname and IP Address of the Mobility Router

To preserve the existing Mobility Router configuration and avoid having to reconfigure the Mobility Router after creating the redundancy cluster, you must change the hostname and eth0 IP address of the Mobility Router. Make sure that you note the original hostname and IP address, as you will need to specify them when configuring redundancy cluster settings.

If the Mobility Router has Secure Remote Voice and secure enterprise services configured using the eth1 interface, you also need to change the eth1 interface. Make a note of the original IP address, as you will need to specify it as the remote access virtual IP address after the second Mobility Router joins the redundancy cluster.

To change the hostname and IP address of the Mobility Router:

1. Click **System > Networking > Express Setup**. The **Express Setup** page displays.
2. In the **Hostname** field, type the new Mobility Router hostname. The hostname can be up to 64 alphanumeric characters long and can contain spaces, hyphens (-), and underscores (_).
3. In the eth0 IP Address area, change the IP address of the eth0 interface, and select a subnet mask.
4. If you have Secure Remote Voice and secure enterprise services configured, change the IP address of the eth1 interface, and select a subnet mask.
5. To save your changes, click **Apply**.

Importing the Existing Mobility Router Certificate as the Virtual Certificate

You must copy the existing Mobility Router certificate and import it as the Mobility Router virtual certificate:

1. Click **Configuration > System > Certificate > Mobility Router**. The Mobility Router page displays.
2. Select all the text of the certificate.
3. Right-click and select Copy.
4. Click **Configuration > System > Certificate > Mobility Router > Clustered > Local Access (Virtual)**.
5. Click **Import**.
6. Click in the text box to make it active.
7. Right-click and select Paste to paste the certificate text into the text box.

8. Click **Import**. If the certificate is valid, a Restart prompt displays. If the certificate is not valid, an Error prompt displays. In the case of an error, generate a valid certificate or obtain a new certificate to paste in the field.

9. Restart the Mobility service and activate the newly generated certificate, click **OK**.

Note

If you do not want to restart the Mobility Router, click Cancel. The newly generated certificate is stored on the Mobility Router until the next restart.

10. Refresh the browser to regain access, then log in. Optionally, click **Verify** to view if the certificate is valid.

You now need to configure the redundancy cluster settings, as described in “Configuring Redundancy Cluster Settings” on page 186.

Configuring Redundancy Cluster Settings

After importing the Mobility Router virtual certificate, configure the redundancy cluster settings:

1. Click **Configuration > Clustering > Redundancy**. The Redundancy page displays.

2. Select the **Enabled** check box to enable redundancy on this Mobility Router.

3. In the **Name** field, type the original hostname of the Mobility Router.

4. In the **Virtual IP Address** field, type the original IP address of the Mobility Router, and select the subnet mask from the list.

This IP address is the management address you access when you need to configure the redundancy cluster. This is the IP address that mobile devices and the IP-PBX communicate with, rather than one of the individual physical IP addresses. By using the original IP address of the Mobility Router, you do not need to make any changes on the IP-PBX or reprovision mobile devices.

5. To save your changes, click **Apply**.

6. The **Services Restart** message displays. If selected, you are prompted with another message depending on Mobility Router joining or leaving the cluster. If joining, “Wait for Mitel Mobility Router to join the cluster” displays. If leaving the cluster, “Wait for Mitel Mobility Router to leave the cluster” displays. Mobility Router services automatically restart.

You can verify the state of the redundancy cluster by selecting **Monitor > Clustering > Redundancy**. The first Mobility Router is now the active node in the cluster.

Now that you have configured the first Mobility Router to create the redundancy cluster, you need to enable the users again, as described in “Enabling Existing Users” on page 189.

Enabling Existing Users

To enable users:

1. Click **Configure > Groups and Users > Users**. The Users page displays.

2. Select all users.
3. Click **Enable**. All the users are enabled.

After enabling existing users, you now need to configure the second Mobility Router, as described in “Configuring the Second Mobility Router” on page 190.

Adding the Second Mobility Router to the Redundancy Cluster

After configuring the first Mobility Router of the redundancy cluster, perform the following tasks on the second Mobility Router:

1. Configure redundancy cluster settings and enable the cluster.
2. When prompted, restart the Mobility Router services.

Configuring Redundancy Cluster Settings

To configure redundancy cluster settings:

1. Log in to the first Mobility Router.
2. Click **Configuration > Clustering > Redundancy**. The Redundancy page displays.
3. Select the **Enabled** check box to enable redundancy on this Mobility Router.
4. In the **Name** field, type the name of the redundancy cluster. The name can be up to 50 characters long and cannot contain any special characters except for spaces, hyphens (-), and underscores (_). Make sure that the name for the redundancy cluster is unique for each cluster. If you already have a redundancy cluster and are creating another cluster, the name of the new cluster must be different from the existing cluster.
5. In the **Virtual IP Address** field, type the shared IP address, and select the subnet mask from the list. This IP address is the management address you access when you need to configure the redundancy cluster. This is the IP address that mobile devices and the IP-PBX communicate with, rather than one of the individual physical IP addresses.
6. To save your changes, click **Apply**.
7. The **Services Restart** message displays. If selected, you are prompted with another message depending on Mobility Router joining or leaving the cluster. If joining, “Wait for Mitel Connect Mobility Router to join the cluster” displays. If leaving the cluster, “Wait for Mitel Connect Mobility Router to leave the cluster” displays. Mobility Router services automatically restart.

You can verify the state of the redundancy cluster by selecting **Monitor > Clustering > Redundancy**. The second Mobility Router is now the standby node in the cluster.

You can now make configuration changes to the virtual IP address of the redundancy cluster. You must specify the original eth1 IP address of the Mobility Router that had remote access configured as the remote access virtual IP address.

To specify the remote access virtual IP address:

1. Click **Configuration > Clustering > Redundancy**. The **Redundancy** page displays.
2. Select **Enable**.
3. In the **Name** field, type the name of the cluster. This should be the same cluster name as the master configuration.
4. In the **Eth0 Virtual IP Address** field or **Eth1 Virtual IP Address** field, type the master eth0 or eth1 virtual IP address of the Mobility Router that had remote access configured (from "Reconfiguring the Previously Configured Mobility Router" on page 192).
5. To save your changes, click **Apply**.

Managing Redundancy Clusters

After you have verified the cluster's status, to make configuration changes to the cluster, access the virtual IP address. Making configuration changes using the virtual IP address ensures that the changes are propagated to the cluster.

You need to directly access the active and standby Mobility Routers for the following tasks:

- Add or delete licenses. For example, add a Secure Remote Voice license to each Mobility Router. Because a license is bound to a Mobility Router MAC address, access the physical IP address of the Mobility Router, rather than access the virtual IP address.
- You need to access logs for a Mobility Router. Logs are maintained on each Mobility Router.
- You need to add a Mobility Router certificate.
- Enable and Disable of the cluster.

Removing a Second Mobility Router from Redundancy Cluster

Mobility Routers in a Standby node may be removed from the Redundancy Cluster. This node will fall out of the Cluster.

1. Login to the Standby Mobility Router using the physical IP address of the Standby box.
2. Click **Monitor > Clustering > Redundancy** to verify the IP addresses of the Master and Standby Mobility Routers.
3. Go to/launch the Standby Mobility Router. Click **Configuration > Clustering**. Clear **Enable** to disable the Clustering settings.

4. A prompt “Standby server’s configuration will be set to default. Continue?” displays. Click **OK** to continue. After the standby Mobility Router is removed from the cluster, it reboots with a base configuration including license and networking information.
5. A prompt “Wait for Mitel Connect Mobility Router to leave the cluster” message displays. Click **OK** to continue.
6. Click **Monitor > Clustering** to verify the Standby Mobility Router has been removed from the cluster. You may need to click **Refresh**.

Upgrading Redundancy Clusters

Mitel recommends upgrading the Standby Mobility Router first, followed by the Master Mobility Router.

