CHAPTER 13

System Settings

Configuration Settings Page

Table 13-1 System > Configuration > Settings Page

Field	Considerations
Default Schedule	Select the default schedule, which is used for all Cisco Unity operations unless specifically changed for a call handler, subscriber account, or call routing table. Default: Weekdays.
Use 24-Hour Time Format for Conversation and Schedules	Check this check box to use a 24-hour time format for all Cisco Unity operations. For example, 1:00 p.m. is shown as 13:00 in the Cisco Unity Administrator, and subscribers hear 13:00 when listening to the timestamps for their messages by phone. When this check box is left unchecked, Cisco Unity uses the 12-hour clock format as the system default.
Enable Spelled Name Search	Check this check box to allow subscribers to address messages to other subscribers by spelling the subscriber first or last name by phone. In addition, when this check box is checked, subscribers who are editing private lists can search for subscribers by spelling the subscriber name by phone. Addressing by name requires lettered keypads on subscriber phones. Note that checking this check box does not prevent subscribers from searching for subscribers by entering subscriber extensions by phone when editing private lists or addressing messages. In the subscriber conversation, subscribers can switch between addressing by name and addressing by extension by pressing ## or 00 at any time. When this check box is not checked, subscribers can search for subscribers by phone only by entering subscriber extensions. The option to address by spelled name cannot be used on the Subscribers > Conversation page and in the Cisco Unity Assistant. Default: Check box checked.

Table 13-1 System > Configuration > Settings Page (continued)

Field	Considerations
Play the "Still Searching..." Prompt	Indicate how many times Cisco Unity should play a "Still searching..." prompt when searching for subscriber messages. Cisco Unity searches for two seconds and then plays the "Still searching..." prompt. When Cisco Unity has played the prompt the number of times that you specify, it searches for messages for two more seconds and then cancels the search. For example, if you set this to two times, Cisco Unity searches for messages for approximately 10 seconds before canceling the search and prompting the subscriber to either enter new search criteria or play any search results. This setting does not enable the Message Locator feature for subscribers. You specify whether subscribers can use the Message Locator feature on the Features page for subscriber templates and individual subscribers. Default: Two times.
Responding to Phone Menus	For each caller, you can specify the following: • How long Cisco Unity waits for the subscriber to press a first key after playing a menu. This setting is also known as "First Digit Timeout." The range of valid entries is 500 to 10,000 milliseconds. Default: 5,000 milliseconds. • How long Cisco Unity waits for additional key presses after the subscriber has pressed a key when entering subscriber names or extensions to address a message, to update passwords, to change call transfer or message notification numbers, and so on. This setting is also known as "Input Interdigit Timeout." The range of valid entries is 1,000 to 10,000 milliseconds. Default: 3,000 milliseconds. • How long Cisco Unity waits for additional key presses after the subscriber has pressed a key that represents the first digit of more than one possible key combination in a particular phone menu. (For example, in the After Message menu for the standard conversation, subscribers can press 4 to reply to a message, 42 to reply to all, or 44 to call the subscriber.) This also applies when using ## to switch addressing modes. This setting is also known as "Phone Menu Interdigit Timeout." The range of valid entries is 250 to 10,000 milliseconds. Default: 1,500 milliseconds. • How many times Cisco Unity repeats a menu if the subscriber has not responded to the menu. The range of valid entries is 0 to 250. Default: 3. **Note** Use caution when significantly increasing the number of times that Cisco Unity repeats a menu for subscribers. In the event that a subscriber puts a call to Cisco Unity on hold and forgets to return to it, or if the call is not disconnected as expected when the subscriber hangs up, Cisco Unity can tie up a voice port for long periods of time by repeating a phone menu. The values that you specify for the above settings control the phone menus for conversations that are heard by outside callers and subscribers. For security reasons, you cannot change timeouts for the conversations played to validate subscriber IDs and passwords.

Table 13-1 System > Configuration > Settings Page (continued)

