

Advanced Settings

See the following sections:

- [Search SMPP Providers, page 11-1](#)
- [New SMPP Provider, page 11-2](#)
- [Edit SMPP Provider, page 11-3](#)
- [Conversation Configuration, page 11-9](#)
- [Messaging Configuration \(Cisco Unity Connection 7.1\), page 11-15](#)
- [Telephony Configuration, page 11-16](#)
- [Report Configuration, page 11-18](#)
- [Connection Administration Configuration, page 11-19](#)
- [TRAP Configuration, page 11-21](#)
- [Edit Disk Capacity Configuration, page 11-21](#)
- [PCA Configuration, page 11-22](#)
- [RSS Configuration, page 11-23](#)
- [Cluster Configuration, page 11-23](#)
- [Fax Configuration, page 11-24](#)
- [External Services Configuration, page 11-24](#)

Search SMPP Providers

Table 11-1 *Search SMPP Providers Page*

Field	Description
Find SMPP Providers Where Name	To find all SMPP providers on this Cisco Unity Connection server, click Find. To find selected SMPP providers, enter specifications for the names of the providers that you want to find, and click Find.
Name	<i>(Display only)</i> The name of the SMPP provider. To display more information on an SMPP provider, click the name.
Delete Selected	To delete an SMTP provider, check the check box to the left of the display name, and click Delete Selected. You can delete multiple SMTP providers at once.

Table 11-1 Search SMPP Providers Page (continued)

Field	Description
Add New	Click Add New to add another SMPP provider.

- The “[Setting Up SMS \(SMPP\) Message Notifications](#)” section in the “Setting Up SMTP and SMS (SMPP) Message Notifications” chapter of the *System Administration Guide for Cisco Unity Connection*.

New SMPP Provider

Table 11-2 New SMPP Provider Page

Field	Description
Enable	Check this check box to enable the SMPP provider. The providers that you enable are available to all applicable users to use for SMS (SMPP) message notifications.
Name	<p>Enter the name that represents the service provider in Cisco Unity Connection applications. The name you enter here is listed on the Provider SMPP lists displayed on the SMS (SMPP) Message Notification pages for templates and individual users in Cisco Unity Connection Administration, as well as in the Cisco Unity Assistant.</p> <p>For multilingual systems, consider adding an SMPP provider for each language that users use and then name and configure the providers accordingly. (Use the Data Coding field to specify language preference.)</p>
System ID	<p>Enter the name or system ID that is associated with the account that your organization has with the SMSC, as provided by your service provider. Cisco Unity Connection uses the information in this field to identify itself when communicating with the SMPP server at the SMSC.</p> <p>This field corresponds to the system_id in the SMPP Protocol Specification.</p>
Host Name/Address	Enter the IP address or host name of the SMPP server at the SMSC.
Source Address	<p>If the SMPP Provider requires a source address for the server sending the message, enter the IP address for the Cisco Unity Connection server.</p> <p>If the SMPP Provider does not require a source address, enter the number that the user calls to check messages. The format and the number that you enter depends on the SMPP Provider. The provider may require that you include international country codes, beginning with a plus sign (+) and followed by the country code, area, city, or trunk code, and then the number for the device (for example, +12065551234). Do not start with a zero or the international dialing prefix. Do not include spaces, dashes, parentheses or other punctuation.</p> <p>Note that some SMPP Providers replace the number that you enter in the Source Address field with their own phone number. For an alternative method of including a call back number, try entering the number that the user calls to check messages in the Send field.</p>

Table 11-2 New SMPP Provider Page (continued)

Field	Description
Owner	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> To restrict provider use, select a user as owner of the selected SMPP provider. Click the User button and then select the applicable user from the list. To allow the SMPP provider to be used by all users on this server, select System as owner of the selected SMPP provider.

See Also

- The “[Setting Up SMS \(SMPP\) Message Notifications](#)” section in the “Setting Up SMTP and SMS (SMPP) Message Notifications” chapter of the *System Administration Guide for Cisco Unity Connection*.

Edit SMPP Provider

Revised May 2009

Table 11-3 Edit SMPP Provider Page

Field	Description
Enable	Check this check box to enable the SMPP provider. The providers that you enable are available to all applicable users to use for SMS (SMPP) message notifications.
Name	<p>Enter the name that represents the service provider in Cisco Unity Connection applications. The name you enter here is listed on the Provider SMPP lists displayed on the SMS (SMPP) Message Notification pages for templates and individual users in Cisco Unity Connection Administration, as well as in the Cisco Unity Assistant.</p> <p>For multilingual systems, consider adding an SMPP provider for each language that users use and then name and configure the providers accordingly. (Use the Data Coding field to specify language preference.)</p>
Host Name/Address	Enter the IP address or host name of the SMPP server at the SMSC.
Port	<p>Enter the port used by the SMPP server to connect to an ESME like Cisco Unity Connection.</p> <p>When the Connection server is set up behind a firewall, you must configure the TCP port to allow incoming and outgoing communication between Connection and the SMPP server.</p>
System ID	<p>Enter the name or system ID that is associated with the account that your organization has with the SMSC, as provided by your service provider. Cisco Unity Connection uses the information in this field to identify itself when communicating with the SMPP server at the SMSC.</p> <p>This field corresponds to the system_id in the SMPP Protocol Specification.</p>
Password	<p>Enter the password that is associated with the account that your organization has with the SMSC, as provided by your service provider. Cisco Unity Connection uses the information in this field to identify itself when communicating with the SMPP server at the SMSC.</p> <p>This field corresponds to the password in the SMPP Protocol Specification.</p>

Table 11-3 Edit SMPP Provider Page (continued)

Field	Description
System Type	<p>If applicable, enter the value provided to you by your service provider. (If your provider did not specify a value, leave the field blank.) The information in this field categorizes the type of ESME that is communicating with the SMPP server at the SMSC. For example, an application like Cisco Unity Connection may be categorized as a “VMS” (voice messaging system).</p> <p> Caution This field is case-sensitive. Check the SMPP configuration documentation from your service provider for the correct capitalization, then enter it here exactly as specified.</p> <p>This field corresponds to <code>system_type</code> in the SMPP Protocol Specification.</p>
Interface Version	<p>Indicate the version of the SMPP protocol that the SMPP server uses to communicate with ESMEs like Cisco Unity Connection.</p> <p>This field corresponds to the <code>interface_version</code> in the SMPP Protocol Specification.</p>
Address NPI	<p>Address Number Plan Identifier (NPI). If applicable, select the value provided to you by your service provider. (If your provider did not specify a value, leave the field set to Unknown.) The information in this field defines the numeric plan indicator that users can use when specifying the To and From fields for SMS (SMPP) message notifications in Cisco Unity Connection Administration and in the Cisco Unity Assistant. Select the applicable value from the list:</p> <ul style="list-style-type: none"> • Unknown • ISDN (E163/E164) • Data (X.121) • Telex (F.69) • Land Mobile (E.212) • National • Private • ERMES (European Radio Messaging System) • Internet (IP) • WAP (Wireless Application Protocol) Client ID <p>This field corresponds to the <code>addr_npi</code> in the SMPP Protocol Specification. The <code>addr_ton</code> and <code>addr_npi</code> values tell the SMSC how to interpret the address found in the <code>address_range</code> field.</p>