1. Login to the Standby Mobility Router using the physical IP address of the Standby box.
2. Click **Maintenance > Images > Mobility Router** to install the new image.
3. Once the new image is installed, select the new image and click **Set Next Boot**. After the new image is selected for the Next Boot, click the **Reboot** button to boot the standby with the new image. After rebooting, go to **Monitor > Clustering** to verify the newly rebooted Mobility Router comes on and joins as the Standby.
4. After 5 minutes, upgrade and then reboot the current Master Mobility Router. While this Master Mobility Router is in the process of rebooting, the newly upgraded Standby Mobility Router becomes the new Master Mobility Router. When the previous Master finishes its rebooting cycle, it joins as the Standby.

Monitoring Cluster Status

After you have configured the redundancy cluster, you can monitor its status. The Redundancy monitoring page allows you to check the state of each Mobility Router and which one is the active node.

Troubleshooting

The following lists issues you might encounter after implementing redundancy clusters and how to verify your configuration.

The second Mobility Router fails to join the cluster and is in the Unknown state.

Both Mobility Routers are in the active state.

Communication between the active and standby nodes is required to maintain the redundancy cluster and provide stateful high availability. Verify that the communication between the two Mobility Routers is active by using the following troubleshooting commands:

- Troubleshooting > Commands > ping
- Troubleshooting > Commands > traceroute

Also verify that PortFast is enabled on the switch ports to which the Mobility Routers are connected.

Connect Platform cannot communicate with the Mobility Router.

During initial provisioning, reprovisioning, or upgrading of the Connect Platform, verify that the Mobility Router IP address specified is the virtual IP address of the redundancy cluster.

In the Connect Platform, verify that the IP address of the Mobility Router in the General preferences is set to the virtual IP address of the redundancy cluster.

End users' mobile devices cannot register to the Mobility Router.

End users do not get a registration icon on the mobile device.

This happens for one of the following reasons:

- The SIP server lost the PBX registration state of the user.
- The standby Mobility Router became the active node in the cluster without a failover occurring.
- The SIP server failed after the user was created but before responding to the registration request to the PBX for the user.

Check the Mobility Router log and search for "503 Policy Check Failure." If you see this message, the SIP server needs to reregister with the PBX to get the new registration state to respond to the client's registration request. To do this, do one of the following:

- Disable the user, and then enable the user again.
- Wait for the timeout of 180 seconds so that the SIP server sends a new PBX registration request.

Users on Wi-Fi calls see delayed response after failover.

If a user is on an active Wi-Fi call when failover occurs, the Connect Platform makes a Hold request to the Mobility Router. It can take at least 6 to 10 seconds for the Mobility Router to receive the request.

This situation occurs when a WLAN controller filters ARP broadcast requests. After switchover, the new active Mobility Router ARP broadcast is not received by the Connect Platform. After multiple attempts, the Connect Platform makes an ARP request to get the MAC address of the new active Mobility Router. The requests are now received by the active Mobility Router.

To avoid this situation, the active and standby Mobility Routers should not be in the same subnet as the WLAN controller.

Continuous switchover occurs.

This might be caused by service failure. Look at the Mobility Router log and check whether any of the Mobility Router services has failed.

Access the physical IP address of one of the Mobility Routers and disable the cluster. The other Mobility Router is still in the cluster and is the active node. Look at the Mobility Router log of the active node for service failures. Verify the configuration of the active node to make sure that everything is configured properly. After you have confirmed that the configuration is appropriate and the Mobility Router services are stable, then add the other Mobility Router back into the redundancy cluster.

CHAPTER

16

Maintaining the System

You can reboot, restart, shut down, and restore the factory-default settings for the Mobility Router. System level maintenance also allows you to manage Mobility Router and Client images, in addition to viewing detailed records that are scheduled for export. Use the system level maintenance to configure to bulk provision users and perform a directory query.

This chapter contains the following sections:

Backup the Mobility Router

The Mobility Router configuration can be backed up to an FTP, SCP, or TFTP server by using the On-Demand method or by scheduling a backup.

Note

To restore a configuration, refer to “Restoring the Mobility Router Configuration” on page 203.

On Demand Backup

To perform and On Demand back up of the Mobility Router configuration:

1. Click **Maintenance > System > On Demand Backup**.
2. Enter the **Hostname or IP address** of the location to send the configuration file.
3. Select the **Protocol** by which to send the file: FTP, SCP or TFTP.
4. Enter the **Port** number.
5. Enter the **User ID**. The entry must match the User ID for the selected server (FTP/SCP/TFTP).
6. Enter the **Password** for the User.
7. In the **Path** field, type the 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.

WARNING!

/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.

8. Select **Backup**.

The Mobility Router 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.

Scheduled Backup

To schedule a backup of the Mobility Router configuration:

1. Click **Maintenance > System > Scheduled Backup**. The **Schedules** tab displays any previous scheduled backup yet to be performed. The **History** tabs displays previously performed backups.
2. To add a new scheduled backup, select **Add** on the **Schedules** tab.
3. On the **Add Schedule** page, enter a **Name** for the backup. This name displays on the Mobility Router ‘s **Schedules** and **History** pages.
4. Enter a **Description**.
5. Select the frequency at which the backup occurs as follows:
   a. **Daily**: Select the **Hour** in 24-hour increments.
   b. **Weekly**: Select the **Day** of the week and the **Hour** in 24-hour increments.
   c. **Monthly**: Select the **Date** and the **Hour** in 24-hour increments.
6. Enter the **Hostname or IP address** of the location to send the configuration file.
7. Select the **Protocol** by which to send the file: FTP, SCP or TFTP. Depending upon the type of protocol, for example FTP or SCP, enter the relevant information such as **Port number**, **User ID** and **Password**.
8. In the **Path** field, type the path to the directory to which you want to save the configuration file, for example “/home/user/backup/”.

Note

The FTP or TFTP server must be running for the backup to succeed.

WARNING!

/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.

9. Enter the **Filename Prefix**. This is the name of the file as it displays at the backup location. This name prepends the default file name which includes the Mobility Router 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-CMR-20110826-103000.bak”.

Restoring the Mobility Router Configuration

If you need to roll back to a previous Mobility Router configuration file, you can restore the previous configuration. Note that you can restore a configuration file only if has been saved and uploaded to a TFTP, FTP, or SCP server.

To restore the Mobility Router configuration:

1. Click **Maintenance > System > Restore**.
2. Enter the **Hostname or IP address** of the configuration file's location.
3. Select the **Protocol** by which to receive the file: FTP, SCP or TFTP. Depending upon the type of protocol, for example FTP or SCP, enter the relevant information such as **Port number**, **User ID** and **Password**.
4. Enter the **User ID**. The entry must match the User ID for the selected server (FTP/SCP/TFTP).
5. Enter the **Password** for the User.
6. In the **Path** field, type the path to the directory from which to retrieve the file, for example "/home/user/backup/".

Note

The FTP or TFTP server must be running for the backup to succeed.

7. Select **Include License**, **Include Network Information** and/or **Include Certificates** as appropriate.
8. Select **Restore**. Status about the restore process displays. 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.
9. Exit and restart the browser.
10. Log in to the Mobility Router by entering the admin login and password.

Restoring Factory-Default Settings

If necessary, you can restore the Mobility Router to its factory-default settings. If you restore the Mobility Router to its default settings, all settings but the following are reset to default values:

- Mobility Router IP address
- Default gateway
- Domain name
- CDR Reporting information

Note

When you restore the Mobility Router to its default settings, administrative account passwords must also be changed from factory default.

To restore the Mobility Router to the factory-default configuration:

1. Click **Maintenance > System > Factory Defaults**.
2. Click **Revert**.
3. Click **OK** to confirm setting the Mobility Router to the factory-default configuration. You are logged out.
4. Exit and restart the Web browser. Log in as administrator.

Restarting Mobility Router Services

You can restart the services on the Mobility Router. You might need to restart services if there are problems with calls on mobile devices, and nothing appears to be wrong with the Mobility Router configuration or the mobile devices.