Field	Considerations
RSA Two Factor	Check this check box to enable enhanced phone security, which uses RSA two-factor user authentication. To use enhanced phone security, an ACE/Server must be installed and configured for your system. Additionally, you must create a new class of service (COS) or modify an existing COS for the subscribers who are using enhanced phone security. To disable enhanced phone security, uncheck this check box, and then change every affected COS to use regular phone security. Otherwise, subscribers who are members of an enhanced phone security COS will not be allowed to log on to Cisco Unity. Default: Check box not checked.
Disable Identified Subscriber Messaging	Check this check box to disable identified subscriber messaging (ISM) systemwide. ISM affects what subscribers hear when they call other subscribers from their primary or alternate extensions and are forwarded to the greetings of the subscribers they call. If they then leave a message, ISM affects what the called subscriber hears and can do when listening to the message. When ISM is enabled, Cisco Unity recognizes that the calling extension is associated with a subscriber and accordingly plays the internal greeting of the called subscriber. Additionally, when the called subscriber later listens to the message, Cisco Unity plays the recorded voice name of the subscriber who left the message and allows the called subscriber to record a reply. This field is applicable only when the phone system provides caller and called party information to Cisco Unity. It is a system-wide setting that is not configurable for an individual subscriber or subscriber template. Regardless of whether ISM is enabled, when a subscriber logs on to the Cisco Unity conversation before sending a message (“Press 2 to send a message”), Cisco Unity correctly identifies the message as being from the subscriber. Default: Check box not checked.
Cisco Personal Communications Assistant (PCA)	Enter the URL for the Cisco Personal Communications Assistant (PCA) so that it is automatically included as a link in the body of the e-mail message that is sent to subscribers who have Cisco Unity Inbox message notifications set up. (Subscribers use the Cisco PCA to access their Cisco Unity Inboxes.) Note that the Media Master, which is displayed on many Cisco PCA pages, is not available across a firewall that blocks DCOM communications. You can set up Cisco Unity Inbox message notification on the message notification pages for subscribers or subscriber templates.
Cleanup Interval for Logger Data Files in Days	Indicate how often data files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files. Log-based Cisco Unity reports are based on the data stored in these files. Default: Seven days.
Cleanup Interval for Logger Diagnostic Files in Days	Indicate how often diagnostic files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files. Default: Seven days.
Cleanup Interval for Report Files in Days	Indicate how often report files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files. Note that you specify how long Cisco Unity stores the data used in log-based reports in the Cleanup Interval for Logger Data Files in Days field. Default: Seven days.

Table 13-1 System > Configuration > Settings Page (continued)

Field	Considerations
Replicate Cisco Unity Directory Objects	Choose Changed Objects to manually synchronize changes from Active Directory into the Cisco Unity SQL Server database. For example, changing the distribution list by which the directory handler is scoped requires a synchronization. Synchronization takes place automatically when the Cisco Unity directory services (AvDSAD and AvDSGlobalCatalog) poll the directory for any changes to be applied to the SQL Server database, which usually occurs within 15 to 20 minutes after the directory handler scope change is made in the Cisco Unity Administrator. However, you can also initiate the synchronization immediately by choosing Changed Objects. Choose All Objects only if Cisco Unity has been down for a considerable length of time.
Cisco Unity Computer Settings	*Display only.* Shows the name of the Cisco Unity server and the name of the Active Directory domain of which the Cisco Unity server is a member.
Fax Settings	Shows the name of the fax domain.
Disk Usage	*Display only.* Shows, in megabytes, the total, used, and free disk space on the Cisco Unity server.
Display Fields Required for Cisco Unity Bridge Networking on Subscribers Profile Page *(used only when the Bridge Networking option is configured for messaging with Octel systems)*	Check this check box to display the Unity Node Serial Number and Legacy Mailbox ID fields on the Subscribers Profile and Add Subscriber pages. The Unity Node Serial Number and Legacy Mailbox ID are required for all Cisco Unity subscribers who will be messaging with subscribers on an Octel system via the Cisco Unity Bridge. Without these numbers, a Cisco Unity subscriber cannot send messages to nor receive messages from Octel subscribers. Default: Check box not checked.
Substitute Recipient	Select the subscriber or public distribution list that will receive messages left for a call handler or interview handler, if the subscriber originally configured for this purpose is at any time deleted in the Cisco Unity Administrator. By default, the Example Administrator is configured as the Substitute Recipient. We recommend that you review this setting periodically, and update it if you wish to use a different substitute, so that these entities can be properly reassigned any time a subscriber is deleted.
Substitute Owner	Select the subscriber or public distribution list to which Cisco Unity will assign ownership of a distribution list, call handler, directory handler, or interview handler, if the subscriber originally configured for this purpose is at any time deleted in the Cisco Unity Administrator. Select a recipient type from the list, then click Select Subscriber or Select Distribution List. By default, the Example Administrator is configured as the Substitute Owner. We recommend that you review this setting periodically, and update it if you wish to use a different substitute, so that these entities can be properly reassigned any time a subscriber is deleted.
Substitute After Message Call Handler	Select the call handler that will be associated with the After Message Action setting (on a subscriber account, subscriber template, or call handler) or with the After Interview Action setting (on an interview handler), if the subscriber originally configured for this purpose is at any time deleted in the Cisco Unity Administrator. By default, the Goodbye call handler is configured as the Substitute After Message Call Handler. We recommend that you review this setting periodically, and update it if you wish to use a different substitute, so that these entities can be properly reassigned any time a subscriber is deleted.

