CHAPTER 29

Managing the Phone System Integrations

You can manage the phone system integrations by adding or deleting phone systems, port groups, ports, phone system trunks, and servers. You can also change the settings for existing phone systems, port groups, ports, phone system trunks, and servers.

See the following sections:

Managing Phone Systems

The phone system pages in Cisco Unity Connection Administration identify the phone systems that Cisco Unity Connection integrates with. In Connection Administration, a phone system has one or more port groups, which in turn have voice messaging ports. You can manage the phone systems to meet the changing needs of your system.

See the following sections:

Adding a New Phone System Integration

You can integrate multiple phone systems with Cisco Unity Connection. For a matrix of supported combinations, see the *Multiple Integration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support adding new phone system integrations.

To Add a New Phone System Integration

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, under Phone System Search Results, click **Add New**. The New Phone System page appears.

Step 3 On the New Phone System page, in the Phone System Name field, enter a descriptive name for the phone system and click **Save**.

Step 4 On the Phone System Basics page, enter the applicable settings and click **Save**.

Deleting a Phone System Integration

You can delete a phone system when the phone system is no longer used by Cisco Unity Connection. Before you can delete a phone system, you must delete or reassign to another phone system all of the following objects that are associated with the phone system that you want to delete:

- All users (including MWI devices and notification devices)
- All user templates
- All system call handlers
- All call handler templates

Note You can see a list of all users who are associated with the phone system on the Phone System Associations page. For instructions, see the "Listing the Users Who Are Associated with the Phone System" section on page 29-3.

Cisco Unified Communications Manager Business Edition (CMBE) does not support deleting a phone system integration.

To Delete a Phone System Integration

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, under Phone System Search Results, check the check box next to the name of the phone systems that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm that you want to delete the phone systems, click **OK**.

Changing Phone System Settings

You can change the settings for a phone system after it is integrated with Cisco Unity Connection. The phone system settings identify the phone system that Connection integrates with and regulate certain phone system features. (Integration configuration settings are located in the port groups that belong to the phone system.)

To Change Phone System Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the phone system for which you want to change the settings.

Step 3 On the Phone System Basics page, change the applicable settings and click **Save**.

Listing the Users Who Are Associated with the Phone System

You can view a list of all of the Cisco Unity Connection users who are associated with the phone system.

To List the Users Who Are Associated with the Phone System

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the phone system.

Step 3 On the Phone System Basics page, on the Edit menu, click **Phone System Associations**.

Step 4 On the Phone System Associations page, the list of users who are associated with the phone system is displayed.

Disabling the Use of the Same Port for Turning On and Off an MWI

If you created the phone system integration to use the same voice messaging port to turn on and off an MWI (the Use Same Port for Enabling and Disabling MWIs field was checked), you can do the following procedure to disable this configuration without leaving MWIs on when there are no voice messages for the user.

To Disable the Use of the Same Port for Turning On and Off an MWI

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the phone system.

Step 3 On the Phone System Basics page, check the **Force All MWIs Off for This Phone System** check box and click **Save**.

Step 4 Uncheck the **Use Same Port for Enabling and Disabling MWIs** and the **Force All MWIs Off for This Phone System** check boxes, then click **Save**.

Step 5 Click **Run** in front of Synchronize All MWIs on This Phone System.

Synchronizing MWIs for the Phone System

You can synchronize all message waiting indicators (MWIs) for a phone system without affecting MWIs on other phone systems.

To Synchronize MWIs for the Phone System

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the phone system.

Step 3 On the Phone System Basics page, click **Run** in front of Synchronize All MWIs on This Phone System.

Configuring Phone View Settings (Cisco Unified Communications Manager Integrations Only)

For Cisco Unified Communications Manager integrations, Phone View allows users to see search results on the LCD screens of their Cisco IP phones when they use the Find Message or the Display Message menu. Phone View requires that Cisco Unified CM also be configured. For details, see the "Setting Up Phone View" chapter.