If you restart the Mobility Router and you have a redundancy cluster enabled, active calls are not disrupted. If you do not have a redundancy cluster, active calls might be dropped. PBX functionality, initiation of new calls, and handovers of active calls between Wi-Fi and cellular networks are not available while the Mobility Router is restarted.

To restart the Mobility Router:

1. Click **Maintenance >System > Restart/Reboot/Shutdown**.
2. Click **Restart Services**.
3. Click **OK** to confirm the restart.
4. At the confirmation prompt, click **OK**.
5. Access a Web browser and log in to re-authenticate to the Mobility Router.

Rebooting the Mobility Router

You can reboot the Mobility Router. A reboot restarts services and also restarts the entire system. An example of when you might need to reboot is if you have problems connecting to the network interfaces.

If you reboot the Mobility Router and you have a redundancy cluster enabled, active calls are not disrupted. If you do not have a redundancy cluster, active calls might be dropped. PBX functionality, initiation of new calls, and handovers of active calls between Wi-Fi and cellular networks are not available while the Mobility Router is rebooting.

To reboot the Mobility Router:

1. Click **Maintenance > System > Restart/Reboot/Shutdown**.

2. Click **Reboot**.
3. Click **OK** to confirm the reboot. The Mobility Router immediately reboots, and you are immediately logged out.
4. Exit and restart the Web browser. You must re-authenticate to the Mobility Router by entering the admin login and password.

Shutting Down the Mobility Router

You can shut down and power off the Mobility Router. All active calls are gracefully disconnected, but services, including handovers, PBX features, and initiation of new calls are not available to active calls during and after the Mobility Router is shut down.

WARNING!

To restore services after you shut down the Mobility Router, you must manually press the power button on the Mobility Router. Before shutting down, make sure someone is located near the Mobility Router.

To shut down the Mobility Router:

1. Select **Maintenance > System > Restart/Reboot/Shutdown**.
2. Click **Shutdown**.
3. Click **OK** to confirm the shutdown. You are immediately logged out, and the Mobility Router shuts down.

To restore services after you shut down the Mobility Router, you must press the power button on the Mobility Router.

Starting and Stopping Mobility Router Services

If you need to contact Mitel Technical Support, you might be asked to restart one or more Mobility Router services.

WARNING!

Do not restart any Mobility Router services unless directed to do so by Technical Support.

To start or stop a Mobility Router service:

1. Click **Maintenance > Start/Stop Services**. On the Start/Stop Services page, the services and status (running or stopped) are listed. Next to the service status are Start and Stop buttons, which you can use to start and stop a service, respectively.

2. Find the service that you want to change, and do one of the following:
   - Click **Start** to start the service.
   - Click **Stop** to stop the service.
3. Repeat Step 2 for each service that you want to start or stop.

Managing Mobility Router Images

The Mobility Router contains two hard-drive partitions. When you receive a Mobility Router, it has the factory-default system image installed on each partition.

The Mobility Router Images page provides information about Mobility Router images that have already been installed and options to upload a new Mobility Router image from an URL or a local file.

Reviewing Installed Mobility Router Images

To review installed Mobility Router images, select **Maintenance > System > Images > Mobility Router Images**. The **Mobility Router Images** page lists the following:

- Mobility Router images installed
- Partition on which each image is installed (partitions 1 and 2)
- Which image is currently active (selected check box in the **Active** column)
- Which image will be used at the next reboot of the Mobility Router (selected check box in the **Next Boot** column)
- Uploading and Installing Mobility Router Images to the Mobility Router

Uploading and Installing Mobility Router Images to the Mobility Router

You can install Mobility Router images from a local file system or using HTTP, SCP, or FTP.

Note

If you are uploading the Mobility Router image from a local file system, you must use the Microsoft Internet Explorer Web browser.

WARNING!

When you upload and install a Mobility Router image, you cannot use the Administration Portal until the upload and installation are finished.

To install a Mobility Router image:

1. Click Main**tenance > System > Images > Mobility Router.**
2. Do one of the following:
   - **Select From URL**—Type the hostname, select the protocol, and enter the path of the server on which the Mobility Router image is installed. If using FTP or SCP, a User ID is required. If using FTP, the FTP server must be running for the upload to succeed.
   - **Select From local file**—Select to install the Mobility Router image from a local file system or click Browse to navigate the file system. Navigate to and select the Mobility Router image (*.img) and click Open.
3. Click **Install**. The image is uploaded to the Mobility Router. The image is now available for Mobility users to install.

Changing the Mobility Router Image Used at the Next Reboot

After installing a Mobility Router image, you can specify that it be used at the next reboot:

1. Click **Maintenance > System > Images > Mobility Router**. The **Mobility Router** Images page displays.
2. In the list of installed Mobility Router images, select the image to be used at the next Mobility Router reboot.
3. Click **Set Next Boot**. The next time the Mobility Router is rebooted, the image selected becomes the active image.
4. To reboot the Mobility Router, click **Reboot**. You are logged out, and the Mobility Router is restarted.
5. After the Mobility Router is restarted, log in. The system software image for the Mobility Router is updated.

Reviewing Patch Mobility Router Images

To review available Mobility Router patch images, Click **Maintenance > System > Images > Patch Mitel Connect Mobility Router**. The Patch Mobility Router page lists the available Mobility Router images.

Installing Patch Mobility Router Images

You can install Mobility Router patch images from a local file system or using HTTP, SCP, or FTP.

Note

If you are uploading the Mobility Router image from a local file system, you must use one of the following browsers:

- Google Chrome
- Microsoft Edge

- Mozilla Firefox

WARNING!

When you upload and install a Mobility Router image, you cannot use the Administration Portal until the upload and installation are finished.

To install a Mobility Router patch image:

1. Click **Maintenance > System > Images > Patch Mobility Router**. The Patch Mobility Router page displays.
2. Do one of the following:
   - **Select From URL**—Type the hostname, select the protocol, and enter the path of the server on which the Mobility Router patch image is installed. If using FTP or SCP, a User ID is required. If using FTP, the FTP server must be running for the upload to succeed.
   - **Select From local file**—Select to install the Mobility Router patch image from a local file system or click Browse to navigate the file system. Navigate to and select the Mobility Router patch image (*.img) and click **Open**.
3. Click **Apply Patch**. The patch image is uploaded to the Mobility Router. The image is now available for Mobility users to install.

Click **Save** to save the file to the Mobility Router image to the local PC.

Directory Query

The Mobility Router provides Admin users with tools to lookup users in the corporate directory. To search for a user:

1. Click **Maintenance > Users > Directory Query**.
2. In the **Search For** field, enter the digits or letters of the user to lookup. This is a wide search criterion. To narrow the criteria, select the “more” button to expand the options for searching. The available fields include:
   - User ID
   - Full Name
   - Enterprise Full Number
   - Enterprise Extension
   - Email
   - Cellular Number
   - Home Number
3. From the **Search In** drop down, select your directory
4. Click **Search**. The table populates with the users that have been found using the search criteria.

CHAPTER

17

Monitoring the System

You can monitor the status and usage of the Mobility Router by using the reports that are available as part of the mobility solution. Historical data and real-time reports are available.

This chapter contains the following sections:

Using the Dashboard

When you first log in as an administrator, the Dashboard is shown. Use the Dashboard to quickly get an overview of the activity on the Mobility Router.

To access the Dashboard, click **Monitor > Dashboard**.

