



# CHAPTER 12

## Telephony Integrations

---

See the following sections:

- [Search Phone Systems, page 12-2](#)
- [New Phone System, page 12-2](#)
- [Phone System Basics, page 12-2](#)
- [Edit AXL Servers, page 12-4](#)
- [Phone System Associations, page 12-5](#)
- [Search Port Groups, page 12-6](#)
- [New Port Group, page 12-6](#)
- [Port Group Basics, page 12-8](#)
- [Edit Servers, page 12-10](#)
- [Edit Advanced Settings, page 12-12](#)
- [Edit Codec Advertising, page 12-13](#)
- [Search Ports, page 12-13](#)
- [New Port, page 12-14](#)
- [Port Basics, page 12-15](#)
- [View Port Certificate, page 12-17](#)
- [Search Phone System Trunks, page 12-18](#)
- [New Phone System Trunk, page 12-18](#)
- [View Root Certificate, page 12-19](#)
- [Search SIP Certificates, page 12-19](#)
- [New SIP Certificate, page 12-20](#)
- [Edit SIP Certificate, page 12-20](#)
- [Search SIP Security Profiles, page 12-21](#)
- [New SIP Security Profile, page 12-21](#)
- [Edit SIP Security Profile, page 12-22](#)

# Search Phone Systems

**Table 12-1** Search Phone Systems Page

Field	Description
Delete Selected	To delete a phone system, check the check box to the left of the display name, and click Delete Selected. You can delete multiple phone systems at once.
Add New	To add a phone system, click the Add New button. A new page opens, on which you enter data applicable to the new phone system.
Display Name	<i>(Display only)</i> The name of the phone system.
Port Count	<i>(Display only)</i> The number of voice messaging ports that have been created in Cisco Unity Connection for use by the phone system.

### See Also

- The “[Managing Phone Systems](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Phone System

**Table 12-2** New Phone Systems Page

Field	Description
Phone System Name	Enter a descriptive name for the phone system.

### See Also

- The “[Managing Phone Systems](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Phone System Basics

Revised May 2009

**Table 12-3** Phone System Basics Page

Field	Description
Phone System Name	Enter a descriptive name for the phone system.
Default TRAP Switch	Check this check box when you want TRAP connections to occur through this phone system. Default setting: Check box not checked.
Synchronize All User Templates on This Phone System	<i>(Cisco Unified Communications Manager Business Edition only)</i> Click Run to synchronize user templates so that they are all assigned to this phone system.

Table 12-3 Phone System Basics Page (continued)

Field	Description
Send Message Counts	<p>(Cisco Unity Connection 7.1 or later) Check this check box so that Cisco Unity Connection sends the message count and requests to turn on a user MWI each time that a new voice message arrives, even though the MWI may already be on.</p> <p>Uncheck this check box so that Connection does not send the message count and requests to turn on the MWI when a new voice message arrives, if the MWI already appears to be on.</p> <p>Default setting: Check box not checked.</p>
Use Same Port for Enabling and Disabling MWIs	<p>Check this check box so that requests to turn off an MWI use the same port that was used to turn it on.</p> <p>Uncheck this check box so that requests to turn off an MWI are not required to use the same port that was used to turn it on.</p> <p>Default setting: Check box not checked.</p>
Force All MWIs Off for This Phone System	<p>Check this check box to turn off all MWIs for the phone system. When used before clicking the Synchronize All MWIs on This Phone System button, this check box is useful for resetting incorrect MWIs.</p> <p>Default setting: Check box not checked.</p>
Synchronize All MWIs on This Phone System	<p>Click Run to synchronize MWIs for all users who are assigned to this phone system.</p>
Enable for Supervised Transfers	<p>Check this check box so that Cisco Unity Connection uses DTMF to detect and reject calls that have been transferred to another extension (by using supervised transfer) and that have been transferred back to Connection. If the call loop is not detected and rejected, Connection records a voice message that contains the prompt to leave a voice message.</p> <p>Default setting: Check box not checked.</p>
Enable for Forwarded Message Notification Calls (by Using DTMF)	<p>Check this check box so that Cisco Unity Connection uses DTMF to detect and reject new-message notifications that are sent to a device (such as a mobile phone) and that the device forwards back to Connection because the device did not answer. If the call loop is not detected and rejected, the call creates a new voice message for the user and triggers Connection to send a new-message notification call to the device.</p> <p>Default setting: Check box not checked.</p>
DTMF Tone to Use	<p>Click the fourth-column DTMF touchtone that is used to detect call loops.</p> <p>Default setting: A.</p>
Guard Time	<p>If call loop detection by using DTMF is enabled, enter the time, in milliseconds, that Cisco Unity Connection plays the DTMF tone for detecting a call loop.</p> <p>Default setting: 2,500 milliseconds.</p>
Enable for Forwarded Message Notification Calls (by Using Extension)	<p>Check this check box so that Cisco Unity Connection uses the extension to detect and reject new-message notifications that are sent to a device (such as a mobile phone) and that the device forwards back to Connection because the device did not answer. If the call loop is not detected and rejected, the call creates a new voice message for the user and triggers Connection to send a new-message notification call to the device.</p> <p>Default setting: Check box not checked.</p>