Table 13-1 System > Configuration > Settings Page (continued)

Field	Considerations
Substitute Exit Call Handler	Select the call handler that will be associated with the If Caller Exits setting on a directory handler, if the subscriber originally configured for this purpose is at any time deleted in the Cisco Unity Administrator. By default, the Goodbye call handler is configured as the Substitute Exit Call Handler. We recommend that you review this setting periodically, and update it if you wish to use a different substitute, so that these entities can be properly reassigned any time a subscriber is deleted.

Configuration Recordings Page

Table 13-2 System > Configuration > Recordings Page

Field	Considerations
Allowed Time for Recording in Milliseconds	Select the number of milliseconds for the DTMF clip length. This setting indicates how much to truncate the end of a recording when a message is terminated with a touchtone. Default: 170 milliseconds.
Allowed Time for Short Recording in Seconds	Select the number of seconds that Cisco Unity uses as a cutoff for short and long recordings. Recordings shorter than this number are considered to be a short recording; recordings longer than this number are considered to be a long recording. Default: Ten seconds.
Allow How Much Silence Before Time Out in Seconds	Select the number of seconds after which Cisco Unity will end the message, greeting, or recorded name if the subscriber or caller has not begun speaking. A value lower than two or three seconds may not give the subscriber or caller enough time to begin speaking. Default: Five seconds.
Discard Any Recording Less Than in Seconds	Select the minimum length of recordings, in seconds, for messages or greetings. Default: One second.
Short Recording (Short Recording Trail Limit or Less)	Select the number of seconds of silence that Cisco Unity uses to detect the end of a short recording. When Cisco Unity detects a pause equal to the number of seconds specified, it assumes that the speaker has finished recording the message, greeting, or recorded name. Callers are more likely to pause longer during long messages, so you may want to set a smaller pause length for short recordings than for long recordings. Cisco Unity uses the Allowed Time for Short Recording in Seconds setting to determine whether a recording is short or long. Default: Two seconds.
Long Recording (Over Short Recording Trail Limit)	Select the number of seconds of silence that Cisco Unity uses to detect the end of a long recording. When Cisco Unity detects a pause equal to the number of seconds specified, it assumes that the speaker has finished recording the message, greeting, or recorded name. Callers are more likely to pause longer during long messages, so you may want to set a greater pause length for long recordings than for short recordings. Cisco Unity uses the Allowed Time for Short Recording in Seconds setting to determine whether a recording is short or long. Default: Three seconds.

Configuration Contacts Page

Table 13-3 System > Configuration > Contacts Page

Field	Considerations
Site Name	Name of organization using Cisco Unity. This information is useful to administrators and technicians who are accessing Cisco Unity remotely.
Cisco Unity Administrator	Name of person responsible for maintaining or administering the Cisco Unity server. This information is useful to administrators and technicians who are accessing Cisco Unity remotely.
Customer Contact	Name of person involved with purchase and installation of Cisco Unity on site. This information is useful to administrators and technicians who are accessing Cisco Unity remotely.
Customer Phone Number	Phone number for customer contact. This information is useful to administrators and technicians who are accessing Cisco Unity remotely.
Alternate Contact	Contact information that can be used by administrators and technicians who are accessing Cisco Unity remotely when the Cisco Unity Administrator and/or customer contact is not available.
Alternate Phone Number	Phone number for alternate contact. This information is useful to administrators and technicians who are accessing Cisco Unity remotely.

Configuration Phone Languages Page

Table 13-4 System > Configuration > Phone Languages Page

Field	Considerations
License Counts – Total	*Display only.* Shows the total number of phone language licenses for your installation, which determines how many phone languages can be loaded at one time. Note that the number of phone language licenses does not limit the number of phone languages actually installed on the Cisco Unity server.
License Counts – Loaded	*Display only.* Shows the number of languages in the Loaded list.
License Counts – Unused	*Display only.* Shows the number of unused phone language licenses. Note that this number might not be the same as the number of languages in the Available list.
Available	Displays the languages that have been installed on the Cisco Unity server but that are not currently loaded. When you load a language by moving it from the Available list to the Loaded list, the Loaded and Unused License Count fields are adjusted accordingly. You can move languages to the Loaded list only if the Unused License Count is greater than zero.
Loaded	Displays the languages that can be selected for use by the subscriber conversation and various Cisco Unity components such as call handlers. When you unload a language by moving it from the Loaded list to the Available list, the Loaded and Unused License Count fields are adjusted accordingly. Any call handlers or other Cisco Unity components that were using the unloaded language will now be reset to use the default phone language