Table 11-3 Edit SMPP Provider Page (continued)

Field	Description
Address Type of Number (TON)	<p>If applicable, enter the value provided to you by your service provider. (If your provider did not specify a value, leave the field set to Unknown.) The information in this field defines the type of number (TON) that users must use when specifying the Address Range field for SMS (SMPP) message notification in Cisco Unity Connection Administration and the Cisco Unity Assistant.</p> <p>Select the applicable value from the list:</p> <ul style="list-style-type: none"> • Unknown • International • National • Network Specific • User Number • Alphanumeric • Abbreviated <p>The Address TON field corresponds to the <code>addr_ton</code> in the SMPP Protocol Specification. The <code>addr_ton</code> and <code>addr_npi</code> values tell the SMSC how to interpret the address found in the <code>address_range</code> (Address Range) field.</p>
Address Range	<p>If applicable, enter the value provided to you by your service provider. (If your provider did not specify a value, leave the field blank.) The SMPP server uses the address range to communicate with the Cisco Unity Connection server. You may need to enter a set of addresses or a single address.</p> <p>This field corresponds to the <code>address_range</code> in the SMPP Protocol Specification.</p>
Owner	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • To restrict provider use, select a user as owner of the selected SMPP provider. Click the User button and then select the applicable user from the list. • To allow the SMPP provider to be used by all users on this server, select System as owner of the selected SMPP provider.

Table 11-3 Edit SMPP Provider Page (continued)

Field	Description
Data Coding	<p>If applicable, select the character set that you want each SMS message converted to when the messages are sent to the SMS device. (If your provider did not specify a value, select Default Alphabet.) For multilingual systems, consider creating a separate SMPP provider for each character set that you want to offer to users.</p> <p>Select the applicable character set:</p> <ul style="list-style-type: none"> • Default Alphabet (GSM 3.38), 7-bit characters • IA5/ASCII, 7-bit characters • Latin 1 (ISO-8859-1), 8-bit characters • Japanese (JIS), multi-byte characters* • Cyrillic (ISO-8859-5), 8-bit characters • Latin/Hebrew (ISO-8859-8), 8-bit characters • Unicode (USC-2), 16-bit characters • Korean (KS C 5601), multi-byte characters* <p>* For multi-byte character sets, most characters are 16 bits; some of the more common characters are eight bits.</p> <p>Not all cell phones support all character sets; most support the GSM 3.38 default alphabet.</p> <p>The number of characters that can fit into an SMS message is determined by the character set selected here. For 7-bit character sets, the limit is 160 characters; for 8-bit character sets, the limit is 140 characters; for 16-bit character sets, the limit is 70 characters; for multi-byte character sets, the limit is somewhere between 70 and 140 characters, depending on which characters make up the text of the message.</p>
Source Address	<p>If the SMPP Provider requires a source address for the server sending the message, enter the IP address for the Cisco Unity Connection server.</p> <p>If the SMPP Provider does not require a source address, enter the number that the user calls to check messages. The format and the number that you enter depends on the SMPP Provider. The provider may require that you include international country codes, beginning with a plus sign (+) and followed by the country code, area, city, or trunk code, and then the number for the device (for example, +12065551234). Do not start with a zero or the international dialing prefix. Do not include spaces, dashes, parentheses or other punctuation.</p> <p>Note that some SMPP Providers replace the number that you enter in the Source Address field with their own phone number. For an alternative method of including a call back number, try entering the number that the user calls to check messages in the Send field.</p>

Table 11-3 Edit SMPP Provider Page (continued)

Field	Description
Source Address NPI	<p>If applicable, enter the value provided to you by your service provider. (If your provider did not specify a value, leave the field blank.) The information in this field defines the numeric plan indicator that users can use when specifying the To and From fields for SMS (SMPP) message notification in Cisco Unity Connection Administration and the Cisco Unity Assistant.</p> <p>Select the applicable value from the list:</p> <ul style="list-style-type: none"> • Unknown • ISDN (E163/E164) • Data (X.121) • Telex (F.69) • Land Mobile (E.212) • National • Private • ERMES (European Radio Messaging System) • Internet (IP) • WAP (Wireless Application Protocol) Client ID <p>The Source Address NPI field corresponds to the <code>source_addr_npi</code> in the SMPP Protocol Specification. The <code>source_addr_ton</code> and <code>source_addr_npi</code> values tell the SMSC how to interpret the address found in the <code>source_addr</code> (From) field.</p>
Source Address TON	<p>If applicable, enter the value provided to you by your service provider. (If your provider did not specify a value, leave the field set to Unknown.) The information in this field defines the type of number (TON) that users must use when specifying the From field for SMS (SMPP) message notification in Cisco Unity Connection Administration and the Cisco Unity Assistant.</p> <p>Select the applicable value from the list:</p> <ul style="list-style-type: none"> • Unknown • International • National • Network Specific • User Number • Alphanumeric • Abbreviated <p>This field corresponds to the <code>source_addr_ton</code> in the SMPP Protocol Specification. The <code>source_addr_ton</code> and <code>source_addr_npi</code> values tell the SMSC how to interpret the address found in the <code>source_addr</code> (From) field.</p>

Table 11-3 Edit SMPP Provider Page (continued)