**Table 12-3** Phone System Basics Page (continued)

Field	Description
Enable Phone View	Check this check box to enable Phone View for the Cisco Unified Communications Manager phone system. Default setting: Check box not checked.
CTI Phone Access User Name	The name of the application user that was created in Cisco Unified Communications Manager Administration and associated with user phones.
CTI Phone Access Password	The password for the application user that is associated with user phones.
Enable Outgoing Calls	When this option is selected, Cisco Unity Connection places outgoing calls (for example, setting MWIs) as needed through the phone system. Default setting: Option selected.
Disable All Outgoing Calls Immediately	When this option is selected, Cisco Unity Connection does not place any outgoing calls (for example, setting MWIs). This option is useful when the phone system cannot respond to outgoing calls because of maintenance. Default setting: Option not selected.
Disable All Outgoing Calls Between	When this option is selected, Cisco Unity Connection does not place any outgoing calls (for example, setting MWIs) between the times set in the Beginning Time field and the Ending Time field. This option is useful when the phone system cannot respond to outgoing calls because of scheduled maintenance. Default setting: Option not selected.

**See Also**

- The “[Managing Phone Systems](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Edit AXL Servers

**Table 12-4** Edit AXL Servers Page

Field	Description
Delete Selected	To delete an AXL server, check the check box to the left of the display name, and click Delete Selected. You can delete multiple AXL servers at once.
Add New	To add an AXL server, click the Add New button. A new page opens, on which you enter data applicable to the new AXL server.
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 (or host name) of the AXL server that Cisco Unity Connection connects to.

**Table 12-4** Edit AXL Servers Page (continued)

Field	Description
Port	<p>Enter the AXL server port that Cisco Unity Connection connects to. This setting must match the port that the AXL server uses.</p> <p>If you enter a non-SSL port (typically port 80), you must also select a non-SSL version in the Cisco Unified Communications Manager Version field. If you enter an SSL-enabled port (typically port 443 or port 8443), you must also select an SSL-enabled version in the Cisco Unified Communications Manager Version field.</p>
User Name	Enter the user name that Cisco Unity Connection uses to log on to the AXL server.
Password	Enter the password that Cisco Unity Connection uses to log on to the AXL server.
Cisco Unified Communications Manager Version	<p>Click the applicable setting that accurately describes the following:</p> <ul style="list-style-type: none"> <li>• The version of Cisco Unified Communications Manager that you are integrating with Cisco Unity Connection.</li> <li>• Whether the AXL port is enabled for SSL.</li> </ul> <p>If you select the non-SSL version, the AXL port must be a non-SSL port (typically port 80). If you select the SSL-enabled version, the AXL port must be an SSL-enabled port (typically port 443 or port 8443).</p>

**See Also**

- The “[Managing Phone Systems](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Phone System Associations

**Table 12-5** Phone System Associations Page

Field	Description
User Alias	<i>(Display only)</i> The alias of the user that is associated with this phone system.
MWI	<i>(Display only)</i> The number of MWIs for this user that are turned on and off by this phone system.
Notification Device	<i>(Display only)</i> The number of notification devices for this user that connect through this phone system.

**See Also**

- The “[Managing Phone Systems](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search Port Groups

**Table 12-6** Search Port Groups Page

Field	Description
Delete Selected	To delete a port group, check the check box to the left of the display name, and click Delete Selected. You can delete multiple port groups at once.
Add New	To add a port group, click the Add New button. A new page opens, on which you enter data applicable to the new port group.
Port Group Name	<i>(Display only)</i> The descriptive name for the port group. Click this name to view and edit the phone system settings.
Phone System Display Name	<i>(Display only)</i> The phone system that uses the port group.
Port Count	<i>(Display only)</i> The number of voice messaging ports that have been created in Cisco Unity Connection for use by the port group.
Integration Method	<i>(Display only)</i> The method of integration that is used to connect Cisco Unity Connection and the phone system.
Needs Reset	<i>(Display only)</i> Indicates whether the port group needs to be reset to assure all functions.

### See Also

- The “[Managing Port Groups](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Port Group

Revised May 2009

**Table 12-7** New Port Group Page

Field	Description
Phone System	Click the phone system that uses the port group.
Create From	Choose one of the following: <ul style="list-style-type: none"> <li>Port Group Template—Cisco Unity Connection creates the new port group from the template that is selected from the list. The new port group has the default settings of the selected template.</li> <li>Port Group—Connection creates the new port group from the existing port group that is selected from the list. The new port group has the current settings of the selected port group.</li> </ul>
Display Name	Enter a descriptive name for the port group.
Device Name Prefix	<i>(Cisco Unified CM SCCP integrations only)</i> Enter the prefix that Cisco Unified Communications Manager adds to the device name for voice ports. This prefix must match the prefix used by Cisco Unified CM.
MWI On Extension	<i>(Cisco Unified CM SCCP integrations only)</i> Enter the extension that you specified in Cisco Unified CM Administration for turning MWIs on.
MWI Off Extension	<i>(Cisco Unified CM SCCP integrations only)</i> Enter the extension that you specified in Cisco Unified CM Administration for turning MWIs off.