The Dashboard includes the following information:

- System Status—Shows the hostname and model number of the Mobility Router. Also provides information about the CPU and memory utilization, percent of free memory, and system uptime. This area is updated every two minutes.
- Call Mix—Shows the percentage of calls on the Mobility Router that are being handled by the VoIP and the cellular networks. Position the cursor over the chart to view the total duration of VoIP and cellular calls. This information can be displayed for the last 1 hour, 24 hours, last 7 days, or last 30 days.
- Call Statistics—Shows the volume of calls handled on cellular and VoIP networks. This information is displayed in number of minutes and number of calls. Position the cursor over a specific point on the chart to view the exact number of minutes or number of calls at that time. If set to Last 1 hour or 24 Hours, this graph shows call statistics on a per hour display. If set to display Last 7 Days or Last 30 days, this graph shows call statistics per day. This area is updated every two minutes.
- Real-Time Statistics—Shows the number of users on the Mobility Router in various states, including:
  - Total Devices—Number of devices associated with this Mobility Router.
  - Provisioned Devices—Number of devices that are provisioned on this Mobility Router.
  - Registered Devices—Number of devices currently registered over the VoIP network and connected to the Mobility Router.
  - Total Users—Number of users who have been created and authorized on the Mobility Router.
  - Active Calls—Number of current active calls.
- End-User Licensing —Shows the number of users on the Mobility Router in various states, including:
  - Max Platform Devices —the number of devices supported by a specific platform. For example, if there are 100 Total Devices and there are 100 Users, then each user is limited to 1 device, or if there are 50 Users in this example, then each user can have 2 devices.
  - Platform Devices Available number of available devices outside of the Max Platform Devices.
  - Max Licensed End Users— The maximum number of end users allowed on this Mobility Router.
  - End User Licenses in Use —Number of end user licenses. As the “Available End User Licenses” count increases, this number will decrease.

- End User Licenses Available —Number of available end user licenses. The “End User Licensed in Use” count decreases as this number increases.

- Top 5 Users—Shows the top five users of the Mobility Router based on the total number of minutes used in the time span specified. This information can be displayed for the last 1 hour, 24 hours, last 7 days, or last 30 days.

Monitoring Call Status

The following types of usage reports are available for the Mobility Router:

- “Active Calls Reports” on page 218
- “Call Admission Control” on page 219

Active Calls Reports

The Active Calls report displays calls currently active on the Mobility Router. When an active call is ended, the call information becomes part of the Detail Records report (for more information, see “Call Admission Control” on page 219).

The Active Calls report includes the following information:

- Session ID—Session number of the active call
- User ID—Mobility user name of one of the participants on the active call
- Device—Device model type.
- From (Calling Party)—Phone number of the originator of the active call
- To (Called Party)—Phone number of the recipient of the active call
- Handovers—How many times the active call has been handed over from VoIP to cellular or cellular to VoIP
- Cell Duration—Number of minutes that the active call has been on the cellular network
- VoIP Duration—Number of minutes that the active call has been on the VoIP Network
- Total Call Duration—Total number of minutes the call has been active
- Currently on VoIP—Call is currently on VoIP if selected. If not selected, the call is on the cellular network.

Active Calls can be searched for and filtered based on multiple criteria.

To search for Active Calls:

5. Click **Monitor > Calls > Active Calls**.
6. In the **Session ID** dropdown window, select the means by which to find the Active Call. The options are Session ID, User ID, To, and From.
7. Select the criteria by which to find the user. The options are equal to or contains.
8. Type the appropriate string in the search field and press Enter. All rows containing the configured criteria display in the table.
9. You can click a column heading to alphabetically sort all pages by that criteria. For example, to sort by VoIP Duration, click the VoIP Duration column heading to view a listing in order of duration.
10. The current page number displays at the bottom right. Select a new page number to begin with and the number of rows to follow using the Go to page field and the Retrieve pulldown on the bottom right. The valid values are 50, 100 and 500. For example, enter Go to row 101 and select Retrieve 50 to begin sorting the rows on number 101 and end on number 151.
11. Select **Prev** or **Next** to view the pages before or after the current page.
12. Use the **Move** button to move a user to a different group in the table.
13. Click **Clear** to return to the original table.

To delete an active call, select the call, and click **Delete**. If you delete the call while it is active, the call is disconnected.

Call Admission Control

- Click **Monitor > Calls > Call Admission Control**.
  - Current bandwidth usage displays amount of network bandwidth, in kbps, currently used by all the ongoing SRV calls.
  - Current Active calls displays number of currently active SRV calls
  - Rejected calls due to bandwidth limit - The number of SRV calls, since last reset, that were rejected due to bandwidth limitation. Please note that such calls are routed through cellular network if cellular network is available at that time.
  - Rejected calls due to call limit - The number of SRV calls, since last reset, that were rejected due to the number of SRV calls limitation. Please note that such calls are routed through cellular network if the cellular network is available at that time. See “Call Admission Control” on page 52.

Monitoring Users

You can view information about events taking place on the Mobility Router in real-time. The following reports are available:

Active Users

The Active Users report displays a list of active users on the Mobility Router. To review the Active Users report, click **Monitor > Users > Active Users**.

Details listed include:

- User ID—Mobility user name.
- Device—Device model type.
- Enterprise Extension—Enterprise extension number of the Mobility user.
- Provisioning Status
  - Provisioned—The Mobility user has been through the provisioning process.
  - Authorized—The Mobility user account has been created on the Mobility Router, but the user has not gone through the provisioning process.
- PBX Registration Status
  - Registered
  - Unknown
- Client SIP Contact
  - Address
  - Expires In <xx> seconds
  - Service (All, Voice or Data)
  - Link (Wi-Fi-local, Wi-Fi-remote, or Cell Data)
  - Expires in (Sec)

Active Users can be searched for and filtered based on multiple criteria.

Search for Active User

To search for Active Users:

1. Click **Monitor > Users > Active Users**. The Active Users page displays.
2. In the **User ID** dropdown window, select the means by which to find the Active User. The options are **User ID, Enterprise Extension, Provisioning Status, PBX Registration Status, Address, Service Link**.
3. Select the criteria by which to find the user. The options are equal to or contains.
4. Type the appropriate string in the search field and press Enter. All rows containing the configured criteria display in the table. Search criteria is not case sensitive.
5. You can click a column heading to alphabetically sort all pages by that criteria. For example, to sort by PBX Registration Status, click the PBX Registration Status column heading to view an alphabetical listing of the registration status of the listed PBXs.
6. The current page number displays at the bottom right. Select a new page number to begin with and the number of rows to follow using the Go to page field and the Retrieve pulldown on the bottom right. The valid values are 50, 100 and 500. For example, enter Go to row 101 and select Retrieve 50 to begin sorting the rows on number 101 and end on number 151.
7. Select **Prev** or **Next** to view the pages before or after the current page.
8. Use the **Move** button to move a user to a different group in the table.
9. Click **Clear** to return to the original table.

Delete an Active User

To delete an active user:

1. Select the call.
2. Click **Delete**. If you delete the call while it is active, the call is disconnected.

Update an Active User

To update the **Active Users** page, click **Refresh**.

Monitor an Active User

To monitor an active user:

1. Select a user.
2. Double-click this user or click **User Monitoring**. The **User Monitoring** page displays.

For information about user monitoring, see “User Monitoring” on page 229.

Active Remote Users

You can monitor the currently active remote sessions and associated counters.

To review the Active Remote User report, click **Monitor > Users > Active Remote Users**.

All users who have active remote sessions are listed on the Users tab. Table 13 lists the information you can review for active remote users.

Table 13: Active Remote User Information

Header Name	Description
User ID	Mobility user name.
Device	Device model type
Session ID	Session identification number.
LAN IP Address	IP address of the mobile device
Protocol	Security protocol used for the remote session: dTLS or TLS.
Established	Date and time when the remote session was established.
Rx Packets	Number of packets received by the mobile device.
Tx Packets	Number of packets transmitted by the mobile device.
Rx Bytes	Number of bytes received by the mobile device.
Tx Bytes	Number of bytes transmitted by the mobile device.

Active Remote Users can be searched for and filtered based on multiple criteria.

Search for Active Remote User

To search for Active Remote Users:

1. Click **Monitor > Users > Active Remote Users**. The Active Remote Users page displays.
2. In the **User ID** dropdown window, select the means by which to find the Active User. The options are User ID, Session ID, LAN IP, Protocol, Established.
3. Select the criteria by which to find the user. The options are equal to or contains.
4. Type the appropriate string in the search field and press Enter. All rows containing the configured criteria display in the table. Search criteria is not case sensitive.
5. You can click a column heading to alphabetically sort all pages by that criteria. For example, to sort by User ID, click the User ID column heading to view an alphabetical listing of the listed Users.