Field	Description
Destination Address TON	<p>If applicable, enter the value provided to you by your service provider. (If your provider did not specify a value, leave the field set to Unknown.) The information in this field defines the type of number (TON) that users must use when specifying the To field for SMS (SMPP) message notification in Cisco Unity Connection Administration and the Cisco Unity Assistant.</p> <p>Select the applicable value from the list:</p> <ul style="list-style-type: none"> • Unknown • International • National • Network Specific • User Number • Alphanumeric • Abbreviated <p>The Destination TON field corresponds to the <code>dest_addr_ton</code> in the SMPP Protocol Specification. The <code>dest_addr_ton</code> and <code>dest_addr_npi</code> values tell the SMSC how to interpret the address found in the <code>destination_addr</code> (To) field.</p>
Destination Address NPI	<p>If applicable, select the value provided to you by your service provider. (If your provider did not specify a value, leave the field set to Unknown.) The information in this field defines the numeric plan indicator that users can use when specifying the To and From fields for SMS (SMPP) message notifications in Cisco Unity Connection Administration and the Cisco Unity Assistant.</p> <p>Select the applicable value from the list:</p> <ul style="list-style-type: none"> • Unknown • ISDN (E163/E164) • Data (X.121) • Telex (F.69) • Land Mobile (E.212) • National • Private • ERMES (European Radio Messaging System) • Internet (IP) • WAP (Wireless Application Protocol) Client ID <p>This field corresponds to the <code>dest_addr_npi</code> in the SMPP Protocol Specification. <code>dest_addr_ton</code> and <code>dest_addr_npi</code> values tell the SMSC how to interpret the address found in the <code>destination_addr</code> (To) field.</p>

Table 11-3 Edit SMPP Provider Page (continued)

Field	Description
Allow to Replace Message	<p>Check this check box to have Cisco Unity Connection request that the SMSC or SMS device replaces one or more previously submitted message notifications with the latest one. Depending on whether the user device is turned on or off, message notifications are replaced as follows:</p> <ul style="list-style-type: none"> When the device is on, Connection submits message notifications to the SMSC, which forwards them to the device. If the source address, destination address, and protocol ID fields in a new message notification match the same fields in a previous one, the device replaces the previous one with the latest. When the device is off or otherwise disconnected from the GSM network, Connection submits message notifications to the SMSC. The SMSC replaces any message notifications that are still pending delivery with the latest one if the source address, destination address, and service type match the same fields in the new message notification. <p>In both scenarios, the user receives only the latest message notification.</p> <p>Note Service providers may not support some or all of the above functionality. For example, some providers may support replacing previous notifications only when the device is either turned on or off. Other providers may not support replacing previous notifications at all.</p> <p>This field corresponds to the <code>replace_if_present_flag</code> and the <code>protocol_id</code> fields in the SMPP Protocol Specification.</p>

See Also

- The “[Setting Up SMS \(SMPP\) Message Notifications](#)” section in the “Setting Up SMTP and SMS (SMPP) Message Notifications” chapter of the *System Administration Guide for Cisco Unity Connection*.

Conversation Configuration

Revised May 2009

Table 11-4 Conversation Configuration Page

Field	Description
Enable Remote Port Status Output	<p>When this check box is checked, Cisco Unity Connection is enabled to send real-time port status information over port 5000 to the Remote Port Status Monitor clients.</p> <p>Default setting: Check box not checked.</p>
IP Addresses Allowed to Connect for Port Status Monitor Output (Comma-Separated)	<p>Enter up to three IP addresses for the Remote Port Status Monitor clients that are allowed to connect to Cisco Unity Connection. You must separate the IP addresses with commas or semi-colons. Clients that do not have their IP address list here are refused access to Cisco Unity Connection.</p>

Table 11-4 Conversation Configuration Page (continued)

Field	Description
Save Speed and Volume Changes Made by User (Cisco Unity Connection Release 7.1 Only)	<p>When this check box is checked, speed and volume changes that the user makes while listening to messages or to the Cisco Unity Connection conversation will be saved as new default settings for the user.</p> <p>When this check box is not checked, any speed and volume changes that the user makes while listening to messages are in effect only for that individual message. Any speed and volume changes that the user makes while listening to the Connection conversation are in effect only for the duration of that phone session. (Note that the voice-recognition conversation is the only conversation that allows users to change the Connection conversation speed or volume by phone.)</p> <p>Default setting: Check box checked.</p>
Request Entry of User ID after Failed Password Entry from Known Extension	<p>When users log on to Cisco Unity Connection from a known extension, they are asked only for a password. When this check box is checked, if users enter an incorrect password, Connection asks the users to enter a user ID as well as a password on subsequent attempts. When this check box is not checked, Connection asks only for a password on re-entry attempts.</p> <p>Note If a user calls from an extension that is not associated with a user, Connection always requests a user ID.</p> <p>Default setting: Check box checked.</p>
Disable Identified User Messaging Systemwide	<p>When a user calls another user and the call is forwarded to the greeting of the called user, the ability of Cisco Unity Connection to identify that it was a user who left the message is referred to as identified user messaging (IUM). Some sites prefer to leave all messages as unidentified caller messages unless the user first logs on to Connection and then sends a message.</p> <p>Check this check box to disable IUM systemwide.</p>
Full Mailbox Check for Outside Caller Messages	<p>Indicates whether Cisco Unity Connection first determines if a user mailbox is full before allowing an outside caller to leave a message for the user. (The maximum size of a mailbox is determined by quota settings either on the Message Storage > Mailbox Quotas page or, if the quota is overridden for an individual user, on the Mailbox page for that user.)</p> <p>When this check box is checked, if the user mailbox is full, the outside caller is not allowed to leave a message.</p> <p>When this check box is not checked, Connection does not determine whether the mailbox is full; the outside caller is allowed to leave the message even if mailbox is full.</p> <p>Note that this setting is applicable only to outside callers. If a Connection user logs on and sends a message to another user, Connection always checks whether the user mailbox is full regardless of whether this setting is enabled.</p> <p>Default setting: Check box not checked.</p>
Enable Go to Message	<p>Check this check box to allow users to jump directly to a specific message number in their saved message stack. Uncheck this check box to disable this feature systemwide.</p> <p>Note that this setting is not available for the voice-recognition conversation.</p> <p>Default setting: Check box checked.</p>
Address Message Before Recording	<p>Check this check box to have Cisco Unity Connection prompt users to address a message first and then record it when they send or forward messages to other users or distribution lists.</p> <p>Default setting: Check box not checked.</p>

Table 11-4 Conversation Configuration Page (continued)