Table 12-7 New Port Group Page (continued)

Field	Description
Authenticate with SIP Server	<i>(SIP integrations only)</i> Check this check box so that Cisco Unity Connection authenticates with the SIP server. Default setting: Check box not checked.
Authentication User Name	<i>(SIP integrations only)</i> Enter the user name that Cisco Unity Connection uses to authenticate with the SIP server.
Authentication Password	<i>(SIP integrations only)</i> Enter the password that Cisco Unity Connection uses to authenticate with the SIP server.
Contact Line Name	<i>(SIP integrations only)</i> Enter the voice messaging line name (or pilot number) that users use to contact Cisco Unity Connection and that Connection uses to register with the SIP server.
SIP Security Profile	<i>(PIMG/TIMG and SIP integrations only)</i> Click the SIP security profile that Cisco Unity Connection uses. Default setting: 5060.
SIP Transport Protocol	<i>(PIMG/TIMG and SIP integrations only)</i> Click the SIP transport protocol that Cisco Unity Connection uses. Default setting: UDP.
Security Mode	<i>(PIMG/TIMG and SIP integrations only)</i> Click the applicable security mode that Cisco Unity Connection uses: <ul style="list-style-type: none"> <li>• <b>Authenticated</b>—The integrity of call-signaling messages is 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.</li> <li>• <b>Encrypted</b>—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.</li> </ul> Default setting: Authenticated.
Secure RTP	<i>(PIMG/TIMG and SIP integrations only)</i> Check this check box so that the media stream (RTP) is encrypted. <b>Note</b> Media stream encryption is supported only with Cisco Unified Communications Manager 7.x or later. Default setting: Check box not checked.
IP Address or Host Name	Enter the IP address (or host name) of the phone system, SIP server, or PIMG/TIMG unit that the port group connects to.
Port	<i>(Cisco Unified CM SCCP integrations only)</i> Enter the TCP port of the primary Cisco Unified Communications Manager server that Cisco Unity Connection connects to. We recommend that you use the default setting. Default setting: 2000.
Port	<i>(PIMG/TIMG integrations only)</i> The SIP port on the PIMG/TIMG unit that Cisco Unity Connection connects to. When you configure more than one PIMG/TIMG unit (each PIMG/TIMG unit is in its own port group), increase this setting by 1 for each successive unit. For example, unit 2 will be 5061, unit 3 will be 5062, and so on. Default setting: 5060.

Table 12-7 New Port Group Page (continued)

Field	Description
Port	( <i>SIP integrations only</i> ) The SIP port on the SIP server that Cisco Unity Connection connects to. We recommend that you use the default setting. Default setting: 5060.
TLS Port	( <i>Cisco Unified CM SCCP integrations only</i> ) Enter the TLS port of the Cisco Unified Communications Manager server that you are integrating with Cisco Unity Connection. Default setting: 2443.

**See Also**

- The “[Managing Port Groups](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Port Group Basics

Revised May 2009

Table 12-8 Port Group Basics Page

Field	Description
Display Name	Enter a descriptive name for the port group.
Integration Method	( <i>Display only</i> ) The method of integration that is used to connect Cisco Unity Connection and the phone system.
Device Name Prefix	( <i>Cisco Unified CM SCCP integrations only</i> ) Enter the prefix that Cisco Unified Communications Manager adds to the device name for voice ports. This prefix must match the prefix used by Cisco Unified CM.
Reset Status	( <i>Display only</i> ) Indicates whether the port group needs to be reset to assure all functions.
<b>PIMG Settings</b>	
IP Address or Host Name	( <i>PIMG/TIMG integrations only</i> ) Enter the IP address (or host name) of the PIMG/TIMG unit that the port group connects to.
Port	( <i>PIMG/TIMG integrations only</i> ) The SIP port on the PIMG/TIMG unit that Cisco Unity Connection connects to.  When you configure more than one PIMG/TIMG unit (each PIMG/TIMG unit is in its own port group), increase this setting by 1 for each successive unit. For example, unit 2 will be 5061, unit 3 will be 5062, and so on.  Default setting: 5060.
<b>Session Initiation Protocol (SIP) Settings</b>	
Register with SIP Server	( <i>SIP integrations only</i> ) Check this check box so that Cisco Unity Connection registers with the SIP server.
Authenticate with SIP Server	Check this check box so that Cisco Unity Connection authenticates with the SIP server. Default setting: Check box not checked.
Authentication User Name	Enter the user name that Cisco Unity Connection uses to authenticate with the SIP server.