6. The current page number displays at the bottom right. Select a new page number to begin with and the number of rows to follow using the Go to page field and the Retrieve pulldown on the bottom right. The valid values are 50, 100 and 500. For example, enter Go to row 101 and select Retrieve 50 to begin sorting the rows on number 101 and end on number 151.
7. Select **Prev** or **Next** to view the pages before or after the current page.
8. Use the **Move** button to move a user to a different group in the table.
9. Click **Clear** to return to the original table.

Delete an Active Remote User

To delete an active remote user:

1. Select the call.
2. Click **Delete**. If you delete the call while it is active, the call is disconnected.

Update an Active Remote Users Page

Click **Refresh** to update the **Active Remote Users** page.

User Monitoring

The User Monitoring page monitors the activity of a specific user on the Mobility Router. To review the User Monitoring report, click **Monitor > Users > Monitoring**.

In the **User ID** field, type the user name of the user to be monitored, and click **Start**. The user name entered must match a user ID on the Mobility Router.

Real-time information of the activity on the Mobility Router is displayed for the user specified. Information is refreshed every 5 seconds. Monitoring of the user is discontinued when you click Stop or navigate from the Monitoring the page.

Monitoring Redundancy Cluster Status

To review redundancy cluster status, click **Monitor > Clustering > Redundancy**. The Redundancy page displays.

The following basic cluster information is listed:

- Name—Cluster name
- Management Address—IP address of the virtual IP address used to manage the cluster
- Switchover—Switches from the master Mobility Router to the Standby router.

Table 14 lists the information of the table on the Redundancy page.

Table 14: Redundancy Information

Column Title	Description
Node	Name of the cluster member
IP Address	Physical IP address of the cluster member
Role	Role of the cluster member: Master—Active node Standby—Standby node
State	Network status of the cluster member: Online Offline

Monitoring System Status

You can review the status of the following:

- Interfaces (See “Reviewing Interface Status” on page 232.)

Reviewing Interface Status

You can review the status of the eth0, eth1, and loopback (lo) interfaces on the Mobility Router. To review interface status, click **Monitor > System > Interfaces**.

Table 15 lists the interface information shown on the Interfaces page.

Table 15: Interface Information

Column Title	Description
Name	Interface name
IP Address	Interface IP address
MAC Address	Interface MAC address (Ethernet interfaces only)
Speed	Interface speed (Ethernet interfaces only)
Admin Up	Indicates whether the interface can be administered
Link Up	Indicates whether the network link is up

CHAPTER

18

Troubleshooting

Client and Mobility Router logs are available to assist in troubleshooting the Connect Platform and the Mobility Router.

This chapter contains the following sections:

Managing Client Logs

The Mobility Router stores up to 500 client log files before replacing the oldest files.

Reviewing Client Logs

To review a client log:

1. Click **Troubleshooting > Client Logs**. The **Client Logs** page displays.
2. Select a client log to review.
3. Click **View**. The client log opens in a new browser window.
4. Scroll through the log to review the activity for the selected client.
5. When finished, close the browser window.

Saving Client Logs

You can save client logs to your computer's hard drive. To save a client log:

1. Click **Troubleshooting > Client Logs**. The **Client Logs** page displays.
2. Select the client log that you want to save.
3. Click **Save to Local Disk**.
4. Navigate to the location to which you want the log saved and click **Save**. When the log is saved, a "Transfer complete" message displays on the **Client Logs** page.

The client log is saved to your computer as a text file with a filename using the following format:

```
user-id.directory-number.mobile-device-type.day_month_date_year_time.txt
```

The following is an example of a client log file name:

```
sydney.8000.N95.Mon_Aug_26_2008_15_10_55.txt.
```

Deleting Client Logs

To delete a client log:

5. Click **Troubleshooting > Client Logs**. The **Client Logs** page displays.
6. Select the client log that you want to delete.
7. Click **Delete**. The client log is deleted from the Mobility Router.

Refreshing the Client Log List

To refresh the client log list:

1. Click **Troubleshooting > Client Logs**. The **Client Logs** page displays.
2. Click **Refresh**. The client log list is refreshed.

Running Network Troubleshooting Commands

Run the following network troubleshooting commands:

- ping (See "Running ping" on page 239)
- traceroute (See "Running traceroute" on page 240)
- nslookup (See "Running nslookup" on page 240)
- netstat (See "Running netstat" on page 241)

Note

The Administrator accounts have root privileges and can run the same commands from CLI.

Running ping

Run the ping command to check the reachability of a host and network connectivity. The ping command sends Internet Control Message Protocol (ICMP) echo request messages to the host and listens for ICMP echo response messages from the host.

To run the ping command:

1. Click **Troubleshooting > Commands**.
2. In the Command list, select **ping**.
3. In the **Host** field, type the IP address or name of the device that you are trying to ping.
4. Click **OK**. The ping output displays.

The following is an example of ping output:

```
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=63 time=0.319 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=63 time=0.165 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=63 time=0.311 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=63 time=0.208 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=63 time=0.355 ms

--- 192.168.1.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.165/0.271/0.355/0.074 ms
```

The output lists five ping attempts to 192.168.1.10 and a summary of the attempts.

Running traceroute

Run the traceroute command to check the route packets that take to a specified host. To run the traceroute command:

1. Click **Troubleshooting > Commands**.
2. In the Command list, select **traceroute**.
3. In the **Host** field, type the IP address or name of the device for which you want to trace the route.
4. Click **OK**. The traceroute output displays.

The following is an example of traceroute output:

```
traceroute to www.example.com (192.168.5.39), 30 hops max, 40 byte packets
 1  192.168.5.39 (192.168.5.39)  0.479 ms  0.864 ms  1.051 ms
 2  server10.example.com (192.168.2.21)  1.989 ms  2.186 ms  2.250 ms
```

The first row of the output lists the target destination, maximum number of hops, and packet size. Each numbered row provides information about one hop. The rows are listed in the order in which the hops occur, starting with the hop closest to the Mobility Router. Each row for a hop lists the time in milliseconds (ms) for each packet to reach the destination and return to the host.

Running nslookup

Run the nslookup command to get Domain Name System (DNS) information for a specified host. To run the nslookup command:

1. Click **Troubleshooting > Commands**.
2. In the Command list, select **nslookup**.
3. In the **Host** field, type the IP address or name of the device for which you are trying to look up.
4. Click **OK**. The nslookup output displays.

The following is an example of nslookup output:

```
Server:      server1.example.com
Address:     192.168.8.4

Name:        server2.example.com
Address:     192.168.2.240
```

The first two lines list the name and IP address of the device providing the information for the nslookup request. The last two lines provide the name and IP address of the device being looked up.

Running netstat

Run the netstat command to get information about incoming and outgoing network connections, routing tables, and network interface statistics.

The following options are supported with the netstat command:

-a	-g	-N	-t
-C	-i	-o	-u
-e	-l	-r	-v
-F (default)	-n	-s	-w

The following options are not supported with the netstat command:

- -c
- -M
- -p

To run the netstat command:

1. Click **Troubleshooting > Commands**.
2. In the Command list, select **netstat**.
3. (Optional) In the **Flags** field, type the options that you want to use with the netstat command.
4. Click **OK**. The netstat output displays.

Running Sniffer

Run the Sniffer to monitor the command exchange between the Mobility Router and the associated IP-PBX.

1. Select **Troubleshooting > Commands**.
2. Select **Start Sniffer,** or use the keyboard shortcut CTRL+ALT+S.
3. Use the associated controls below the Sniffer screen to Search for a specific string, copy to the clipboard, clear the screen, or close the Sniffer. The string is not case-sensitive. A list of up to 50 messages displays. Select/highlight the message to display the details below.

Internal Call Routing Table

Select **Troubleshooting > Internal Call Routing Table** to display the internal call routing table used by the SIP Server to route calls to the various internal modules. This table is useful for debugging voice call routing issues.