Table 13-4 System > Configuration > Phone Languages Page (continued)

Field	Considerations
Default Phone Language	Select the default language in which system prompts are played to subscribers and callers. Only the languages shown in the Loaded list can be chosen as the default language.
Default Text to Speech Language	Select the default language that subscribers hear when having their e-mail read to them by phone. This is typically the same language that you selected in the Default Phone Language field with the following exceptions: • If you selected Australian or New Zealand English as your phone language, select either United States English or UK English as your default Text to Speech language. • There is no applicable Text to Speech language available for Czech or Korean.

Configuration GUI Languages Page

Table 13-5 System > Configuration > GUI Languages Page

Field	Considerations
License Counts – Total	*Display only.* Shows the total number of GUI language licenses for your installation, which determines how many GUI languages can be loaded at one time. Note that the number of GUI language licenses does not limit the number of GUI languages actually installed on the Cisco Unity server.
License Counts – Loaded	*Display only.* Shows the number of languages in the Loaded list.
License Counts – Unused	*Display only.* Shows the number of unused GUI language licenses. Note that this number might not be the same as the number of languages in the Available list.
Available	Displays the languages that have been installed on the Cisco Unity server but that are not currently loaded. When you move a language from the Available list to the Loaded list, the Loaded and Unused License Count fields are adjusted accordingly. You can move languages to the Loaded list only if the Unused License Count is greater than zero.
Loaded	Displays the languages that can be used in the browser display of the Cisco Unity Administrator. When you unload a language by moving it from the Loaded list to the Available list, the Loaded and Unused License Count fields are adjusted accordingly.
Default GUI Language	Select the default GUI language from the Loaded list. Cisco Unity uses the default GUI language only if the language selected in the browser is not among the loaded GUI languages.

Configuration Message Security Settings Page

Table 13-6 System > Configuration > Message Security Settings Page

Field	Considerations
Unidentified Caller Message Security	Select whether messages from unidentified callers are encrypted: • Do Not Encrypt Messages—Messages are not encrypted. • Encrypt All Messages—All messages are encrypted. Default: Do Not Encrypt Messages.
Message Aging	Check this check box to enable message aging for encrypted messages. After the specified period of time, the certificate used to encrypt the message will expire and Cisco Unity will no longer be able to decrypt the message. Message expiration applies to all encrypted messages regardless of whether the message recipient has listened to the message. Non-encrypted messages do not have a message expiration period. When message aging is enabled, a new security certificate is created each day and certificates older than the message expiration period are deleted. This prevents any messages that were encrypted by using those certificates from being decrypted, and thus rendering them inaccessible. Expired secure messages will still be in the recipient mailbox. If the recipient attempts to play a message, he or she is informed that the message has expired and cannot be played. Message aging of secure messages works in parallel with the Message Store Manager utility, by making secure messages older than the configured time period inaccessible, until such time as the Message Store Manager and Exchange delete them. When messages expire, they expire at midnight coordinated universal time (UTC). We recommend setting the time frame to 30 days or more, depending on your message retention policies. A short expiration period could result in undesired behavior. For example, if message aging is configured for a time frame of 1 day and an encrypted message is recorded at 11:50 p.m. UTC, the recipient of that message has only ten minutes to listen to it before Cisco Unity will no longer be able to decrypt the message. Default: Message aging is disabled. Valid entries for the timeframe that messages become unavailable: 1 to 180 days. Default: 30 days.

Schedules Page

Table 13-7 System > Schedules Page

Field	Considerations
Observe Holidays	Check this check box to have Cisco Unity play closed (off-hour) greetings and to observe closed transfer rules on the dates that are defined on the System > Holidays page.
Click Individual Blocks to Set Hours	Click the blocks in the grid to change from closed to open (standard) hours. Click a block again to undo your change. Note that you can set open (standard) and closed hours for one day, then use the Copy Day's Schedule box to copy the settings to other days.

Table 13-7 System > Schedules Page (continued)

Field	Considerations
Copy Day's Schedule	Select a day to copy from the list, then select which days to copy the schedule settings to. Use the Copy Day's Schedule field and >> functions to avoid clicking the same blocks for more than one day.

Holidays Page

Table 13-8 System > Holidays Page

Field	Considerations
Edit Holiday For	Enter the applicable year, month, and day for the holiday that you want to modify.