Table 12-8 Port Group Basics Page (continued)

Field	Description
Authentication Password	Enter the password that Cisco Unity Connection uses to authenticate with the SIP server.
Contact Line Name	Enter the voice messaging line name (or pilot number) that users use to contact Cisco Unity Connection and that Connection uses to register with the SIP server.
SIP Security Profile	<i>(PIMG/TIMG and SIP integrations only)</i> Click the SIP security profile that Cisco Unity Connection uses. Default setting: 5060.
SIP Transport Protocol	<i>(PIMG/TIMG and SIP integrations only)</i> Click the SIP transport protocol that Cisco Unity Connection uses. Default setting: UDP.
Security Mode	<i>(PIMG/TIMG and SIP integrations only)</i> Click the applicable security mode that Cisco Unity Connection uses: <ul style="list-style-type: none"> <li>• <b>Authenticated</b>—The integrity of call-signaling messages is 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.</li> <li>• <b>Encrypted</b>—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.</li> </ul> Default setting: Authenticated.
Secure RTP	<i>(PIMG/TIMG and SIP integrations only)</i> Check this check box so that the media stream (RTP) is encrypted. <b>Note</b> Media stream encryption is supported only with Cisco Unified Communications Manager 7.x or later. Default setting: Check box not checked.
<b>Advertised Codec Settings</b>	
Change Advertising	<i>(PIMG/TIMG and SIP integrations only)</i> Click this button to manage the codecs (audio formatting) that Cisco Unity Connection advertises that it can use when dialing out.
Display Name	<i>(PIMG/TIMG and SIP integrations only)</i> The name of the codecs (audio formatting) that Cisco Unity Connection advertises that it can use when dialing out.
Packet Size	<i>(PIMG/TIMG and SIP integrations only)</i> Click the packet size, in milliseconds, that you want to use for this codec (audio formatting). Default setting: 20 milliseconds.
<b>Message Waiting Indicator Settings</b>	
Enable Message Waiting Indicators	Check this check box so that voice messaging ports in the port group are enabled to turn message waiting indicators (MWIs) on and off. Only the voice messaging ports that have the Send MWI Requests check box checked turn MWIs on and off.  Uncheck this check box so that turning message waiting indicators (MWIs) on and off is disabled for all voice messaging ports in the port group. Even when voice messaging ports have the Send MWI Requests check box checked, they do not turn MWIs on and off. Default setting: Check box checked.

Table 12-8 Port Group Basics Page (continued)

Field	Description
MWI On Extension	(Cisco Unified CM SCCP integrations only) Enter the extension that you specified in Cisco Unified CM Administration for turning MWIs on.
MWI Off Extension	(Cisco Unified CM SCCP integrations only) Enter the extension that you specified in Cisco Unified CM Administration for turning MWIs off.
Delay Between Requests _____ Milliseconds	Enter the minimum length of wait time, in milliseconds, between subsequent MWI requests. Default setting: 0 milliseconds.
Maximum Concurrent Requests	Enter the maximum number of messaging waiting indicator (MWI) requests that are attempted at the same time so that a spike in MWI requests does not demand a large portion of Cisco Unity Connection resources. Default setting: 0 requests.
Retries After Successful Attempt	Enter the number of times an MWI request is retried after success is reported so that MWI success is assured. Default setting: 0 retries.
Retry Interval After Successful Attempt _____ Milliseconds	Enter the wait time, in milliseconds, between MWI retries that occur after success is reported. Default setting: 5 milliseconds.

**See Also**

- The “[Managing Port Groups](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Edit Servers

Table 12-9 Edit Servers Page

Field	Description
<b>Cisco Unified Communications Manager Servers</b>	
Delete Selected	To delete a server, check the check box to the left of the display name, and click Delete Selected. You can delete multiple servers at once.
Add	To add a server, click the Add button. A new row appears, in which you enter data applicable to the new server.
Order	Enter the order of priority for the Cisco Unified Communications Manager server that the port group connects to. The lowest number is the primary Cisco Unified CM server, the higher numbers are the secondary servers.
IP Address or Host Name	Enter the IP address (or host name) of the Cisco Unified Communications Manager server that the port group connects to.
Port	Enter the TCP port of the Cisco Unified Communications Manager server that Cisco Unity Connection uses. We recommend that you use the default setting. Default setting: 2000.