To Configure Phone View Settings (Cisco Unified Communications Manager Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the phone system.

Step 3 On the Phone System Basics page, under Phone View Settings, enter the applicable settings and click **Save**.

Changing Call Loop Detection Settings

Calls that Cisco Unity Connection forwards (for example, to notify a user that a message has been received) are sometimes forwarded back to Connection. When call loop detection is enabled, Connection detects when a call loop has occurred and rejects the call.

You can change the call loop detection settings to enable or disable the types of calls that are checked, to set the fourth-column DTMF tone that Connection uses, and to set the guard time.

The call loop detection settings should not be changed without understanding the effect that they have on calls that Connection forwards.

To Change Call Loop Detection Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the phone system.

Step 3 On the Phone System Basics page, under Call Loop Detection by Using DTMF, enter applicable settings and click **Save**.

Managing AXL Servers

AXL servers are supported only for Cisco Unified Communications Manager phone systems and are needed when Cisco Unity Connection must have access to the Cisco Unified CM database for importing Cisco Unified CM users and for changing certain phone settings for users of Connection personal call transfer rules.

AXL servers are not supported for Cisco Unified Communications Manager Express integrations.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support adding AXL servers. Adding AXL servers is not needed for Cisco Unified CMBE.

When a Connection cluster is configured, you must be logged on to the publisher server of the Connection cluster to import Cisco Unified CM user data.

See the following procedures:

- To Add AXL Servers, page 29-5
- To Delete an AXL Server, page 29-7
- To Change AXL Server Settings, page 29-7

To Add AXL Servers

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the Cisco Unified CM phone system.

Step 3 On the Phone System Basics page, on the Edit menu, click **Cisco Unified Communications Manager AXL Servers**.

Step 4 On the Edit AXL Servers page, under AXL Servers, click **Add New**.

Step 5 Enter the following settings for the AXL server and click **Save**.

Table 29-1 Settings for the AXL Servers

Field	Setting
Order	Enter the order of priority for the AXL server. The lowest number is the primary AXL server, the higher numbers are the secondary servers.
IP Address	Enter the IP address of the AXL server.
Port	Enter the AXL server port that Connection connects to. This setting must match the port that the AXL server uses. For Cisco Unified Communications Manager version 4.1(x), the port number is typically 443. For Cisco Unified Communications Manager version 5.x or later, the port number is typically 8443.

Step 6 Repeat Step 4 and Step 5 for all remaining AXL servers that you want to add.

Step 7 Under AXL Server Settings, enter the following settings and click **Save**.

Table 29-2 Settings for the AXL Server Settings

Field	Setting
User Name	Enter the user name that Connection uses to log on to the AXL server. **Note** This user must match the user name of a Cisco Unified CM application user who is assigned to the "Standard AXL API Access" role.
Password	Enter the password for the user that Connection uses to log on to the AXL server. **Note** This password must match the password of the Cisco Unified CM application user entered in the User Name field.
Cisco Unified Communications Manager Version	Select the Cisco Unified CM version in the list: • Pre 5.0 (Non-SSL) • Pre 5.0 (SSL) • 5.0 or Greater (SSL) If you select the Pre 5.0 (Non-SSL) version, the AXL port must be a non-SSL port (typically port 80). If you select the Pre 5.0 (SSL) version, the AXL port must be an SSL-enabled port (typically port 443 with Pre 5.0 versions). If you select the 5.0 or Greater (SSL) version, the AXL port must be an SSL-enabled port (typically port 8443).

Caution After the changes to this page are saved, you can click **Test** (next to the AXL server port number) to verify the connection to the AXL server. If the AXL port that you enter and the Cisco Unified CM Version setting conflict concerning whether SSL is used, the results of the test require more than 10 minutes to appear.

Step 8 To add a corresponding application server to Cisco Unified CM, log on to Cisco Unified CM Administration.

Step 9 In Cisco Unified CM Administration, go to the **System > Application Server** page.