Authentication Page

Table 13-9 System > Authentication Page

Field	Considerations
Remember Logons for __ Days	Check this check box and enter the number of days that Cisco Unity will store logon information, if applicable. When you check this check box, Cisco Personal Communications Assistant (PCA) logons are stored as encrypted cookies on the subscriber workstation. In addition, the Log On page for the Cisco PCA offers subscribers the following options: • Remember User Name • Remember Domain When subscribers specify that Cisco Unity remember their user name or domain, subscribers will not have to enter them the next time that they log on to the Cisco PCA. Instead, the fields are automatically populated in the Log On page. Allowing subscribers to specify whether Cisco Unity remembers their credentials may reduce support desk requests for the information. Alternatively, for security reasons, you may not want the Log On page to offer subscribers the above options. If this is the case, uncheck this check box to prevent the options from appearing on the Log On page, and require that subscribers enter their user name and domain each time that they log on to the Cisco PCA. If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. Default: Check box not checked.

Table 13-9 System > Authentication Page (continued)

Field	Considerations
Remember Passwords for __ Days	Check this check box and enter the number of days that Cisco Unity will store password information, if applicable. When you check this check box, Cisco Personal Communications Assistant (PCA) passwords are stored as encrypted cookies on the subscriber workstation. In addition, the Log On page for the Cisco PCA offers subscribers the Remember Passwords option. When subscribers specify that Cisco Unity remember their password, they will not have to enter it the next time that they log on to the Cisco PCA. Instead, the password field is automatically populated in the Log On page. Allowing subscribers to specify whether Cisco Unity remembers their password may reduce support desk requests for resetting forgotten passwords. Alternatively, for security reasons, you may not want the Log On page to offer subscribers the option. If this is the case, uncheck this check box to prevent the Remember Password option from appearing on the Log On page, and require that subscribers enter their password each time that they log on to the Cisco PCA. If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. Default: Check box not checked.
Session Key Duration	Indicates the length of time that the browser can be left unattended before Cisco Unity automatically logs the subscriber off the Cisco Personal Communications Assistant (PCA). The value in IIS dictates the browser session duration, but you can use this field to change the value for the Session Timeout field in IIS. When you change the value for the Session Timeout field directly in IIS, however, the changes you make are not reflected here. Regardless of whether you update the session duration here or directly in IIS, the new timeout value applies the next new browser session. If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. Default: 20 minutes.
Disallow Blank Passwords	Check this check box so that subscribers are prohibited from logging on to the Cisco Personal Communications Assistant (PCA) without entering a password in the Log On page, even if the Active Directory domain account policy allows blank passwords. If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor.

Table 13-9 System > Authentication Page (continued)

Field	Considerations
Lock Out Accounts	Check this check box if you want to specify an account lockout policy for the subscribers who use the Cisco Personal Communications Assistant (PCA). When this check box is checked, enter the applicable values in the following fields: • Accounts Are Locked Out For __ Minutes • Accounts Will Lock Out After __ Logon Attempts • Reset Account Lockout Counters After __ Minutes If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. Default: Check box checked.
Accounts Are Locked Out for __ Minutes	Enter the number of minutes that Cisco Unity will prevent subscribers from accessing Cisco Unity by using the Cisco Personal Communications Assistant (PCA). If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. This option is unavailable when the Lock Out Accounts check box is not checked. Default: 30 minutes.
Accounts Will Lock Out After __ Logon Attempts	Enter the number of failed logon attempts after which subscribers cannot access Cisco Unity by using the Cisco Personal Communications Assistant (PCA). If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. This option is unavailable when the Lock Out Accounts check box is not checked. Default: Five attempts.
Reset Account Lockout Counters After __ Minutes	Enter the number of minutes after which Cisco Unity will clear the count of failed logon attempts to the Cisco Personal Communications Assistant (PCA), unless the failed logon limit is already reached and the account is locked. If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and to the Status Monitor. This option is unavailable when the Lock Out Accounts check box is not checked. Default: 30 minutes.

Ports Page

Table 13-10 System > Ports Page

Field	Considerations
Extension	Enter the extension for the port as assigned on the phone system.