Field	Description
Use Star to Deactivate Notification Device	<p>By default, on a notification dialout, the person answering the phone can press 1 to deactivate outdials to the phone number that Cisco Unity Connection called.</p> <p>When this check box is checked, instead of pressing 1 to deactivate a device, the star key deactivates the device.</p> <p>When this check box is not checked, the 1 key is used to deactivate notification devices.</p> <p>Default setting: Check box not checked.</p>
Play Option to Turn Off Message Notification	<p>By default, on a notification dialout, the person answering the phone is given the option to deactivate message notifications to the phone number that Cisco Unity Connection called. This is helpful in cases where the wrong phone number was entered for the notification device.</p> <p>When this check box is checked, the person answering the phone is given the option to deactivate all message notifications to the device.</p> <p>When this check box is not checked, Connection does not offer the option to deactivate message notifications.</p> <p>Default setting: Check box checked.</p>
Disable Message Summary on Replay	<p>By default, when a user replays a message by phone, Cisco Unity Connection replays both the summary and the body of the message. Check the Disable Message Summary on Replay check box to change the Connection conversation so that it replays only the message body when a user replays a voice message.</p> <p>Note The change is only applicable to replaying voice messages.</p>
Disable Spelled Name Searches	<p>This setting disables the spelled name option for addressing a message. Note that this setting is not available for the voice-recognition conversation.</p>
Treat Skipped Messages as Saved	<p>You can change how Cisco Unity Connection behaves when a user chooses to skip a message. By default, when a user skips a message, it is marked new again and the message waiting indicator stays on.</p> <p>When this check box is checked and a user skips a message, the message is marked as saved, and the message waiting indicator is turned off.</p> <p>Default setting: Check box not checked.</p>
Play Receipt Reason Code	<p>By default, when users play a nondelivery receipt (NDR), Cisco Unity Connection plays the NDR reason code and then plays a prompt that explains why the user received the NDR. By hearing the reason code along with the reason prompt, users can eventually learn why an NDR was received without having to listen to the entire receipt. In addition, users can more easily communicate an NDR issue by specifying the reason code to support desk personnel.</p> <p>Uncheck this check box if you do not want Connection to play NDR reason codes.</p> <p>Note This setting affects users systemwide, regardless of their conversation style.</p>
Confirm Deletion of Deleted Messages	<p>By default, when users permanently delete a deleted message as they review deleted messages by phone, Cisco Unity Connection does not ask them to confirm the deletion. Check this check box to enable Connection to request confirmation from users before proceeding with the deletion.</p>

Table 11-4 Conversation Configuration Page (continued)

Field	Description
Multiple Message Delete Mode	<p>By default, when users press keys from the main menu to delete multiple deleted messages at once, Cisco Unity Connection allows them to choose which messages they want to delete; users can either delete their deleted voice messages or delete all of their deleted messages. You can change how Connection handles the way in which multiple deleted messages are deleted by adjusting the following values to specify what plays and what messages are deleted when users delete multiple deleted messages:</p> <ul style="list-style-type: none"> • 1—Users choose which messages are deleted; Connection prompts them: “To delete only your voice messages, press 1. To delete all messages, press 2.” (Default setting) • 2—Connection does not prompt users to choose which messages to delete; instead, Connection deletes all of their deleted voice messages. • 3—Connection does not prompt users to choose which messages to delete; instead, Connection deletes all of their deleted messages (voice messages, receipts, and email messages, as applicable). <p>Note that this setting affects users systemwide, regardless of their class of service (COS) settings and conversation style. This setting is not available for the voice-recognition conversation.</p>
System Transfers: Confirm Number Before Transfer	<p>By default, when a caller uses the System Transfer conversation, Cisco Unity Connection prompts the caller to confirm the transfer number before transferring the call (by releasing to the switch). Uncheck this check box if you do not want Connection to prompt callers to confirm the number before transferring calls.</p> <p>Note System transfers that are initiated from a greeting never ask callers to confirm the number that they entered when the Allow Transfers to Numbers Not Associated with Users or Call Handlers setting has been enabled for the greeting.</p>
Skip Recording of Greeting During Enrollment	<p>Check this check box so that Cisco Unity Connection does not prompt callers to record a greeting during enrollment.</p> <p>Default setting: Check box not checked.</p>
Time to Wait Between Spoken Words (in Milliseconds)	<p>Specify how long Cisco Unity Connection waits for a caller to say additional words before acting on the words already spoken.</p> <p>Default setting: 750 milliseconds.</p>
Voice Recognition Confirmation Confidence Threshold	<p>Use this setting to adjust the likelihood that Cisco Unity Connection prompts the voice recognition caller to confirm caller intentions. For example, if callers complain that the system mistakenly hears them say “cancel” or “hang up,” you can try increasing the value of this setting to prevent callers from accidentally committing actions they did not intend. Alternatively, if callers complain that the system prompts for confirmation too frequently, try adjusting this setting to a lower value.</p> <p>The range of valid entries is 0 to 100. When the value is set to 0, Connection never asks for confirmation; when the value is set to 100, Connection always asks for confirmation.</p> <p>A realistic range of values for this setting is 30 to 90. The default value should reliably filter out most errors and provide confirmation when necessary for most systems. Note that if the value is set too low, the system may improperly recognize and act on commands.</p> <p>Default setting: 60.</p>

Table 11-4 Conversation Configuration Page (continued)

Field	Description
Allow Voice Recognition Users to Speak Their Voice Mail Passwords	<p>Check this check box so that voice recognition users can say the digits in their voice mail passwords to log on when calling Cisco Unity Connection from their primary or alternate extensions. Connection attempts to match the spoken digits to the user voice mail password as an alternative to entering the digits on the keypad; it does not attempt to recognize the individual voice print of the user or otherwise apply biometrics to the login process.</p> <p>Default setting: Check box not checked.</p>
Use Advanced Name Dictionary for Voice Recognition	<p>Check this check box and restart the Connection Voice Recognizer service to have Cisco Unity Connection use the advanced name dictionary. Enabling this setting could impact system performance. We recommend that you do not make any changes to this setting unless the Cisco Technical Assistance Center (Cisco TAC) specifies the change.</p> <p>Default setting: Check box not checked.</p>
Maximum Call Transfer Attempts Allowed	<p>Specifies the maximum number of transfer attempts Cisco Unity Connection performs. Enter a number between 0 (zero) and 30.</p> <p>Default setting: 5 attempts.</p>
Wait Time in Seconds Between Call Transfer Attempts	<p>Specifies the wait time in seconds between call transfer attempts. Enter a number between 1 and 60 seconds.</p> <p>Default setting: 5 seconds.</p>
Require Users to Record Names at Enrollment	<p>By default, Cisco Unity Connection prompts users to record a voice name during first-time enrollment, but it does not prevent them from completing the enrollment process if they do not. When listing a user in directory assistance, Connection will play the display name of the user by using Text to Speech when the user does not have a recorded voice name. If you prefer to have all voice names played in the user voices, you may want to change how Connection handles first-time enrollment.</p> <p>Check this check box if you want to force users to record a voice name. When this check box is checked, users who do not record a voice name during first-time enrollment are not enrolled as Connection users and cannot access their messages. They hear the first-time enrollment conversation each time that they log on to Connection until they successfully enroll.</p> <p>Note This setting affects all users who are associated with the Connection server, regardless of their conversation style.</p>
System Broadcast Message: Retention Period (in Days)	<p>Specifies how long Cisco Unity Connection retains expired broadcast messages on the server. By default, Connection purges the WAV file and any data that is associated with a broadcast message 30 days after its end date and time.</p> <p>To change the retention period for expired broadcast messages, enter a number between 1 and 60. Enter the value in days.</p> <p>Default setting: 30 days.</p>
System Broadcast Message: Default Active Days	<p>Specify how long broadcast messages remain active when the messages are sent without a specified end date and time. By default, messages that are sent without an end date and time are active for 30 days.</p> <p>To change how long a message without an end date and time remains active, enter a number between 1 and 365. Enter the value in days.</p> <p>Note This setting does not affect broadcast messages that are set to play indefinitely.</p>