**Table 12-9** *Edit Servers Page (continued)*

Field	Description
TLS Port	Enter the TLS port of the Cisco Unified Communications Manager server. We recommend that you use the default setting. Default setting: 2443.
Server Type	Click the type of Cisco Unified Communications Manager server that Cisco Unity Connection is integrating with—Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. Default setting: Cisco Unified Communications Manager.
Ping	To verify the IP address (or host name) of the SIP server, click the Ping button.
<b>SIP Servers</b>	
Delete Selected	To delete a SIP server, check the check box to the left of the display name, and click Delete Selected. You can delete multiple SIP servers at once.
Add	To add a server, click the Add button. A new row appears, in which you enter data applicable to the new server.
Order	Enter the order of priority for the SIP server that the port group connects to. The lowest number is the primary SIP server, the higher numbers are the secondary servers.
IP Address or Host Name	Enter the IP address (or host name) of the SIP server that the port group connects to.
Port	Enter the IP port number that Cisco Unity Connection uses to connect to the SIP server. We recommend that you use the default setting. Default setting: 5060.
TLS Port	Enter the TLS port of the SIP server. Default setting: 5061.
Ping	To verify the IP address (or host name) of the SIP server, click the Ping button.
<b>TFTP Servers</b>	
Delete Selected	To delete a TFTP server, check the check box to the left of the display name, and click Delete Selected. You can delete multiple TFTP servers at once.
Add	To add a server, click the Add button. A new row appears, in which you enter data applicable to the new server.
Order	Enter the order of priority for the TFTP server that the port group connects to. The lowest number is the primary TFTP server, the higher numbers are the secondary servers.
IP Address or Host Name	Enter the IP address (or host name) of the TFTP server that the port group connects to.
Ping	To verify the IP address (or host name) of the TFTP server, click the Ping button.

**See Also**

- The “[Managing Port Groups](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Advanced Settings

**Table 12-10** Edit Advanced Settings Page

Field	Description
Delay After Answer ____ Milliseconds	Enter the wait time, in milliseconds, after a call is connected to Cisco Unity Connection and before Connection plays a greeting.  Default setting: 0 milliseconds.
Outgoing Guard Time _____ Milliseconds	Enter the wait time, in milliseconds, that a voice messaging port must be inactive before Cisco Unity Connection uses it for an outgoing call.  Default setting: 1,000 milliseconds.
Outgoing Pre-Dial Delay _____ Milliseconds	Enter the wait time, in milliseconds, before Cisco Unity Connection dials an outgoing call.  Default setting: 0 milliseconds.
Outgoing Post-Dial Delay _____ Milliseconds	Enter the wait time, in milliseconds, after Cisco Unity Connection dials an outgoing call.  Default setting: 0 milliseconds.
DTMF Interdigit Delay _____ Milliseconds	Enter the wait time, in milliseconds, after a caller dials a digit and before Cisco Unity Connection acts on the digits that it has received.  Default setting: 300 milliseconds.
Recording DTMF Clip	Enter the amount of time, in milliseconds, to truncate at the end of a recording when a message is terminated with a DTMF touchtone.  Default setting: 170 milliseconds.
Recording Tone Extra Clip	Enter the amount of time, in milliseconds, to truncate at the end of a recording when a message is terminated by the caller hanging up, which may cause the phone system to provide a tone (such as a reorder tone).  Default setting: 250 milliseconds.
Wait For Call Information	<i>(PIMG/TIMG integrations only)</i> The time (in milliseconds) that Cisco Unity Connection waits to receive call information from a PIMG/TIMG unit before playing the greeting.  This setting applies to integrations through TIMG units or analog PIMG units only. The setting may vary depending on the phone system configuration.  Default setting: 0 milliseconds.
Remote-Party-ID	<i>(PIMG/TIMG and SIP integrations only)</i> Enter the text that appears on the phone when the pilot number for the voice messaging ports is dialed. For example, enter “Cisco Unity Connection voice mail.”
Use DTMF KPML	<i>(PIMG/TIMG and SIP integrations only)</i> Check this check box so that DTMF digits for call control are sent through SIP NOTIFY messages in compliance with RFC 4730.  Default setting: Check box checked.
Use DTMF RFC 2833	<i>(PIMG/TIMG and SIP integrations only)</i> Check this check box so that DTMF digits for call control are sent through the RTP (audio) stream in compliance with RFC 2833.  Default setting: Check box checked.

**Table 12-10** Edit Advanced Settings Page (continued)

Field	Description
Address to Specific PIMG/TIMG port	( <i>PIMG/TIMG integrations only</i> ) When this option is selected, Cisco Unity Connection turns off an MWI by using the same port that was used to turn it on. Default setting: Option selected.
Not Port Specific	( <i>PIMG/TIMG integrations only</i> ) When this option is selected, Cisco Unity Connection uses any available dial-out port to turn off an MWI. Default setting: Option not selected.
Enable AGC	Check this check box so that Cisco Unity Connection automatically adjusts the recording volume of voice messages and user greetings to match the setting of the Automatic Gain Control (AGC) target decibels field on the System Settings > General Configuration page. Default setting: Check box checked.

**See Also**

- The “[Managing Port Groups](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Edit Codec Advertising

**Table 12-11** Edit Codec Advertising Page

Field	Description
Advertised Codecs	Move to this list the codecs (audio formats) that Cisco Unity Connection advertises that it can use when dialing out. The phone system must transcode if it uses different codecs.
Unadvertised Codecs	Move to this list the codecs (audio formats) that Cisco Unity Connection does not advertise when dialing out.