Managing Mobility Router Logs

To view the Mobility Router logs:

1. Click **Troubleshooting > Mobility Router Log > View**. The Mobility Router log displays in a separate browser window with the most recent data displayed first.
2. Scroll through the log to review the activity for the Mobility Router. Switch the display from the Current Log to the Archived Logs by selecting one of the Archived Logs from the list at the side of the page.
3. Click the **Prev** and **Next** buttons to view additional pages of data.

The Mobility Router keeps a log that provides detailed information that you can use when troubleshooting. The current Mobility Router log is named “messages”, and it is stored uncompressed on the Mobility Router. Archived Mobility Router logs are stored as files that are compressed by the GNU zip (gzip) utility. The gzip utility is available on most UNIX-based systems. Third-party compression utilities, such as WinZip, also support this compression format. For more information about gzip, see http://www.gnu.org/software/gzip/.

How many and how often Mobility Router logs are archived are determined by the local log configuration settings, as described in “Configuring Local Log Settings” on page 28. Archived Mobility Router logs are named messages.*n*.gz, where *n* is a number starting with one and incremented for each archived log (for example, messages.5.gz).

Archivable log modules are:

Table 19: Unknown Access Point Information

Log Name	Description
Infrastructure	Complete message log of the system.
Configuration	CMR configuration daemon logs.
Directory	CMR Directory daemon logs (useful for Active Directory query related logs).
Database	The Database Server manages the CMR configuration and monitored data stored on the Postgres DB.
Media Processor	Media processing events (for example, transcoding.).
Mobility	CMR mobility daemon logs (useful for location, fingerprinting related logs).

Table 19: Unknown Access Point Information

Log Name	Description
OLP	The Off-Line Processing (OLP) Server retrieves configuration and monitoring data via the database server and helps with such off-line processing tasks as CDR export, call summary reporting and trending, and so on.
Provisioning	Provisioning of CMRC log events.
Remote Access	Secure Remote Voice (a.k.a Secure Tunnel [RAST] in log data) log events.
Session Logger	CDR and call statistics related log events.
SIP	SIP protocol and Call log events.
UC	Presence & IM log events.

To set SIP server submodule levels, use following:

1. Call Control - incoming and outgoing user call information including SIP, CAC and HMP.
2. Registration - server and client registration information
3. UC - presence related information
4. Framework - SIP configuration, high availability and call detail record information
5. Filter by User ID - enter the User ID for a user to troubleshoot for that user only. This feature is useful when there are multiple users in the system and there is need to troubleshoot for a specific user. Log entries for other users are discarded.
6. Strict Filtering - check this option to strictly filter the log specified in “Filter by User ID”.
7. Miscellaneous - all categories not covered by the previous selections.
8. Click Apply to save changes.

To save a Mobility Router log:

1. Click **Troubleshooting > Mobility Router Logs**.
2. To view current logs, select the **Current** tab.
3. Use the **Log Name** field to select the Mobility Router log you want to save or view. There are 3 ways to view the log:
   a. Click **View** to see the contents of the entire file.
   b. Click **View Continuous** to see the data in the file as it is written.
   c. Click **Save to Local Disk** to select a location to download the Mobility Router log, then click Save. When the log is saved, a “Transfer complete” message displays on the Mobility Router Logs page.

The Mobility Router log is saved to your computer. By default, if you save the current Mobility Router log, it is saved as a text file named mobility_router_log.txt. If you save an archived server log, it is saved as a file compressed with gzip (for example, messages.5.gz).

4. To view/save older logs, select the **Archive** tab. Refer to "Configuring Logging and Monitoring Options" on page 24 for information about configuring the details of the log files. The files shown in the Archive tab are dependent upon these settings.

   a. Select a file and click **Save.**

   b. Select a location to download the Mobility Router log, then click **Save**. When the log is saved, a "Transfer complete" message displays on the Mobility Router Logs page.

      The Mobility Router log is saved to your computer. By default, if you save the current Mobility Router log, it is saved as a text file named mobility_router_log.txt. If you save an archived server log, it is saved as a file compressed with gzip (for example, messages.5.gz).

Use a utility such as gunzip or a third-party compression utility, such as WinZip, that supports the .gz format to decompress the archived Mobility Router log. After you decompress the file, you have an ASCII file, which you can open in a text editor.

Managing Technical Support Snapshots

If you need to contact Technical Support, you might be asked to provide a support snapshot, which is a a compressed file that contains files that provide information about the Mobility Router.

Generating Support Snapshots

When you generate a support snapshot, a set of files containing diagnostic information is compressed (.tgz) and added to the Mobility Router.

To generate a support snapshot:

1. Click **Troubleshooting > Support Snapshots**.
2. Click **Generate**. A support snapshot is generated and displays on the Support Snapshots page.

The snapshot name is in the following format:

```
sysdump-server_name-timestamp.tgz
```

where timestamp is the year, month, day, and time (for example, sysdump-server1-20080902-094428.tgz).

Reviewing Support Snapshots

After generating a support snapshot, you can review a summary of the snapshot. To review a support snapshot:

1. Click **Troubleshooting > Support Snapshots**.

2. Select the support snapshot that you want to review.
3. Click **View**. The support snapshot summary is opened in a new Web browser window.
4. Close the browser window when you are finished reviewing the support snapshot.

Saving System Snapshots

After generating a support snapshot, you can save it to your computer's hard drive. To save a support snapshot:

1. Click **Troubleshooting > Support Snapshots**.
2. Select the support snapshot that you want to save.
3. Click **Save**. Select a location to download the Mobility Router log, then click **Save**.
4. Navigate to the location to which you want to save the support snapshot, and if necessary, change the name of the snapshot.

By default, the name of the snapshot is in the following format:

```
sysdump-server_name-timestamp.tgz
```

where timestamp is the year, month, day, and time (for example, sysdump-server1-20080902-094428.tgz).

5. To save the snapshot, click **Save**.

As the snapshot is saved, you can see the progress of the save process on the Support Snapshots page. When the save process is complete, a "Transfer complete" message displays on the Support Snapshots page. The snapshot is saved as a .tgz file.

Support snapshots are compressed by the GNU zip (gzip) utility. The gzip utility is available on most UNIX-based systems. Third-party compression utilities, such as WinZip, also support this compression format. For more information about gzip, see http://www.gnu.org/software/gzip/.

Deleting System Snapshots

After generating a support snapshot, you can delete it from the Mobility Router. To delete a support snapshot:

1. Click **Troubleshooting > Support Snapshots**. The **Support Snapshots** page displays.
2. Select the support snapshot that you want to delete.
3. You can select multiple snapshots to delete. To select contiguous snapshots, press the Shift key while selecting the snapshots. To select non-contiguous snapshots, press the Ctrl key while selecting the snapshots.
4. Click **Delete**.

5. When prompted to confirm whether you want to delete the snapshot, click **OK**. The snapshot is deleted from the Mobility Router.

Capturing Packets

You can capture (dump) packet details on a specific interface by using the Packet Capture function.