Step 10 On the Find and List Application Servers page, click **Find** to display all application servers.

Step 11 In the Name column, click the name of the Cisco Unity Connection server.

Step 12 On the Application Server Configuration page, in the Available Application User field, select the Cisco Unified CM application user that you used in Step 7 and click the **Down** arrow to move it to the Selected Application User field.

Step 13 Click **Save**.

To Delete an AXL Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the Cisco Unified CM phone system.

Step 3 On the Phone System Basics page, on the Edit menu, click **Cisco Unified Communications Manager AXL Servers**.

Step 4 On the Edit AXL Servers page, under AXL Servers, check the check box next to the AXL server that you want to delete.

Step 5 Click **Delete Selected**.

Step 6 When prompted to confirm that you want to delete the AXL server, click **OK**.

To Change AXL Server Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the display name of the Cisco Unified CM phone system.

Step 3 On the Phone System Basics page, on the Edit menu, click **Cisco Unified Communications Manager AXL Servers**.

Step 4 On the Edit AXL Servers page, change the applicable settings and click **Save**.

Managing Port Groups

Port groups hold most of the integration configuration settings and some or all of the voice messaging ports for Cisco Unity Connection.

While most phone system integrations need only one port group, multiple port groups may be needed in the following circumstances:

- For integrations with phone systems through PIMG/TIMG units, each PIMG/TIMG unit is connected to one port group with the applicable voice messaging ports. For example, a system that uses five PIMG units requires five port groups, one port group for each PIMG unit.
- For integrations with other phone systems, an additional port group with its own voice messaging ports may be used for testing a new configuration or for troubleshooting.

Connection port groups provide flexibility for integration configuration settings that apply to different sets of port.

See the following sections:

Adding a Port Group

You can add multiple port groups, each with its own integration configuration settings and its own voice messaging ports.

Cisco Unified Communications Manager Business Edition (CMBE) only: Before you can add a port group, you must have existing voice messaging ports in Cisco Unified CM Administration that do not belong to a port group.

Other configurations: For integrations with phone systems through PIMG/TIMG units, one port group is required for each PIMG/TIMG unit. For example, a system that uses five PIMG units requires five port groups, one port group for each PIMG unit.

To Add a Port Group

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, under Port Group Search Results, click **Add New**.

Step 3 On the New Port Group page, enter the applicable settings and click **Save**.

Deleting a Port Group

When you delete a port group, any voice messaging ports that belong to it are deleted at the same time, but the phone system that the port group belongs to is not deleted.

To Delete a Port Group

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, under Port Group Search Results, check the check box next to the port group name of the port groups that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm that you want to delete the port group, click **OK**.

Changing Port Group Settings

You can change the settings for a port group after it has been added. Changes to the settings affect only the voice messaging ports that belong to the port group.

To Change Port Group Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change the settings.

Step 3 On the Port Group Basics page, change the applicable settings and click **Save**.

Changing the Audio Format That Cisco Unity Connection Uses for Calls

For calls, Cisco Unity Connection advertises the audio format (or codec) that is preferred for the media stream with the phone system. You should consider the following when setting the audio format:

- Connection should use the same audio format for the media stream that the phone system uses for the following reasons:
  - To reduce the need for transcoding the media stream from one audio format to another.
  - To minimize the performance impact on the Connection server and on the phone system.
  - To preserve the audio quality of calls.
- When Connection advertises a different audio format than the one used by the phone system, the phone system transcodes the media stream.

To Change the Audio Format That Cisco Unity Connection Uses for Calls

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the first port group that belongs to the phone system integration for which you want to change the audio format of the media stream.

Step 3 On the Port Group Basics page, on the Edit menu, click **Codec Advertising**.

Step 4 On the Edit Codec Advertising page, click the **Up** and **Down** arrows to change the order of the codecs or to move codecs between the Advertised Codec box and the Unadvertised Codecs box.