**See Also**

- The “[Managing Port Groups](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Search Ports

Revised May 2009

**Table 12-12** Search Ports Page

Field	Description
Delete Selected	To delete a port, check the check box to the left of the display name, and click Delete Selected. You can delete multiple ports at once.
Add New	To add a port, click the Add New button. A new page opens, on which you enter data applicable to the new port.

Table 12-12 Search Ports Page (continued)

Field	Description
Display Name	(Display only) The descriptive name for the voice messaging port. The name is created from the port group display name followed by a hyphen and sequence number of the voice messaging port.
Phone System Display Name	(Display only) The phone system that uses the port. Click this name to view and edit the phone system settings.
Extension	(Display only) The extension of the voice messaging port, if applicable.
Server	(Display only) The Cisco Unity Connection server (when a Connection cluster is configured) that handles this port.
Enabled	(Display only) When the column has an X, the port is enabled during normal operation.
Answer Calls	(Display only) When the column has an X, the port is designated for answering calls.
Message Notification	(Display only) When the column has an X, the port is designated for notifying users of messages.
Dialout MWI	(Display only) When the column has an X, the port is designated for turning MWIs on and off.
TRAP Connection	(Display only) When the column has an X, the port enables users to use the phone as a recording and playback device in Cisco Unity Connection web applications and email clients. Typically, TRAP Connection is assigned to the least busy ports.
Security Mode	(Display only) Indicates whether Cisco Unified Communications Manager authentication or encryption is enabled.

**See Also**

- The “[Managing Ports](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## New Port

Revised May 2009

Table 12-13 New Port Page

Field	Description
Enabled	<p>Check this check box so that the port is enabled during normal operation.</p> <p>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.</p> <p>Default setting: Check box checked.</p>
Number of Ports	<p>Enter the number of voice messaging ports that you want to add.</p> <p>Default setting: 1.</p>
Beginning Extension for a Range	<p>(Cisco Unity Connection 7.1 or later) Enter the extension of the first voice messaging port. If you are adding multiple ports, the first port will receive this extension number, the next port will receive the next extension in sequence, and so on.</p> <p> <b>Caution</b> You must confirm that the extensions are not already assigned to another voice messaging port. Otherwise, the phone system integration may not function correctly.</p>

Table 12-13 New Port Page (continued)

Field	Description
Phone System	Click the phone system that the voice messaging port uses.
Port Group	Click the port group that the voice messaging ports belong to.
Server	<i>(Cisco Unified CM and SIP integrations only)</i> When a Cisco Unity Connection cluster is configured, click the name of the Connection server that handles the voice messaging port.
Answer Calls	<p>Check this check box so that the port is designated for answering calls. These calls can be incoming calls from unidentified callers or from users.</p> <p>Uncheck this check box so that the port does not answer calls.</p> <p>Default setting: Check box checked.</p>
Perform Message Notification	<p>Check this check box so that the port is designated for notifying users of messages. Assign Perform Message Notification to the least busy ports.</p> <p>Default setting: Check box checked.</p>
Send MWI Requests	<p><i>(Not used by serial integrations.)</i> Check this check box so that the port is designated for turning MWIs on and off. We recommend that you assign Send MWI Requests to the least busy ports.</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>This check box is disabled for all ports in the port group if the Enable Message Waiting Indicators check box is not checked on the Port Group Basics page.</li> <li>The Enable Message Waiting Indicators check box on the Port Group Basics page of the port group must be checked for the voice messaging port to turn MWIs on and off. If the Enable Message Waiting Indicators check box on the Port Group Basics page of the port group is not checked, the voice messaging port does not turn MWIs on or off.</li> </ul> <p>Uncheck this check box so that message waiting indicators (MWIs) are not set by voice messaging ports in the port group. When this check box is not checked, even when voice messaging ports are configured to send MWI requests, MWIs are not set.</p> <p>Default setting: Check box checked.</p>
Allow TRAP Connections	<p>Check this check box so that users can use the phone as a recording and playback device in Cisco Unity Connection web applications and email clients. Assign Allow TRAP Connections to the least busy ports.</p> <p>Default setting: Check box checked.</p>
Security Mode	<p><i>(Cisco Unified CM integrations only)</i> Click the Cisco Unified Communications Manager security mode that you want to use for the voice messaging port.</p> <p>Default setting: Non-secure.</p>

**See Also**

- The “[Managing Ports](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Port Basics