To capture packets:

1. Click **Troubleshooting > Packet Capture**.
2. Select the Interface on which to capture the packets. Valid interfaces are Any, eth0, eth1 and lo (loopback).
3. Select the **Protocol** to capture. The options are ARP, ICMP, TCP and UDP.
4. Enter number of packets to be captured. The range is 1-100000.
5. Enter the range of ports to be included in the capture in the Start and End fields.
6. You can capture the packets using the following options:
   - In order to save the capture in a pcap format, select **To File** radio button**.** Perform the required troubleshooting, and in the **Capture Output** area press **Esc**. Click **Save** to collect your current capture.
   - For a live feed, select **To Browser** radio button, and then click **Start Capture**. Use the **Capture Output** area to view the capture. The following is an example of ARP capture details:

```
TCPdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:15:13.770168 arp reply 192.168.3.20 is-at 00:30:48:63:02:cc 13:15:13.779377 arp
who-has 192.168.3.20 (Broadcast) tell 192.168.3.20 13:15:28.785852 arp reply
192.168.3.20 is-at 00:30:48:63:02:cc 13:15:28.793387 arp who-has 192.168.3.20
(Broadcast) tell 192.168.3.20 13:15:43.803708 arp reply 192.168.3.20 is-at
00:30:48:63:02:cc 13:15:43.812843 arp who-has 192.168.3.20 (Broadcast) tell
192.168.3.20 13:15:58.821968 arp reply 192.168.3.20 is-at 00:30:48:63:02:cc
13:15:58.830004 arp who-has 192.168.3.20 (Broadcast) tell 192.168.3.20
13:16:13.837083 arp reply 192.168.3.20 is-at 00:30:48:63:02:cc 13:16:13.844120 arp
who-has 192.168.3.20 (Broadcast) tell 192.168.3.20 13:16:17.598572 arp who-has
192.168.3.1 tell 192.168.3.136 13:16:28.852448 arp reply 192.168.3.20 is-at
00:30:48:63:02:cc 13:16:28.861481 arp who-has 192.168.3.20 (Broadcast) tell
192.168.3.20 13:16:43.868711 arp reply 192.168.3.20 is-at 00:30:48:63:02:cc
13:16:43.875797 arp who-has 192.168.3.20 (Broadcast) tell 192.168.3.20
13:16:51.004425 arp who-has 192.168.3.138 tell
```

7. To save a summary of the dump, click **to File** then click **Save**. Select a location to download then click **Save**.

Test Dialer

The test dialer is used to troubleshoot call processing and signaling issues in the Mobility Router with respect to the user.

To test a user's incoming or outgoing calls through the Mobility Router:

1. Click **Troubleshooting > Test Dialer**.
2. Select **Enable**. Enter a valid User ID for the test.
3. Select **Client** to test outgoing calls from the user's device, or **Line** to test incoming calls to the user's device. This step may be performed for more than one user at a time.
4. Once enabled, enter a number in the **Dial To** field. You can log the information, as well as drop one or all calls after the test has run.
5. Disable the user in the Test Dialer when the testing is complete.

APPENDIX

A

Deployment Best Practices

The following section contains best practice information to aid in the deployment of a Mobility Router:

Mobility Router Ports

The following table lists the TCP/IP ports that are utilized on the Mobility Router for communications as described in Chapter 6, Managing Remote Access on page 25. As shown in the table, some of these ports are configurable by the Administrator.

Table 20: Mobility Router ETH 0 Ports Used in Line-Side Integration

Item #	Port Name	SMR	Remote Party		Transport	Connection Direction	Configurable	Notes
		Port Range	Device	Port				
1	SSH Server	22	Any SSH Client	1024+	TCP (SSH)	To SMR	No	Secure Shell (SSH)-used for secure logins, file transfers (SCP, SFTP) and port forwarding. SSH clients initiate SSH connections to the SMR.
2	HTTP Server	80	Web Browsers or RA Clients on local Wi-Fi	1024+	TCP (HTTP, RAMP)	To SMR	No	Web Server's HTTP port, used for RAMP, SMR UI. User and Admin portal URLs on this port are redirected to the https port. SMR receives Web Service requests from web browsers and RA Clients and send responses.
3	NTP Client	123	NTP Server	123	UDP (NTP)	Bi-Directional	No	Used for time syncing with the external NTP server. SMR also listens on that port for NTP query responses.
4	SNMP GET/SET	161	SNMP Clients	1024+	UDP (SNMP)	To SMR	No	SMR's SNMP agent receives queries and send responses. The SMR also quries WLAN controller for BSSID and TX power information of each AP.
5	SNMP Trap Receiver	162	WLAN Controllers	1024+	UDP (SNMP)	To SMR	No	SMR receive trap notifications from WLAN controllers. Information in the TRAP message includes TX Power change notification, which is used by the Symbian clients to make handover decision.
6	HTTPS Server	443	Web Browsers or RA Clients on local Wi-Fi	1024+	TCP(HTTPS, RAMP)	To SMR	NO	Web Server's HTTPS port, used for RAMP and SMR UI. SMR receives Web Service requests from web browsers and RA Clients and send responses.
7	RAST Server	443	RA Clients on remote Wi-Fi or Cell Data	1024+	TCP (TLS) UDP (DTLS, ADS)	To SMR	Yes	SMR RAST Server's TCP and UDP port for TLS and Datagram TLS respectively. Used for Secure Remote Access when RA clients are on remote Wi-Fi or cell data.

Table 1: Mobility Router ETH 0 Ports Used in Line-Side Integration (continued)

Item #	Port Name	SMR	Remote Party		Transport	Connection Direction	Configurable	Notes
		Port Range	Device	Port				
10	SIP Server	5060	PBX or RA Clients	5060	UDP/TCP	Bi-Directional	Yes	Standard SIP Port for SIP conversation between RA Client and SMR as well as SMR and PBX. The communication is bi-directional - if there is a firewall between the SMR and PBX or SMR and RA Clients on Wi-Fi, the port needs to be opened in both directions.
11	Secure SIP	5061	RA Clients	5061	TCP(SIP-TLS)	Bi-Directional	Yes	Standard SIP-TLS Port for Secure SIP conversation between RA Client and SMR. The communication is bi-directional. If there is firewall between the SMR RA clients in enterprise Wi-Fi, the port needs to be opened in both directions. Currently only supported on Symbian client.
12	SIP Trunk	5068	PBX (Trunk Switch)	5068	UDP/TCP	Bi-Directional	Yes	SIP Port used for trunk side communication between SMR and the PBX. This port is configurable in most PBX. The communication is bi-directional - If there is a firewall between the SMR and PBX, the port needs to be opened in both directions.
13	RAST Server Flow Ports	15000 to 25000	IP Phones or Media Gateways	1024+	UDP/TCP	Bi-Directional	Yes (CLI)	The ports in this range are used by the RAST server for Flow-based RAST connections used by BB, iPhone and Android clients. Nokia clients use IP-based RAST connection. SMR uses the first available port starting from 15000 to establish a flow (SIP, RTP or RAMP connection) for a remote RA Client. When the connection is no longer needed, the flow is closed and the port is released. SMR uses a SMART logic to reuse the ports to keep this port range small. For small number of remote clients, allocating 2 ports for every client should be sufficient. To maintain sufficient margin, at least 100 ports are recommended even for small number of clients. Data exchanged is RTP, SIP Signaling or HTTP (for RAMP) The communication is bi-directional - If there is a firewall between the SMR and IP Phones or Media Gateways the ports need to be opened in both directions.
14	Media Server RTP Ports	25370 to 32000	IP Phones or Media Gateways	1024+	UDP(RTP)	Bi-Directional	Yes (CLI)	The ports in this range are used by the SMR Media Server. The Media Server opens the first available port starting from 25370 when it needs to provide a service that requires RTP media pass through the mobility router. The following services require media pass through: • 3-way conference hosted by the SMR • Music On Hold • Force media bridging through the SMR • Media Transcoding • DTMF detection for cellular calls The SMR attempts to close the ports as soon as the call is terminated and it uses a smart logic to reuse the ports to keep this port range as small as possible. For small number of clients, allocating 2 ports for every client should be sufficient. To maintain sufficient margin, at least 100 ports are recommended even for small number of clients. Data exchanged is RTP. The communication is bi-directional - If there is a firewall between the SMR and IP Phones or Media Gateways the ports need to be opened in both directions.

Table 1: Mobility Router ETH 0 Ports Used in Line-Side Integration (continued)

Item #	Port Name	SMR	Remote Party		Transport	Connection Direction	Configurable	Notes
		Port Range	Device	Port				
15	RA Client RTP Ports	42000 to 42100	SMR, IP Phones or Media Gateways	1024+	UDP(RTP)	Bi-Directional	Yes (CLI)	An RA Client uses this range of port to receive and send RTP media when the client is on the local corporate wireless network. The communication is bi-directional - If there is a firewall between corporate IP media endpoints (SMR, IP Phones, Media Gateways) and RA Clients on local Wi-Fi the ports need to be opened in both directions.
16	SIP Server Registration Client Ports	50000 to 60000	PBX Line-side Interface	5060	TCP/UDP	Bi-Directional	No	SMR uses the ports in this range to uniquely identify clients to the PBX. SMR registers each client to the PBX with a unique SIP contact that has same IP but unique port. The port value starts from 50000 and goes up to 60000. If a customer has 100 users, the ports from 50000 to 50100 will be used for this purpose. Default transport is UDP but it can be changed to TCP. The communication is bi-directional - if there is a firewall between the SMR and PBX, the ports need to be opened in both directions.