Table 11-4 Conversation Configuration Page (continued)

Field	Description
System Broadcast Message: Maximum Recording Length in Milliseconds	<p>Specify the maximum length of broadcast messages. By default, users can record broadcast messages up to 300,000 milliseconds (5 minutes) in length.</p> <p>To change the maximum recording length, enter a number between 60,000 (1 minute) and 3,600,000 (60 minutes). Enter the value in milliseconds.</p> <p>Note The maximum recording length for regular messages left by users is set on the applicable Edit Class of Service page. The maximum recording length for messages left for a user by unidentified callers is set on the Edit Message Settings page for the user.</p>
System Broadcast Message: Play Oldest Message First	<p>Specify the order in which Cisco Unity Connection presents broadcast messages to users. By default, the oldest broadcast messages play first. Uncheck this check box to change the playback order so that the newest broadcast messages are played first.</p> <p>Note This setting affects all users who are associated with the Connection server. The playback order that users specify for their new, saved, and deleted messages (as applicable) is unaffected by this setting.</p>
Use Last (Rather than First) Redirecting Number for Routing Incoming Call	<p>When this check box is checked, Cisco Unity Connection uses the last redirecting number for routing incoming calls.</p> <p>Default setting: Check box not checked.</p>
Apply User Accessibility Settings for Voice Mail Password Entry Conversation	<p>When this check box is checked, Cisco Unity Connection applies individual user accessibility settings during the password collection conversation when users call from a known extension (their primary or an alternate extension). When this check box is checked, the following accessibility settings are applied:</p> <ul style="list-style-type: none"> • Conversation Speed • Conversation Volume • Language • Time to Wait for First Touchtone or Voice Command • Time to Wait for Additional Key Presses When Entering Names, Extensions, and Passwords <p>When this check box is not checked, individual user accessibility settings are not applied until after the user is authenticated by entering the voice mail password.</p> <p>Default setting: Check box not checked.</p>
Cross-Server Handoff Request DTMF	The sequence of DTMF tones that identify a call as a cross-server logon or transfer. For servers to be able to successfully hand off calls to one another, they must be set to use the same request DTMFs.
Cross-Server Handoff Response DTMF	The sequence of DTMF tones used to respond to a call identified as a cross-server logon or transfer. For servers to be able to successfully hand off calls to one another, they must be set to use the same response DTMFs.
Cross-Server Handoff Response Interdigit Timeout	The interdigit timeout setting used when listening for the handoff response DTMFs.
Cross-Server Data Packet Listen First Digit Timeout	The first digit timeout setting used when listening for the data packet DTMFs. The data packet contains the information required to process the handoff on the destination server.

Table 11-4 Conversation Configuration Page (continued)

Field	Description
Cross-Server Data Packet Listen Interdigit Timeout	The interdigit timeout setting used when listening for the data packet DTMFs.
Play Prompt During Cross-Server Handoff	When this check box is checked, Cisco Unity Connection plays a “Please wait...” prompt to the caller before attempting to do a cross-server logon or transfer. When this check box is not checked, the prompt is not played to the caller. We recommend that you check this check box, because the handoff process can take several seconds or longer, during which the caller is left on the line.
Respond to Cross-Server Handoff Requests	When this check box is checked, Cisco Unity Connection responds to cross-server handoff requests from other Connection locations. When this check box is not checked, Connection does not respond to these requests.
Maximum Age of Names in Addressing Priority Lists	Specifies the maximum age, in days, of names in addressing priority lists. A name is removed if it has not been modified for this number of days. If this value is set to 0, then names are not removed from addressing priority lists based on age.
Maximum Number of Names in a User’s Addressing Priority List	Specifies the maximum number of names that a user can have in an addressing priority list. If this value is set to 0, then the number of names in addressing priority lists is not limited.
Dial Prefix for Live Reply to Unidentified Callers	A prefix applied to the ANI that is dialed on live replies to unidentified callers. This would typically be a trunk access code or other identifying ID that the switch can use for processing the number correctly. The prefix is applied only when the length of the ANI is equal to or greater than the Minimum Number of Digits Required for Prepending Live Reply Dial Prefix setting.
Minimum Number of Digits Required for Prepending Live Reply Dial Prefix	The Dial Prefix for Live Reply to Unidentified Callers setting is applied only when the length of the ANI is equal to or greater than the number set here. A value of 0 means that live replies to unidentified callers never use the prefix.

See Also

- The “[Changing Conversation Settings for All Users](#)” chapter of the *System Administration Guide for Cisco Unity Connection*.

Messaging Configuration (Cisco Unity Connection 7.1)

Added May 2009

Table 11-5 *Messaging Configuration Page*

Field	Description
Allow Relaying of Private Messages	<p>Check this check box so that Cisco Unity Connection relays messages that are marked private for users who have one or more message actions configured to relay messages (or to accept and relay messages). Connection sets the private flag on the message when relaying a private message.</p> <p>Uncheck this check box to prevent Connection from relaying private messages. When this check box is not checked, the message sender receives a non-delivery receipt (NDR) when Connection receives a message that it cannot relay because the message is marked private, and Connection does not accept or relay the message. For example, if Connection is configured to accept and relay voice messages that are sent to User A, and User B sends a private voice message to User A, Connection sends an NDR to User B and discards the message without placing the message in the Connection mailbox for User A or relaying a copy to the relay address for User A.</p> <p>Default setting: Check box checked.</p>
Allow Relaying of Secure Messages	<p>Check this check box so that Cisco Unity Connection relays messages that are marked secure for users who have one or more message actions configured to relay messages (or to accept and relay messages). Connection relays secure messages as regular messages.</p> <p>Uncheck this check box to prevent Connection from relaying secure messages. When this check box is not checked, the message sender receives a non-delivery receipt (NDR) when Connection receives a message that it cannot relay because the message is marked secure, and Connection does not accept or relay the message. For example, if Connection is configured to accept and relay voice messages that are sent to User A, and User B sends a secure voice message to User A, Connection sends an NDR to User B and discards the message without placing the message in the Connection mailbox for User A or relaying a copy to the relay address for User A.</p> <p>Default setting: Check box not checked.</p>

See Also

- The “[Task List for Configuring IMAP Access in Cisco Unity Connection](#)” section in the “Configuring IMAP Settings” chapter of the *System Administration Guide for Cisco Unity Connection*.