Revised May 2009

Table 12-14 Port Basics Page

Field	Description
Enabled	<p>Check this check box so that the port is enabled during normal operation.</p> <p>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.</p> <p>Default setting: Check box checked.</p>
Port Name	<i>(Display only)</i> The descriptive name for the voice messaging port. The name is created from the port group display name followed by a hyphen and sequence number of the voice messaging port.
Restart	<p>Click this button to restart the voice messaging port.</p> <p></p> <p><b>Caution</b> Restarting a voice messaging port terminates any call that is in progress on that port. In Cisco Unity Connection Serviceability, you can stop a port from taking new incoming calls on the Tools &gt; Cluster Management page.</p>
Phone System	<i>(Display only)</i> The display name for the phone system that uses the voice messaging port.
Port Group	<i>(Display only)</i> The port group that the voice messaging ports belong to.
Extension	<i>(PIMG/TIMG integrations only)</i> Enter the extension that the phone system uses to connect to the port.
Server	<i>(Cisco Unified CM and SIP integrations only)</i> When a Cisco Unity Connection cluster is configured, click the name of the Connection server that handles the voice messaging port.
Answer Calls	<p>Check this check box so that the port is designated for answering calls. These calls can be incoming calls from unidentified callers or from users.</p> <p>Uncheck this check box so that the port does not answer calls.</p> <p>Default setting: Check box checked.</p>
Perform Message Notification	<p>Check this check box so that the port is designated for notifying users of messages. Assign Perform Message Notification to the least busy ports.</p> <p>Default setting: Check box checked.</p>
Send MWI Requests	<p><i>(Not used by serial integrations.)</i> Check this check box so that the port is designated for turning MWIs on and off. We recommend that you assign Send MWI Requests to the least busy ports.</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• This check box is disabled for all ports in the port group if the Enable Message Waiting Indicators check box is not checked on the Port Group Basics page.</li> <li>• The Enable Message Waiting Indicators check box on the Port Group Basics page of the port group must be checked for the voice messaging port to turn MWIs on and off. If the Enable Message Waiting Indicators check box on the Port Group Basics page of the port group is not checked, the voice messaging port does not turn MWIs on or off.</li> </ul> <p>Uncheck this check box so that message waiting indicators (MWIs) are not set by voice messaging ports in the port group. When this check box is not checked, even when voice messaging ports are configured to send MWI requests, MWIs are not set.</p> <p>Default setting: Check box checked.</p>

**Table 12-14** Port Basics Page (continued)

Field	Description
Allow TRAP Connections	Check this check box so that users can use the phone as a recording and playback device in Cisco Unity Connection web applications and email clients. Assign Allow TRAP Connections to the least busy ports. Default setting: Check box checked.
Outgoing Hunt Order	<i>(Cisco Unified CM and PIMG/TIMG integrations only)</i> Enter the order of priority that the port is used for outgoing calls, if applicable. When available ports have the same hunt order number, Cisco Unity Connection uses the port that has been idle the longest.
Security Mode	<i>(Cisco Unified CM integrations only)</i> Click the Cisco Unified Communications Manager security mode that you want to use for the voice messaging port. Default setting: Non-secure.
SCCP (Skinny) Device Name	<i>(Display only)</i> The device name that Cisco Unified Communications Manager assigned to the voice messaging port. This device name may be helpful for troubleshooting.
View Certificate	<i>(Cisco Unified CM integrations only)</i> Click this button to view the device certificate data for the voice messaging port.

**See Also**

- The “[Managing Ports](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## View Port Certificate

**Table 12-15** View Port Certificate Page

Field	Description
Subject	<i>(Display only)</i> The content of the Subject field for the port certificate.
Issuer	<i>(Display only)</i> The content of the Issuer field for the port certificate.
Valid From	<i>(Display only)</i> The date and time of beginning validity for the port certificate.
Valid Until	<i>(Display only)</i> The date and time of ending validity for the port certificate.
Version	<i>(Display only)</i> The version of the port certificate.
Serial Number	<i>(Display only)</i> The serial number of the port certificate.
Private Key	<i>(Display only)</i> The encrypted private key of the port certificate.
Subject Alternative Name	<i>(Display only)</i> The content of the Subject Alternative Name field for the port certificate.
Certificate Text	<i>(Display only)</i> The text content of the port certificate.
Generate New	Click this button to generate a new port certificates for all voice messaging ports.

**See Also**

- The “[Managing Ports](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## Search Phone System Trunks

**Table 12-16** Search Phone System Trunks Page

Field	Description
Delete Selected	To delete a phone system trunk, check the check box to the left of the display name, and click Delete Selected. You can delete multiple phone system trunks at once.
Add New	To add a phone system trunk, click the Add New button. A new page opens, on which you enter data applicable to the new phone system trunk.
From Phone System Display Name	<i>(Display only)</i> The phone system from which calls are transferred when Cisco Unity Connection dials the trunk access code for sending calls to another phone system.
To Phone System Display Name	<i>(Display only)</i> The phone system that the phone system trunk connects to when the trunk access code is dialed.
Trunk Access Code	<i>(Display only)</i> The number that Cisco Unity Connection dials to transfer a call from the phone system in the From Phone System field to the phone system in the To Phone System field.

**See Also**

- The “[Managing Phone System Trunks](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

## New Phone System Trunk

**Table 12-17** New Phone System Trunk Page

Field	Description
From Phone System	Click the phone system from which calls are transferred when Cisco Unity Connection dials the trunk access code for sending calls to another phone system.
To Phone System	Click the phone system that the phone system trunk connects to when the trunk access code is dialed.
Trunk Access Code	Enter the trunk access code that Cisco Unity Connection dials to transfer a call from the phone system in the From Phone System field to the phone system in the To Phone System field.