Table 13-10 System > Ports Page (continued)

Field	Considerations
Enabled	Check this check box to enable the port. The port is enabled during normal operation. Uncheck this check box to disable the port. When the port is disabled, calls to the port get a ringing tone but are not answered. Typically, the port is disabled only by the installer during testing.
Answer Calls	Check this check box to designate the port for answering calls. These calls can be incoming calls from unidentified callers or from subscribers.
Message Notification	Check this check box to designate the port for notifying subscribers of messages. Assign Message Notification to the least busy ports, which typically are those with the highest port numbers for the phone system.
Dialout MWI *(not used by serial integrations)*	Check this check box to designate the port for turning MWIs on and off. Assign Dialout MWI to the least busy ports, which typically are those with the highest port numbers for the phone system.
AMIS Delivery *(available with the AMIS licensed feature only)*	Check this check box to designate the port for making outbound AMIS calls to deliver voice messages from Cisco Unity subscribers to users on another voice messaging system. Cisco Unity supports the Audio Messaging Interchange Specification (AMIS) protocol, which provides an analog mechanism for transferring voice messages between different voice messaging systems. This setting affects outbound AMIS calls only. All ports are used for incoming AMIS calls. Because the transmission of outgoing AMIS messages may tie up voice ports for long periods of time, you may want to adjust the schedule on the Network > AMIS > Schedule page so that outgoing AMIS calls are placed during closed hours or at times when Cisco Unity is not processing many calls.
TRAP Connection	Check this check box so that subscribers can use the phone as a recording and playback device in Cisco Unity web applications and e-mail clients. Assign TRAP Connection to the least busy ports, which typically are those with the highest port numbers for the phone system.

Table 13-10 System > Ports Page (continued)

Field	Considerations
Security Mode *(available only with Cisco Unity 4.0(5) and later when integrated with Cisco Unified CM 4.1 and later)*	Click the applicable security mode: • Non-secure—The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream cannot be encrypted, even when the Media Encryption check box is checked. • Authenticated—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. In addition, the media stream can be encrypted when the Media Encryption check box is checked. • Encrypted—The integrity and privacy of call-signaling messages will be ensured on this port because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted. In addition, the media stream can be encrypted when the Media Encryption check box is checked. **Note** Both end points must be registered in authenticated or encrypted mode. When one end point is set for authenticated mode and the other is set for encrypted mode, the media stream will be encrypted. However, if one end point is set for non-secure mode and the other is set for encrypted mode, the media stream will not be encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream will not be encrypted.

SMPP Provider Settings Page

Table 13-11 System > SMPP Provider Settings Page

Field	Considerations
Provider Name	Enter the name that will represent the service provider in Cisco Unity applications. The name you enter here will be listed on the Provider SMPP lists displayed on the SMS (SMPP) Message Notification pages for templates and individual subscribers in the Cisco Unity Administrator, as well as in the Cisco Unity Assistant. For multilingual systems, consider adding an SMPP provider for each language that subscribers use and then name and configure the providers accordingly. (Use the Data Coding field to specify language preference.)
SMPP Version	Indicate the version of the SMPP protocol that the SMPP server uses to communicate with ESMEs like Cisco Unity. This field corresponds to the interface_version in the SMPP Protocol Specification.
SMPP Server Host Name	Enter the IP address or host name of the SMPP server at the SMSC.
SMPP Server Port Number	Enter the port used by the SMPP server to connect to an ESME like Cisco Unity. **Note** When the Cisco Unity server is set up behind a firewall, you must configure the TCP port to allow incoming and outgoing communication between Cisco Unity and the SMPP server.

Table 13-11 System > SMPP Provider Settings Page (continued)

Field	Considerations
User Name	Enter the name or system ID associated with the account that your organization has with the SMSC as provided by your service provider. Cisco Unity uses the information in this field to identify itself when communicating with the SMPP server at the SMSC. This field corresponds to the system_id in the SMPP Protocol Specification.
Password	Enter the password associated with the account that your organization has with the SMSC as provided by your service provider. Cisco Unity uses the information in this field to identify itself when communicating with the SMPP server at the SMSC. This field corresponds to the password in the SMPP Protocol Specification.
Address Range *(optional)*	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 server. You may need to enter a set of addresses or a single address. This field corresponds to the address_range in the SMPP Protocol Specification.
System Type *(optional)*	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 may be categorized as a "VMS" (voice mail system). 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. This field corresponds to the system_type in the SMPP Protocol Specification.
ESME Type of Number (TON) *(optional)*	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 type of number (TON) that subscribers can use when specifying the To and From fields for SMS (SMPP) message notification in the Cisco Unity Administrator and the Cisco Unity Assistant. Select the applicable value from the list to specify: • 0—Unknown • 1—International • 2—National • 3—Network Specific • 4—Subscriber Number • 5—Alphanumeric • 6—Abbreviated This field corresponds to the addr_ton in the SMPP Protocol Specification. The addr_ton and addr_npi values tell the SMSC how to interpret the address found in the address_range field.