If only one codec is in the Advertised Codecs box, Cisco Unity Connection sends the media stream in that audio format. The phone system transcodes if it does not use this audio format.

If two or more codecs are in the Advertised Codecs box, Connection advertises its preference for the first codec in the list but sends the media stream in the audio format from the list that the phone system selects.

Step 5 Click **Save**.

Step 6 *(All integrations except SCCP)* If you want to change the packet size that is used by the advertised codecs, on the Port Group Basics page, under Advertised Codec Settings, click the applicable packet setting for each codec and click **Save**.

Step 7 Click **Next**.

Step 8 Repeat Step 3 through Step 7 for all remaining port groups that belong to the phone system integration for which you want to change the audio format of the media stream.

Changing MWI Settings

Messaging waiting indicators (MWIs) control whether Cisco Unity Connection sets MWIs for users and how retries for MWI requests are handled.

To Change MWI Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change the MWI settings.

Step 3 On the Port Group Basics page, under Message Waiting Indicator Settings, change the applicable settings and click **Save**.

Adding Secondary Cisco Unified Communications Manager Servers

For Cisco Unified Communications Manager integrations, Related Links helps you create the integration only with one Cisco Unified CM server. The secondary Cisco Unified CM servers in the cluster must be added after the integration is created.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support secondary Cisco Unified CM servers.

To Add Secondary Cisco Unified Communications Manager Servers

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to add secondary Cisco Unified CM servers.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under Cisco Unified Communications Manager Servers, click **Add**.

Step 5 Enter the settings for the secondary Cisco Unified CM server and click **Save**.

Step 6 Repeat Step 4 and Step 5 for all remaining secondary Cisco Unified CM servers that you want to add.

Note You can click **Ping** to verify the IP address (or host name) of the Cisco Unified CM server.

Deleting Cisco Unified Communications Manager Servers

You can delete a Cisco Unified Communications Manager server when it is no longer used by the phone system integration.

If you want to move a Cisco Unified CM server to another port group, you must delete the Cisco Unified CM server from one port group and add it to the second port group.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support deleting Cisco Unified CM servers.

To Delete a Cisco Unified Communications Manager Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to delete Cisco Unified CM servers.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under Cisco Unified Communications Manager Servers, check the check box next to the Cisco Unified CM servers that you want to delete.

Step 5 Click **Delete Selected**.

Step 6 When prompted to confirm that you want to delete the Cisco Unified CM servers, click **OK**.

Changing Cisco Unified Communications Manager Server Settings

You can change the Cisco Unified CM server settings after the server has been added.

To Change Cisco Unified Communications Manager Server Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change Cisco Unified CM server settings.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under Cisco Unified Communications Manager Servers, change the applicable settings and click **Save**.

Note You can click **Ping** to verify the IP address (or host name) of the Cisco Unified CM server.

Adding a TFTP Server

For Cisco Unified Communications Manager integrations, TFTP servers are required only when the Cisco Unified CM cluster uses authentication and encryption for the Cisco Unity Connection voice messaging ports.

If your system uses authentication and encryption for the Connection voice messaging ports, you must add a TFTP server after you create the Cisco Unified CM phone system integration.

To Add a TFTP Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to add a TFTP server.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under TFTP Servers, click **Add**.

Step 5 Enter the settings for the TFTP server and click **Save**.

Step 6 Repeat Step 4 and Step 5 for all remaining TFTP servers that you want to add.

Note You can click **Ping** to verify the IP address (or host name) of the TFTP server.

Deleting a TFTP Server

You can delete a TFTP server when it is no longer used by the port group.

For Cisco Unified Communications Manager integrations, TFTP servers are required only when the Cisco Unified CM cluster uses authentication and encryption for the Cisco Unity Connection voice messaging ports.

To Delete a TFTP Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to delete a TFTP server.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under TFTP Servers, check the check box next to the TFTP server that you want to delete.

Step 5 Click **Delete Selected**.