Telephony Configuration

Revised May 2009

Table 11-6 *Telephony Configuration Page*

Field	Description
Minimum Recording Duration in Milliseconds for Termination Warning	<p>Enter the minimum length of message recordings, in milliseconds, before Cisco Unity Connection monitors the recording length to determine whether to play a termination warning. Only message recordings that are allowed to exceed this length are monitored by Connection to determine whether they are too long. Enter a value between 20,000 and 1,200,000 milliseconds.</p> <p>Default setting: 30,000 milliseconds.</p>

Table 11-6 Telephony Configuration Page (continued)

Field	Description
Port Watchdog Threshold in Minutes	Enter the time, in minutes, that a port can be off hook before it is considered to be locked. When a port reaches this threshold, Cisco Unity Connection logs an error. To review errors, see the Real-Time Monitoring Tool. We recommend a setting greater than 30 minutes. Default setting: 240 minutes.
Leading Silence Timeout for Recordings in Milliseconds	Enter the length of time, in milliseconds, after which Cisco Unity Connection ends the message, greeting, or recorded name if the user or caller has not begun speaking. A value lower than two or three seconds may not give the user or caller enough time to begin speaking. Default setting: 5,000 milliseconds.
Trailing Silence Timeout for Recordings in Milliseconds	Enter the length of silence, in milliseconds, that Cisco Unity Connection uses to detect the end of a long recording. When a pause of this length occurs, Connection assumes that the speaker has finished the recording. Default setting: 3,000 milliseconds.
Minimum Recording Duration in Milliseconds	Enter the minimum length of recordings, in milliseconds, for messages or greetings. This setting does not apply to recorded voice names. Enter a value between 0 and 5,000 milliseconds. Default setting: 1,000 milliseconds.
Recording Termination Warning Time in Milliseconds	Enter the length of time, in milliseconds, before reaching the maximum allowed recording time when Cisco Unity Connection plays a termination warning prompt. When the warning is played during a recording session, Connection waits the amount of time indicated in this field before terminating the recording session. Connection plays the warning only for message recordings, not for other recordings such as greetings or recorded names. If the setting is 0, the termination warning feature is disabled. Default setting: 15,000 milliseconds.
Maximum Recording Time in Milliseconds	Enter the maximum recording time, in milliseconds, for messages. This setting does not apply to greetings, recorded voice names, and recordings other than messages. Enter a value between 0 and 3,600,000 milliseconds (one hour). Default setting: 1,200,000 milliseconds (20 minutes).
Minimum Number of Ports (per Phone System) for Answering Calls	Enter the minimum number of voice messaging ports for answering calls that Cisco Unity Connection requires for each phone system integration. Enter a value between 0 and 256. Default setting: 1.
Live Record Beep Interval in Milliseconds	Enter the interval, in milliseconds, between beeps when a phone conversation is being recorded by using the live record feature. (The live record feature is supported only for Cisco Unified Communications Manager integrations.) If the setting is blank, the interval is 15,000 milliseconds. If the setting is 0, the beep is disabled. If the setting is greater than 0, the interval is that number of milliseconds. Default setting: 15,000 milliseconds.
Differentiated Services Code Point (DSCP) Value for Call Signaling Connections	Enter the Differentiated Service Code Point (DSCP) value for call signalling packets. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. Default setting: 24.

Table 11-6 Telephony Configuration Page (continued)

Field	Description
Differentiated Services Code Point (DSCP) Value for the RTP (Audio) Connection	Enter the Differentiated Service Code Point (DSCP) value for the RTP (or audio) packets. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. Default setting: 46.

See Also

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

Report Configuration

Revised May 2009

Table 11-7 Report Configuration Page

Field	Description
Maximum Events Allowed in Audit Log	Enter the maximum number of audit events allowed in the audit log table. When the maximum threshold is reached, the oldest events are removed to make room for new ones. Enter a number between 1 and 100,000. Default setting: 100,000.
Enable Security Log	This setting enables and disables the security log. If this setting is set to disabled, stored procedures stop writing to the security log. Default setting: Check box checked.
Maximum Events Allowed in Security Log	The maximum number of security events allowed in the security log table. Enter a value between 1 and 100,000 events. When the maximum threshold is reached, the oldest events are removed to make room for new ones. Default setting: 100,000.
Milliseconds Between Data Collection Cycles	(<i>Cisco Unity Connection 7.0</i>) Enter the amount of time to wait (in milliseconds) between cycles of gathering report data. Default setting: 1,800,000 milliseconds (30 minutes).
Minutes Between Data Collection Cycles	(<i>Cisco Unity Connection 7.1 or later</i>) Enter the amount of time to wait (in minutes) between cycles of gathering report data. Default setting: 30 minutes.
Days to Keep Data in Reports Database	Enter the number of days to keep data in the reports database. Default setting: 90 days. Note Even if you specify more than this number of days in the time range for the report you are generating, the number of days of data is limited by what you set here.

Table 11-7 Report Configuration Page (continued)

Field	Description
Maximum Records in Report Output	<p>Maximum number of records that can be included in the report output. Enter a value between 5,000 and 30,000.</p> <p>Default setting: 25,000 records.</p> <p>However, note the following:</p> <ul style="list-style-type: none"> • If the report output is generated to HTML, the maximum records returned in the output is 250 even if Maximum Records in Report Output is set higher than 250. • The Maximum Records in Report Output setting for the User Message Activity Report has been restricted to 15,000 records—rather than the default of 25,000 records—because of the size of the report.
Minimum Records Needed to Display Progress Indicator	<p>Enter a value between 1 and 10,000. If the number of records in the requested report is more than this value, a report confirmation page appears prior to running a report and a progress indicator is displayed while the report is being generated. The purpose of the progress indicator is to warn that the requested report is large and likely to take a long time to complete. In Cisco Unity Connection, reports are generated from within a browser, and the browser session must be kept open while the report is being generated. Depending on the size of the database, and the type of report being generated, a report can take a long time to generate; meanwhile, you are unable to use the browser, and must keep the Cisco Unity Connection Administration session open.</p> <p>Default setting: 2,500 records.</p>
Reports Database Size (as a Percentage of Capacity) After Which the Reports Harvester Is Disabled	<p>Enter the maximum percentage of the disc capacity that the reports database is allowed to occupy. When the reports database reaches this percentage, the Connection Report Data Harvester service (in Cisco Unity Connection Serviceability) is deactivated so that the database does not grow.</p> <p>Default setting: 80 percent.</p>
Enable Audit Log	<p>Check this check box to enable the audit log. Uncheck this check box to disable the audit log. When this check box is unchecked, stored procedures stop writing to the audit log.</p> <p>Default setting: Check box checked.</p>

See Also

- The “[Generating Reports](#)” chapter of the *System Administration Guide for Cisco Unity Connection*.