**See Also**

- The “[Managing Phone System Trunks](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# View Root Certificate

**Table 12-18** View Root Certificate Page

Field	Description
Subject	(Display only) The content of the Subject field for the root certificate.
Issuer	(Display only) The content of the Issuer field for the root certificate.
Valid From	(Display only) The date and time of beginning validity for the root certificate.
Valid Until	(Display only) The date and time of ending validity for the root certificate.
Version	(Display only) The version of the root certificate.
File Name	(Display only) The file name of the root certificate.
Serial Number	(Display only) The serial number of the root certificate.
Private Key	(Display only) The encrypted private key of the root certificate.
Certificate Text	(Display only) The text content of the root certificate.
Right-Click to Save the Certificate as a File	Right-click this link and click Save Target As so that you can save the root certificate as a file at the location that you indicate. Note that the file name must match the name indicated and that the extension must be 0 rather than htm.
Generate New	Click this button to generate a new root certificate and new port certificates for all voice messaging ports.

### See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search SIP Certificates

**Table 12-19** Search SIP Certificates Page

Field	Description
Delete Selected	To delete a SIP certificate, check the check box to the left of the display name, and click Delete Selected. You can delete multiple SIP certificates at once.
Add New	To add an SIP certificate, click the Add New button. A new page opens, on which you enter data applicable to the new SIP certificate.
Display Name	(Display only) The name of the SIP certificate.
Subject Name	(Display only) The subject name that matches the subject name of the SIP certificate for the SIP trunk in Cisco Unified CM Administration.

### See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# New SIP Certificate

**Table 12-20**      *New SIP Certificate Page*

Field	Description
Display Name	Enter a descriptive name for the SIP certificate.
Subject Name	<p>Enter a subject name that matches the subject name of the SIP certificate for the SIP trunk in Cisco Unified CM Administration.</p> <p> <b>Caution</b> This subject name must match the subject name of the SIP certificate used by Cisco Unified Communications Manager. Otherwise, Cisco Unified CM authentication and encryption fail.</p>

### See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit SIP Certificate

**Table 12-21**      *Edit SIP Certificate Page*

Field	Description
Display Name	Enter a descriptive name for the SIP certificate.
Subject Name	<p>Enter a subject name that matches the subject name of the SIP certificate for the SIP trunk in Cisco Unified CM Administration.</p> <p> <b>Caution</b> This subject name must match the subject name of the SIP certificate used by Cisco Unified Communications Manager. Otherwise, Cisco Unified CM authentication and encryption fail.</p>
Private Key	<i>(Display only)</i> The encrypted private key of the SIP certificate.
Certificate Text	<i>(Display only)</i> The text content of the SIP certificate.
Generate New	Click this button to generate a new SIP certificate.

### See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search SIP Security Profiles

**Table 12-22** Search SIP Security Profiles Page

Field	Description
Delete Selected	To delete a SIP security profile, check the check box to the left of the display name, and click Delete Selected. You can delete multiple SIP security profiles at once.
Add New	To add a SIP security profile, click the Add New button. A new page opens, on which you enter data applicable to the new SIP security profile.
Display Name	( <i>Display only</i> ) The name of the SIP security profile.

### See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# New SIP Security Profile

**Table 12-23** New SIP Security Profile Page

Field	Description
Port	The port that the Cisco Unified Communications Manager server uses for SIP trunk authentication and encryption of the voice messaging ports.  <b>Note</b> You cannot use the same port for both TLS and non-TLS SIP security.
Do TLS	Check this check box so that call signaling messages are encrypted when sent through the SIP trunk between Cisco Unity Connection and the Cisco Unified Communications Manager server.  Uncheck this check box so that call signaling messages are not encrypted when sent through the SIP trunk between Connection and the Cisco Unified CM server.   <b>Caution</b> When this check box is checked, the Cisco Unified CM server must also enable TLS. Otherwise, SIP security does not function correctly.

### See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit SIP Security Profile

Table 12-24 Edit SIP Security Profile Page

Field	Description
Port	<p>The port that the Cisco Unified Communications Manager server uses for SIP trunk authentication and encryption of the voice messaging ports.</p> <p><b>Note</b> You cannot use the same port for both TLS and non-TLS SIP security.</p>
Do TLS	<p>Check this check box so that call signaling messages are encrypted when sent through the SIP trunk between Cisco Unity Connection and the Cisco Unified Communications Manager server.</p> <p>Uncheck this check box so that call signaling messages are not encrypted when sent through the SIP trunk between Connection and the Cisco Unified CM server.</p> <p> <b>Caution</b> When this check box is checked, the Cisco Unified CM server must also enable TLS. Otherwise, SIP security does not function correctly.</p>

## See Also

- The “[Security \(Cisco Unified Communications Manager Integrations Only\)](#)” section in the “Managing Phone System Integrations” chapter of the *System Administration Guide for Cisco Unity Connection*.