Step 6 When prompted to confirm that you want to delete the TFTP server, click **OK**.

Changing TFTP Server Settings

You can change the TFTP server settings after the server has been added.

For Cisco Unified Communications Manager integrations, TFTP servers are required only when the Cisco Unified CM cluster uses authentication and encryption for the Cisco Unity Connection voice messaging ports.

To Change TFTP Server Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change TFTP server settings.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under TFTP Servers, change the applicable settings and click **Save**.

Note You can click **Ping** to verify the IP address (or host name) of the TFTP server.

Adding a SIP Server

For a phone system integration with Cisco Unified Communications Manager through a SIP trunk or with another SIP server, you can add another SIP server after the phone system has been created.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support SIP servers.

To Add a SIP Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to add SIP servers.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under SIP Servers, click **Add**.

Step 5 Enter the settings for the SIP server and click **Save**.

Step 6 Repeat Step 4 and Step 5 for all remaining SIP servers that you want to add.

Note You can click **Ping** to verify the IP address (or host name) of the SIP server.

Deleting a SIP Server

For a phone system integration with Cisco Unified Communications Manager through a SIP trunk or with another SIP server, you can delete a SIP server when it is no longer used by the port group.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support SIP servers.

To Delete a SIP Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to delete SIP servers.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under SIP Servers, check the check box next to the SIP server that you want to delete.

Step 5 Click **Delete Selected**.

Step 6 When prompted to confirm that you want to delete the SIP server, click **OK**.

Changing SIP Server Settings

For a phone system integration with Cisco Unified Communications Manager through a SIP trunk or with another SIP server, you can change the SIP server settings after the server has been added.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support SIP servers.

To Change SIP Server Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change SIP server settings.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under SIP Servers, change the applicable settings and click **Save**.

Note You can click **Ping** to verify the IP address (or host name) of the SIP server.

Managing PIMG/TIMG Units

For integrations with phone systems through PIMG/TIMG units, each PIMG/TIMG unit is in a separate port group. For example, a system that uses five PIMG units requires five port groups, one port group for each PIMG unit. You can add, change, or delete PIMG/TIMG units after the phone system integration has been created.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support integrations with PIMG/TIMG units.

See the following procedures:

- To Add PIMG/TIMG Units, page 29-15
- To Delete PIMG/TIMG Units, page 29-15
- To Change PIMG/TIMG Settings, page 29-16

To Add PIMG/TIMG Units

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, under Port Group Search Results, click **Add New**.

Step 3 On the New Port Group page, in the Phone System field, click the phone system for which you want to add a PIMG/TIMG unit.

Step 4 Enter the applicable settings and click **Save**.

To Delete PIMG/TIMG Units

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, under Port Group Search Results, check the check box next to the port group for the PIMG/TIMG unit that you want to delete.

Step 3 Click **Delete Selected**.

To Change PIMG/TIMG Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change PIMG/TIMG settings.

Step 3 On the Port Group Basics page, under PIMG Settings, change the applicable settings and click **Save**.

Changing Session Initiation Protocol (SIP) Settings

For integrations that use session initiation protocol (SIP), you can change the SIP settings after the phone system integration has been created.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support integrations that use SIP.

To Change Session Initiation Protocol (SIP) Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change SIP settings.

Step 3 On the Port Group Basics page, under Session Initiation Protocol (SIP) Settings, change the applicable settings and click **Save**.

Changing Port Group Advanced Settings

The port group advanced settings control infrequently used settings such as delays and MWI usage. We recommend that port group advanced settings be left at their default values.

To Change Port Group Advanced Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change the advanced settings.

Step 3 On the Port Group Basics page, on the Edit menu, click **Advanced Settings**.

Step 4 On the Edit Advanced Settings page, under Port Group Advanced Settings, change the applicable settings and click **Save**.

Changing Automatic Gain Control (AGC) Settings

The automatic gain control (AGC) settings control the automatic value adjustments for recording messages. We recommend that AGC settings be left at their default values.