Connection Administration Configuration

Revised May 2009

Table 11-8 Connection Administration Configuration Page

Field	Description
Cisco Unified Mobile Advantage: Accept Self-signed Certificates for Event Service Subscription Notifications	<p>Check this check box so that Cisco Unity Connection accepts self-signed certificates from the Cisco Unified Mobility Advantage server.</p> <p>Uncheck this check box so that Cisco Unity Connection does not accept self-signed certificates from the Cisco Unified Mobility Advantage server.</p> <p>Default setting: Check box checked.</p>
Voice Mail Web Service: Applications Can Cache the Cisco Unity Connection Password	<p>Check the check box to allow applications that use the Voice Mail Web Service to cache the Cisco Unity Connection password. Uncheck the check box so that applications that use the Voice Mail Web Service are not allowed to cache the Cisco Unity Connection password.</p> <p>Default setting: Check box checked.</p>
Voice Mail Web Service: Session Timeout (in Seconds)	<p>Enter the length of time after which Cisco Unity Connection will close an idle Voice Mail Web Service session.</p> <p>Default setting: 300 seconds (5 minutes).</p>
Voice Mail Web Service: Pilot Number for TRAP Connections	<p>Enter the pilot number of the applications that use Voice Mail Web Service. When Cisco Unity Connection dials this number, Voice Mail Web Service initiates a TRAP session.</p> <p>Default setting: Blank.</p>
Voice Mail Web Service: Pilot Number for Voice Mail	<p>Enter the pilot number for Cisco Unity Connection. This setting applies to applications that use the Voice Mail Web Service.</p> <p>Default setting: Blank.</p>
Administration Session Timeout (in Minutes)	<p>Indicates the length of time that the browser can be left unattended before Cisco Unity Connection automatically logs the user off of Cisco Unity Connection Administration.</p> <p>The minimum setting is 1 minute; the maximum is 120 minutes.</p> <p>Default setting: 5 minutes.</p>
Display Schedules in 24-Hour Format	<p>Specifies the default time format for displaying schedules in Cisco Unity Connection Administration. Check this check box for schedules to be shown in the time format of a 24-hour clock. Uncheck this check box for schedules to be shown in the time format of a 12-hour clock.</p>
Host Name/Address for Link to Cisco PCA in Notification Messages	<p>(Optional) For Cisco Unity Connection clusters, enter the IP address or host name that is valid even when one of the Connection servers is not available. When sending notification messages to SMTP devices, Connection uses this name to construct a URL in the format “http://<host name>/ciscopca” that it includes as a link to the Cisco PCA. If this field is left blank, the server name of the Connection server that sends the notification is used for the link to the Cisco PCA.</p>
Database Proxy: Service Shutdown Timer (in Days)	<p>Enter the number of days until the database proxy service is automatically stopped. A value of 0 disables the service.</p> <p>Enter a value between 0 and 999.</p> <p>Default setting: 0.</p>

Table 11-8 Connection Administration Configuration Page (continued)

Field	Description
Database Proxy: Maximum Simultaneous Connections	Enter the maximum number of simultaneous connections allowed by the database proxy. Note that some remote administration tools require more than one connection at a time. Enter a value between 1 and 10. Default setting: 10.

See Also

- The “[Creating a Cisco Unified Mobility Advantage Integration](#)” chapter of the *System Administration Guide for Cisco Unity Connection*.
- The “[Remote Database Administration Tools](#)” section in the “Administrative Tools” chapter of the *System Administration Guide for Cisco Unity Connection*.

TRAP Configuration

Table 11-9 TRAP Configuration Page

Field	Description
Number of Seconds Phone Is Idle Before TRAP Times Out (Cisco Unity Connection 7.1 Only)	When a Telephone Record and Play (TRAP) session is idle longer than the value set here, Cisco Unity Connection disconnects the session. Enter a value between 0 (zero) and 600 seconds. A value of zero means that TRAP sessions never time out. Default setting: 60 seconds.
Number of Rings for a TRAP Dial-Out	Enter a value between 1 and 10 rings. Default setting: 4 rings.

See Also

- The “[Setting Up Playback and Recording Devices for the Media Master](#)” chapter of the *User Workstation Setup Guide for Cisco Unity Connection*.

Edit Disk Capacity Configuration

Table 11-10 Edit Disk Capacity Configuration Page

Field	Description
If the Disk Exceeds This Percent Full, Measures Will Be Taken to Not Allow New Files to Be Created	Specify a maximum capacity for the hard disk on which messages and greetings are stored. When that hard disk fills to the specified percentage limit, the Cisco Unity Connection conversation changes, and Connection users are no longer allowed to send voice messages to other Connection users. Connection also logs an error, which can be viewed in the Real Time Monitoring Tool, on the Tools > SysLog Viewer page. Outside callers can still leave voice messages until the hard disk fills up. Note that you can still send a broadcast message even when the hard disk exceeds the specified limit.

See Also

- The “[Message Storage](#)” section in the “Messaging” chapter of the *System Administration Guide for Cisco Unity Connection*.