Table 13-11 System > SMPP Provider Settings Page (continued)

Field	Considerations
ESME Numbering Plan Identity (NPI) *(optional)*	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 subscribers can use when specifying the To and From fields for SMS (SMPP) message notification in the Cisco Unity Administrator and the Cisco Unity Assistant. Select the applicable value from the list to specify: • 0—Unknown • 1—ISDN (E163/E164) • 3—Data (X.121) • 4—Telex (F.69) • 6—Land Mobile (E.212) • 8—National • 9—Private • 10—ERMES • 14—Internet (IP) • 18—WAP Client ID This field corresponds to the addr_npi in the SMPP Protocol Specification. The addr_ton and addr_npi values tell the SMSC how to interpret the address found in the address_range field.
Source TON *(optional)*	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 type of number (TON) that subscribers can use when specifying the To and From fields for SMS (SMPP) message notification in the Cisco Unity Administrator and the Cisco Unity Assistant. Select the applicable value from the list to specify: • 0—Unknown • 1—International • 2—National • 3—Network Specific • 4—Subscriber Number • 5—Alphanumeric • 6—Abbreviated This field corresponds to the source_addr_ton in the SMPP Protocol Specification. The source_addr_ton and source_addr_npi values tell the SMSC how to interpret the address found in the source_addr (From) field.

Table 13-11 System > SMPP Provider Settings Page (continued)

Field	Considerations
Source NPI *(optional)*	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 subscribers can use when specifying the To and From fields for SMS (SMPP) message notification in the Cisco Unity Administrator and the Cisco Unity Assistant. Select the applicable value from the list to specify: • 0—Unknown • 1—ISDN (E163/E164) • 3—Data (X.121) • 4—Telex (F.69) • 6—Land Mobile (E.212) • 8—National • 9—Private • 10—ERMES • 14—Internet (IP) • 18—WAP Client ID This field corresponds to the source_addr_npi in the SMPP Protocol Specification. The source_addr_ton and source_addr_npi values tell the SMSC how to interpret the address found in the source_addr (From) field.
Destination TON *(optional)*	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 type of number (TON) that subscribers can use when specifying the To and From fields for SMS (SMPP) message notification in the Cisco Unity Administrator and the Cisco Unity Assistant. Select the applicable value from the list to specify: • 0—Unknown • 1—International • 2—National • 3—Network Specific • 4—Subscriber Number • 5—Alphanumeric • 6—Abbreviated This field corresponds to the dest_addr_ton in the SMPP Protocol Specification. The dest_addr_ton and dest_addr_npi values tell the SMSC how to interpret the address found in the destination_addr (To) field.

Table 13-11 System > SMPP Provider Settings Page (continued)

Field	Considerations
Destination NPI *(optional)*	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 subscribers can use when specifying the To and From fields for SMS (SMPP) message notification in the Cisco Unity Administrator and the Cisco Unity Assistant. Select the applicable value from the list to specify: • 0—Unknown • 1—ISDN (E163/E164) • 3—Data (X.121) • 4—Telex (F.69) • 6—Land Mobile (E.212) • 8—National • 9—Private • 10—ERMES • 14—Internet (IP) • 18—WAP Client ID This field corresponds to the dest_addr_npi in the SMPP Protocol Specification. dest_addr_ton and dest_addr_npi values tell the SMSC how to interpret the address found in the destination_addr (To) field.
Service Type *(optional)*	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 allows an ESME like Cisco Unity to do the following: • Use enhanced messaging services such as the replace previous notification option. • Control the teleservice used on the air interface. The following generic service types are defined: • (blank) • CMT Cellular Messaging • CPT Cellular Paging • VMN Voice Mail Notification • VMA Voice Mail Alerting • WAP Wireless Application Protocol • USSD Unstructured Supplementary Services Data Other applicable values are service provider-specific.

Table 13-11 System > SMPP Provider Settings Page (continued)

Field	Considerations
Data Coding *(optional)*	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, leave the field blank.) For multilingual systems, consider creating a separate SMPP provider for each character set that you want to offer to subscribers. Select the applicable value from the list to specify: • 0—GSM 3.38 Default Alphabet: 7 bit • 1—ASCII: 7 bit (Windows code page 20127 or 20105) • 3—Latin 1: 8 bit (Windows code page 28591 or 1252) • 5—Japanese: 16 bit* (Windows code page 20932 or 932) • 6—Cyrillic: 8 bit (Windows code page 28595 or 1251) • 7—Latin/Hebrew: 8 bit (Windows code page 28598 or 1255) • 8—USC-2: 16 bit (Unicode) • 14—Korean: 16 bit* (Windows code page 1361 or 949) * Multi-bit character set: most characters are 16 bit; some are 8 bit.
Replace Previous Notification if Possible *(optional)*	Check this check box to have Cisco Unity request that the SMSC or SMS device will replace one or more previously submitted message notifications with the latest one. Depending on whether the subscriber device is turned on or off, message notifications are replaced as follows: • When the device is on, Cisco Unity 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, Cisco Unity 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. In both scenarios, the subscriber receives only the latest message notification. **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. This field corresponds to the replace_if_present_flag and the protocol_id fields in the SMPP Protocol Specification.