To Change AGC Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change the advanced settings.

Step 3 On the Port Group Basics page, on the Edit menu, click **Advanced Settings**.

Step 4 On the Edit Advanced Settings page, under Automatic Gain Control (AGC) Settings, change the applicable settings and click **Save**.

Managing Ports

The voice messaging ports let Cisco Unity Connection receive calls (for example, to record a message) and let Connection make calls (for example to send message notifications or to set MWIs).

Each voice messaging port can belong to only one port group. Port groups, when there are several, each have their own voice messaging ports. The total voice messaging ports belonging to all port groups must not exceed the maximum number of voice messaging ports that are enabled by the Connection license files.

See the following sections:

- Adding a Port, page 29-17
- Deleting a Port, page 29-18
- Changing Port Settings, page 29-18
- Viewing the Port Certificate, page 29-20

Adding a Port

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system. You can add voice messaging ports after the phone system has been created. The number of voice messaging ports that you add cannot bring the total number of voice messaging ports for all port groups to more than the maximum number of voice messaging ports that are enabled by the Connection license files.

Cisco Unified Communications Manager Business Edition (CMBE) only: Before you can add ports, you must have existing voice messaging ports in Cisco Unified CM Administration that do not belong to a port group.

To Add a New Port

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.

Step 2 On the Search Ports page, under Port Search Results, click **Add New**.

Step 3 On the New Port page, enter the applicable settings and click **Save**.

Caution Verify that there are an appropriate number of ports set to answer calls and an appropriate number of ports set to dial out. Otherwise, the integration may not function correctly. See the "Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection" section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Step 4 In Cisco Unity Connection Administration, in the Related Links list, click **Check Telephony Configuration** and click **Go** to confirm the phone system integration settings.

Step 5 If the test is not successful, the Task Execution Results list displays one or more messages with troubleshooting steps. After correcting the problems, check the configuration again.

Deleting a Port

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system.

To Delete a Port

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.

Step 2 On the Search Ports page, under Port Search Results, check the check box next to the voice messaging ports that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 For the remaining voice messaging ports in the port group, change the settings as necessary so that there are an appropriate number of voice messaging ports set to answer calls and an appropriate number of voice messaging ports set to dial out.

Changing Port Settings

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system. You can change the voice messaging port settings after the phone system integration has been created.

To Change Port Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.

Step 2 On the Search Ports page, click the display name of the voice messaging port for which you want to change the settings.

Step 3 On the Port Basics page, enter the applicable settings and click **Save**.

Depending on the phone system integration, some or all of the fields in Table 29-3 appear.

Table 29-3 Port Basics Page Settings

Field	Considerations
Enabled	Check this check box to enable the port. The port is enabled during normal operation. Uncheck this check box to disable the port. When the port is disabled, calls to the port get a ringing tone but are not answered. Typically, the port is disabled only by the installer during testing.
Server Name *(not available for PIMG/TIMG integrations)*	*(For Cisco Unity Connection redundancy only)* Click the name of the Cisco Unity Connection server that you want to handle this port. Assign an equal number of answering and dial-out voice messaging ports to the Connection servers so that they equally share the voice messaging traffic.
Extension *(available for PIMG/TIMG integrations only)*	Enter the extension for the port as assigned on the phone system.
Answer Calls	Check this check box to designate the port for answering calls. These calls can be incoming calls from outside callers or from users.
Perform Message Notification	Check this check box to designate the port for notifying users of messages. Assign Perform Message Notification to the least busy ports.
Send MWI Requests *(not used by serial integrations)*	Check this check box to designate the port for turning MWIs on and off. Assign Send MWI Requests to the least busy ports. For serial integrations, uncheck this check box. Otherwise, the integration may not function correctly.
Allow TRAP Connections	Check this check box so that users can use the port for recording and playback through the phone in Cisco Unity Connection web applications. Assign Allow TRAP Connections to the least busy ports.
Outgoing Hunt Order *(not available for SIP integrations)*	Enter the priority order in which Cisco Unity Connection uses the ports when dialing out (for example, if the Perform Message Notification, Send MWI Requests, or Allow TRAP Connections check box is checked). The highest numbers are used first. However, when multiple ports have the same Outgoing Hunt Order number, Connection uses the port that has been idle the longest.
Security Mode *(available for Cisco Unified CM SCCP integrations only)*	Click the applicable security mode: • **Non-secure**—The integrity and privacy of call-signaling messages are not ensured because call-signaling messages are sent as clear (unencrypted) text and are connected to Cisco Unified Communications Manager through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream is not encrypted. • **Authenticated**—The integrity of call-signaling messages are ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages are not ensured because they are sent as clear (unencrypted) text. In addition, the media stream are not encrypted. • **Encrypted**—The integrity and privacy of call-signaling messages are ensured on this port because they are connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages are encrypted. In addition, the media stream is encrypted.