URL-Based Dialing

Use the URL-based dialing feature to join conferences or dial extension digits to an automated attendant using the associated link in a conference meeting invitation. The VoIP URL dials the conference access number, followed by a short pause/delay and any Meeting/Participant code.

This feature is supported on iOS devices with the following syntax.

Table 21: URL-Based Dialing Per Device

Device	Wait/prompt	2 second pause
iOS	“;”	“,”

The feature is available under the following conditions:

- A device using the Connect Platform is in corporate/enterprise Wi-Fi network.
- A device using the Connect Platform is in Cellular Network and has registered to the Mobility Router for Secure Enterprise Features.
- A device using the Connect Platform is in the Remote Wi-Fi Network and has registered to the Mobility Router for Secure Enterprise Features.

The following are example uses of this feature:

Table 22: Supported Formats

Format	iPhone
Plain Text Email	☑
HTML Based Email	☑
Hypertext link within an Email	-
Microsoft® Outlook Calendar Invite	☑

Table 23: Example Uses

Description	Example Syntax
VoIP url with , and ; characters sent in an email where the email format is Plain-text format	voip://2113,#;1234567#
VoIP URL sent in a calendar INVITE from the OUTLOOK Exchange client on PC (new meeting). The Client opens the calendar appointment and the user can click the voip URL in NOTES section.	Refer to *iPhone User Guide* for examples.
VoIP URL in a Calendar INVITE sent from the OUTLOOK Exchange through UCB Outlook Plugin (manually added VoIP URL as part of UCB Details in invite).	Refer to *iPhone User Guide* for examples.

Note

Functionality may vary depending on the device.

Refer to the Connect Platform User Guides for usage examples and more information per device.

Integrating Mobility Router with Connect

There are two methods to integrate the Mobility Router with Connect depending on whether the user has an IP (Desk) Phone.

When the user's IP (Desk) Phone is the primary phone, the Connect Platform supports the following "Enhanced Mobility" features:

Table 24: Connect Enhanced Mobility Features

Function Name	Description
Extension Assignment	Provides a list of phone numbers that you can use as alternate numbers instead of your desk phone for routing incoming calls.
Visual Voice Mail	Displays the number of voice mail messages in the voice mailbox, and displays textual information of messages, such as date, time and duration.
Availability State	Changes the availability on the Connect Platform (Available, Vacation, Do Not Disturb, and so on.)

Refer to Configuring Enhanced Mobility for information about configuring the IP PBX for "Enhanced Mobility."

If the user's Connect Platform is the primary phone, the Mobility Router must be configured as the "primary line." In this case, the Connect Platform supports the "Enhanced Mobility" features described in Table 24, as well as Connect In-Call functions shown below:

Table 25: Connect In-Call Functions

Function Name	Description
Dial	Make call.
Answer	Accept call.

Function Name	Description
Hang up	Discontinue call.
Mute/Unmute	Listen to party without being heard/return to normal conversation.
Hold/Unhold	Suspend current call without hanging up/return to normal conversation.
Blind Transfer	Transfer call without introduction to the recipient of the transfer.
Consult Transfer	Transfer call after introducing the call to the recipient.
Mailbox Transfer	Transfer call to recipient's voice mailbox.
Voice Mail Transfer	Transfer call to your voice mailbox.
Transfer to AA	Transfer call to Auto-Attendant.
Blind Conference	Add a participant.
Consult Conference	Add a participant after introducing the conference to the participant.
Drop a Conference Participant	Remove a participant from a conference.
Conference Hold/Unhold	Suspend current conference without hanging up/return to normal conference mode.
Transfer Intercom	Transfer a call to a phone's intercom.
Transfer Whisper	Transfer a call and introduce the call without the 3rd party hearing the introduction.
Intercom	Make a call to a phone's intercom.
Conference Intercom	Add a participant to a conference using the participant's phone intercom.
Conference Intercom	Add a participant to a conference using the participant's phone intercom.
Overhead Page	Make a call to a paging system.
Whisper Page	Intervene in a call and speak to your colleague without the other party knowing. In this mode, you are unable to hear the other caller, as well; you are not listening in on the conversation but just communicating with your colleague.
Transfer to Voice Mailbox while Ringing	Transfer a call to voice mailbox while the call is still ringing.
Call a Voice Mailbox	Leave a voice mail message rather than speak to the recipient.
Record Call	Record your call.
Record Extension	Record someone else's call.
Make-me Conference	A make-me conference is possible only between extension users; it does not work for users connected through the trunk interface. It can also be done if there is any adhoc resources available on the switch that enables it to work.

Configuring Enhanced Mobility

Refer to the Mobility Router Integration Guide for Mitel Connect ONSITE, section *Configuring Users—Enabling Mobility Access for Individual Users* for information regarding configuring Enhanced Mobility.

Enhanced Mobility Extension Considerations

When you upgrade to in combination with Mobility Router 9.x, user details such as the enhanced mobility extension or the client user name do not change. When you modify any other part of the enhanced mobility user's record in Connect Director, the mobility application number configured for the user is modified. This modification invalidates the SIP registration for the enhanced mobility user. When the SIP registration is invalidated, the enhanced mobility user cannot use the mobility application on the device. To work around this issue, the administrator must modify the client user name in the Mobility Router.

When you create a new enhanced mobility user record in Connect Director, the client user name is appended with an underscore and two or three random digits. For example, the client user name for a new enhanced mobility user might be Bob_Smith_<extension>_xxx or Bob_Smith_<extension>_xx.

Controlling Connect for Android or iOS with Connect Client

Several Connect features are available on Mitel supported mobile devices. The controls for integrating and enabling these features are administered using the Mobility Router and Connect Platform (Connect for Android or Connect for iOS).

Connect integration with the Connect Platform requires the Mobility Router to be designated as a primary line or extension on the IP PBX.

Note

Connect integration is not supported for cellular network calls.

Complete the following steps to designate the Mobility Router as a primary line on the IP PBX.

1. Access Connect Director.
2. Click **Administration > Users > Users**.
3. Click the **General** tab.
4. Note the extension number in the “**Extension**” field. It will be used in Step 8.
5. Click the **Telephony** tab.
6. Clear the **Enable enhanced mobility with extension** check box. This registers the Mobility Router to the IP PBX as the primary line/extension. When this check box is cleared, Connect Controlled Device (CCD) settings are available on the mobile device. If this is an existing IP PBX user, that user’s desk phone displays “Available” and outbound calls are displayed with the caller ID “anonymous”. If this is a new user, the mobile device becomes the primary device.
7. On the Mobility Router, click **Configuration > Groups and Users > User**. Select the **Line** tab.

8. Enter the extension **Number** from **Individual Users** from Step 4 in the **PBX Side Digest User ID** field. (Note: Optionally, use the **Client Username** ID from Connect Director in the Mobility Router's **User ID** field.)
9. Confirm the **SIP Password** in Connect Director is the same password in the Mobility Router as shown.
10. Save/Apply your changes.

Refer to Assigning a Connect Controlled Device on page 164 for information about making an individual user's phone/device a Connect Controlled Device. Refer to the Mobility device User Guide for more information about enabling Connect Controlled Device on the individual phone/device.

Note

Connect integration is intended for users whose sole device is the Connect Platform. *Extension re-assignment is not supported.* Mitel may extend the capabilities of integration to include extension re-assignment in a future release.

APPENDIX

B

Third-Party Software Notices

This chapter contains the following sections:

RADVISION

OpenSSL

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, or DES code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)” The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgment: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS”' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]