PCA Configuration

Table 11-11 **PCA Configuration Page**

Field	Description
Cisco PCA Session Timeout (in Minutes)	<p>Indicates the length of time that the browser can be left unattended before Cisco Unity Connection automatically logs the user off of the Cisco Personal Communications Assistant (PCA).</p> <p>The minimum setting is 1 minute; the maximum is 1,440 minutes.</p> <p>Default setting: 20 minutes.</p>
Unity Inbox: Disable Save Recording As Option in Media Master	<p>Check this check box to disable the Save Recording As option in the Media Master.</p> <p>By default, except for private or secure messages, users can save their messages as WAV files to their hard disks by using the Save Recording As option available on the Options menu on the Media Master in the Cisco Unity Inbox. As an added security measure, you can disable the Save Recording As option so that users cannot save any messages to their hard disks.</p> <p>Regardless of whether the Save Recording As option is available on the Media Master in the Cisco Unity Inbox, users can still use the option in the Cisco Personal Communications Assistant web tools to save greetings or recorded names.</p> <p>Consider that by preventing users from archiving messages, users may choose to retain messages in their Inboxes and Deleted Items folders longer.</p> <p>Changing this setting affects all users who are associated with the Cisco Unity Connection server.</p>
Unity Inbox: Message Deletion Confirmation Mode	<p>By default, when users delete messages from the Cisco Unity Inbox, they are not asked to confirm the deletions unless deleting the item will delete it permanently. You can change this setting to have Cisco Unity Connection ask users to confirm the deletion every time that they delete messages from the Cisco Unity Inbox, or you can specify that the Cisco Unity Inbox never asks users to confirm deletions.</p> <p>Enter one of the following values:</p> <ul style="list-style-type: none"> • 0—Ask users to confirm all deletions. • 1—Ask users to confirm only the deletions that will be permanent. For users who belong to a class of service that retains deleted items in a Deleted Items folder, the Cisco Unity Inbox asks users to confirm deletions only when they delete items in the Deleted Items folder. For those who belong to a class of service that does not retain deleted items, the Cisco Unity Inbox confirms deletions of new and saved items, as they would be permanently deleted. • 2—Never ask users to confirm their deletions. <p>Note Changing this setting affects all users who are associated with the Connection server.</p> <p>Default setting: 1.</p>

See Also

- The “[Access to Voice Messages from the Cisco Unified Personal Communicator](#)” and “[Cisco Unity Inbox](#)” sections in the “Setting Up Features and Functionality That Are Controlled by Class of Service” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

RSS Configuration

Table 11-12 RSS Configuration Page

Field	Description
Allow Insecure RSS Connections	When enabled, insecure connections (those that do not use SSL) are allowed access to the RSS feed. Note that when using an RSS reader that does not support secure connections, if this check box is checked, the username and password are transmitted unencrypted over the network.

See Also

- The “[Configuring Access to RSS Feeds of Voice Messages](#)” section in the “Messaging” chapter of the *System Administration Guide for Cisco Unity Connection*.

Cluster Configuration

Table 11-13 Cluster Configuration Page

Field	Description
Deactivate Server with Secondary Status When Replication Is Backlogged	<p>(<i>Cisco Unity Connection cluster only</i>) When replication between the Cisco Unity Connection cluster servers is backlogged, one of the servers may have stopped functioning.</p> <p>Check this check box so that the server with Secondary status automatically changes server status when replication is backlogged.</p> <p>Uncheck this check box so that the server with Secondary status does not automatically change server status when replication is backlogged.</p> <p>Default setting: Check box not checked.</p>
Automatically Change Server Role When the Publisher Server Fails	<p>(<i>Cisco Unity Connection cluster only</i>) Check this check box so that the server with Secondary status automatically changes server status when the publisher server stops functioning.</p> <p>Uncheck this check box so that the server with Secondary status does not automatically change server status when the publisher server stops functioning.</p> <p>Default setting: Check box checked.</p>

See Also

- The “[Configuring a Cisco Unity Connection Cluster](#)” chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection*.

Fax Configuration

Table 11-14 Fax Configuration Page

Field	Description
Faxable File Types	Enter the file extensions (separated by commas) that Cisco Unity Connection keeps in messages that are delivered to the fax server. Connection removes all files with other file extensions before delivering the message to the fax server. Default setting: tif,txt,bmp,doc.
Subject Prefix for Notification of a Successful Fax	Enter the prefix that the fax server adds to the Subject field of fax reports. When Cisco Unity Connection detects this prefix, it generates a delivery receipt and places it in the user mailbox. Default setting: [Fax Success].
Subject Prefix for Notification of a Failed Fax	Enter the prefix that the fax server adds to the Subject field of fax reports. When Cisco Unity Connection detects this prefix, it generates a non-delivery receipt and places it in the user mailbox. Default setting: [Fax Failure].

See Also

- The “[Configuring the Cisco Fax Server](#)” section in the “Creating a Cisco Fax Server Integration” chapter of the *System Administration Guide for Cisco Unity Connection*.

External Services Configuration

Table 11-15 External Services Configuration Page

Field	Description
Default Advanced Notification Interval (In Minutes)	<i>(Calendar integrations only)</i> Enter the length of time (in minutes) before a meeting occurs that users receive a reminder of the meeting. Default setting: 2 minutes.
Number of Hours of Calendar Data to Cache (In Hours)	<i>(Calendar integrations only)</i> Enter the amount of the upcoming Outlook calendar data (in hours) that is cached for each user who is configured for a calendar integration. This setting is useful to reduce the impact when the network connection to the Exchange server is temporarily lost. A larger number increases the size of the database while reducing the impact on meeting notifications and Personal Call Transfer Rules when the network connection to the Exchange server is temporarily lost. A smaller number reduces the size of the database while increasing the impact on meeting notifications and Personal Call Transfer Rules when the network connection to the Exchange server is temporarily lost. Default setting: 48 hours.

Table 11-15 External Services Configuration Page (continued)

Field	Description
Normal Calendar Caching Poll Interval (In Minutes)	<p>(<i>Calendar integrations only</i>) Enter the length of time (in minutes) that Cisco Unity Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.</p> <p>A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.</p> <p>A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.</p> <p>Default setting: 30 minutes.</p>
Short Calendar Caching Poll Interval (In Minutes)	<p>(<i>Calendar integrations only</i>) Enter the length of time (in minutes) that Cisco Unity Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently. The users who benefit from this setting must have the Use Short Calendar Caching Poll Interval check box checked on their Edit User Basics page in Cisco Unity Connection Administration.</p> <p>A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.</p> <p>A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.</p> <p>Default setting: 30 minutes.</p>
Maximum External Service Response Time (In Seconds)	<p>Enter the maximum length of time (in seconds) that Cisco Unity Connection waits in one of the following circumstances for a response from a remote server that is connected as an external service:</p> <ul style="list-style-type: none"> Establishing a connection. Performing a protocol operation (for example, IMAP, WebDAV, or SOAP). <p>A larger number may be necessary when the remote server is heavily loaded, connected across a WAN, or is slow to respond. A larger number may also cause longer pauses in the Connection conversation or the Cisco Personal Communications Assistant when data is being provided by the remote server.</p> <p>A smaller number is possible when the remote server is quick to respond. A smaller number reduces pauses in the Connection conversation or the Cisco Personal Communications Assistant when data is being provided by the remote server.</p> <p>Default setting: 4 seconds.</p>

See Also

- The “[Configuring Access to Emails in an External Message Store](#)” chapter of the *System Administration Guide for Cisco Unity Connection*.
- The “[Creating Calendar Integrations](#)” chapter of the *System Administration Guide for Cisco Unity Connection*.