Step 4 If there are no more voice messaging ports for which you want to change the settings, skip to Step 6. Otherwise, click **Next**.

Step 5 Repeat Step 3 and Step 4 for all remaining voice messaging ports for which you want to change the settings.

Step 6 On the Port menu, click **Search Ports**.

Step 7 On the Search Ports page, confirm that there are an appropriate number of voice messaging ports set to answer calls and an appropriate number of voice messaging ports set to dial out. If necessary, adjust the number of voice messaging ports set to answer calls and an appropriate number of voice messaging ports set to dial out.

Viewing the Port Certificate

Port certificates for voice messaging ports are used only by SCCP integrations with Cisco Unified Communications Manager 4.1 and later, and are required for authentication of the Cisco Unity Connection voice messaging ports. You can view the port certificate to help in troubleshooting authentication and encryption problems.

To View the Port Certificate

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.

Step 2 On the Search Ports page, click the display name of the voice messaging port for which you want to see the device certificate.

Step 3 On the Port Basics page, click **View Certificate**.

Step 4 In the View Port Certificate window, the information from the port device certificate is displayed.

Managing Phone System Trunks

When multiple phone systems are integrated with Cisco Unity Connection, you may want to set up a phone system trunk so that calls on one phone system can be transferred to extensions on another phone system. Phone system trunks are accessed by dialing extra digits (for example, dialing 9) before dialing the extension.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

See the following sections:

- Adding a Phone System Trunk, page 29-21
- Deleting a Phone System Trunk, page 29-21
- Changing Phone System Trunk Settings, page 29-21

Adding a Phone System Trunk

If another phone system integration exists, you can add a phone system trunk to provide access from calls on one phone system to extensions on the other phone system. You can add phone system trunks after the phone system integration has been created.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

To Add a Phone System Trunk

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Trunk**.

Step 2 On the Search Phone System Trunks page, under Phone System Trunk Search Results, click **Add New**.

Step 3 On the New Phone System Trunk page, enter the applicable settings and click **Save**.

Deleting a Phone System Trunk

You can delete a phone system trunk when it is no longer used by a phone system integration.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

To Delete a Phone System Trunk

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Trunk**.

Step 2 On the Search Phone System Trunks page, under Phone System Trunk Search Results, check the check box next to the phone system trunk that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm that you want to delete the phone system trunk, click **OK**.

Changing Phone System Trunk Settings

Phone system trunk settings cannot be changed. However, you can delete the phone system trunk that you want to change and add a new phone system trunk with the settings that you want.

Note Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

To Change Phone System Trunk Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Trunk**.

Step 2 On the Search Phone System Trunks page, check the check box next to the phone system trunk that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm that you want to delete the phone system trunk, click **OK**.

Step 5 Click **Add New**.

Step 6 On the New Phone System Trunk page, enter the applicable settings and click **Save**.

Security (Cisco Unified Communications Manager Integrations Only)

When Cisco Unified Communications Manager authentication and encryption is configured for Cisco Unity Connection voice messaging ports, you can manage certifications and the security profile.

See the following sections:

Viewing the Cisco Unity Connection Root Certificate

Revised May 2009

The root certificate is used by SCCP integrations with Cisco Unified Communications Manager 4.1 and later and SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports. You can view the root certificate to help troubleshoot authentication and encryption problems.

To View the Cisco Unity Connection Root Certificate

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **Root Certificate**.

Step 2 On the View Root Certificate page, the information from the root certificate is displayed.

Saving the Cisco Unity Connection Root Certificate as a File

Revised May 2009

The root certificate is used by SCCP integrations with Cisco Unified CM 4.1 and later and SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports.

To Save the Cisco Unity Connection Root Certificate as a File

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and click **Save Target As**.

Step 3 In the Save As dialog box, browse to the location where you want to save the Connection root certificate as a file.

Step 4 In the File Name field, confirm that the file name has the correct extension, depending on the version of Cisco Unified CM:

- For Cisco Unified CM 5.x or later, confirm that the extension is .pem (rather than .htm).
- For Cisco Unified CM 4.x, confirm that the extension is .0 (rather than .htm).

Caution The certificate must be saved as a file with the correct extension or Cisco Unified CM will not recognize the certificate.

Step 5 Click **Save**.

Step 6 In the Download Complete dialog box, click **Close**.

Step 7 The Connection root certificate file is ready to be copied to all Cisco Unified CM servers in this Cisco Unified CM phone system integration. For instructions, see the applicable Cisco Unified CM integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Adding a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Revised May 2009

The SIP certificate is used only by SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports.

To Add a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **SIP Certificate**.

Step 2 On the Search SIP Certificates page, click **Add New**.

Step 3 On the New SIP Certificate page, in the Display Name field, enter a display name for the SIP certificate.

Step 4 In the Subject Name field, enter a subject name that matches the X.509 subject name of the SIP security profile for the SIP trunk in Cisco Unified CM Administration.

Caution This subject name must match the X.509 subject name of the SIP security profile used by Cisco Unified CM. Otherwise, Cisco Unified CM authentication and encryption fail.

Step 5 Click **Save**.

Deleting a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can delete a SIP certificate when the Cisco Unified CM server is no longer configured for authentication of the Cisco Unity Connection voice messaging ports.

To Delete a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **SIP Certificate**.

Step 2 On the Search SIP Certificates page, check the check box next to the display name of the SIP certificate that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm that you want to delete the SIP certificate, click **OK**.

Changing a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can change a SIP certificate after it is created.

To Change a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **SIP Certificate**.

Step 2 On the Search SIP Certificates page, click the name of the SIP certificate that you want to change.

Step 3 On the Edit SIP Certificate page, enter the applicable settings and click **Save**.

Adding a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

The SIP security profile is used only by SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports.

To Add a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **SIP Security Profile**.

Step 2 On the Search SIP Security Profiles page, click **Add New**.

Step 3 On the New SIP Security Profile page, in the Port field, enter the port number that the Cisco Unified CM server uses for SIP trunk authentication and encryption of the voice messaging ports.

Step 4 To encrypt the call signaling messages, check the **Do TLS** check box.

Step 5 Click **Save**.

Deleting a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can delete a SIP security profile when the Cisco Unified CM server is no longer configured for authentication of the Cisco Unity Connection voice messaging ports.

To Delete a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **SIP Security Profile**.

Step 2 On the Search SIP Security Profiles page, check the check box next to the display name of the SIP security profile that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm that you want to delete the SIP security profile, click **OK**.

Changing a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can change a SIP security profile after it is created.

To Change a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then click **SIP Security Profile**.

Step 2 On the Search SIP Certificates page, click the name of the SIP security profile that you want to change.

Step 3 On the Edit SIP Security Profile page, enter the applicable settings and click **Save**.