Voice Recognition Settings Page

Table 13-12 System > Voice Recognition > Voice Recognition Settings Page

Field	Considerations
IP Address	Enter the IP Address of the server on which the voice recognition software is installed. Default: Blank.
Socket Port	Enter the TCP/IP port that the voice recognition server is listening on. By default the voice recognition server is configured to listen on port 554. Default: 554.
Limit Searches to The	Select the default search scope to be used for looking up names when subscribers address messages by using voice recognition. This setting is only used when the subscriber who is addressing the message does not have the addressing search scope limited to a directory handler on the Subscriber > Profile page. Cisco Unity deployments can scale to very large systems with thousands of users across networked servers. The voice recognition server can handle thousands of names; however, name recognition accuracy degrades as the number of names increases. Depending on the size of your global directory, you may want to limit searches. Choose from the following: • Local Server—All local subscribers and public distribution lists on the Cisco Unity server that is handling the call. This scope is expected to have better accuracy than dialing domain or global directory. • Dialing Domain—All local and remote subscribers and public distribution lists that are in the local dialing domain. This scope is expected to be smaller than the global directory, but could still be fairly large. It should have better accuracy than the global directory. • Global Directory— All local subscribers and public distribution lists, all named remote subscribers and remote public distribution lists. This will be the largest search scope and may have the worst accuracy of all of the search scopes. Note that the number of names is not always equal to the number of subscribers and distribution lists in a scope. The number of names also includes alternate spellings of each name. For example, a 100 user company that has 1 alternate name for each subscriber would generate a global directory scope with 200 names. For this reason, it would be advisable to include only the most common alternate names when considering alternate names. Default: Local Server.

Table 13-12 System > Voice Recognition > Voice Recognition Settings Page (continued)

Field	Considerations
Automatic Rebuild Time	Enter the time of day that Cisco Unity will perform an automatic rebuild of name grammars. Depending on the size of the directory, name grammars may take a long time to build and may affect system performance. We recommended scheduling the automatic rebuild to occur at off-peak times. By default, the automatic rebuild starts at 1:00 a.m. Note that in a failover configuration, this field is read-only on the secondary server.
Start Manual Update	Press Start Manual Update to immediately update the name grammar files. Depending on the size of the directory, name grammars may take a long time to build and may affect system performance. We recommended initiating a manual update only when troubleshooting or during initial configuration. Note that in a failover configuration, this field is read-only on the secondary server.

Integration <Cisco Unified Communications Manager> Page

Table 13-13 System > Integration > <Cisco Unified Communications Manager> Page

Field	Considerations
Integration Type	*Display only.* Displays the name of the Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) integration entered in UTIM.
Switch File	*Display only.* Displays the Cisco Unity phone configuration file (also called switch.ini file) that is being used to initialize the integration.
Primary Server	*Display only.* Displays the IP address of the primary Cisco Unified CM server. This address was entered in UTIM.
Secondary Server	*Display only.* Displays the IP address of the secondary Cisco Unified CM server, if applicable. This address was entered in UTIM.
Device Name Prefix	*Display only.* Displays the prefix that Cisco Unified CM adds to the device name for the voice messaging ports. This prefix was entered in UTIM and must match the prefix that is used by Cisco Unified CM.
MWI On Extension	*Display only.* Displays the extension that Cisco Unified CM uses to turn MWIs on. This extension was entered in UTIM.
MWI Off Extension	*Display only.* Displays the extension that Cisco Unified CM uses to turn MWIs off. This extension was entered in UTIM.
Reconnect After CallManager Failback	*Display only.* Displays whether Cisco Unity will automatically reconnect to the primary Cisco Unified CM server after Cisco Unified CM failover has been corrected. The setting Yes indicates that automatic reconnection is enabled. This value was set in UTIM.

Integration <SIP Server> Page

Table 13-14 System > Integration > <SIP Server> Page

Field	Considerations
Integration Type	*Display only.* Displays the name of SIP integration entered in UTIM.
Switch File	*Display only.* Displays the Cisco Unity phone configuration file (also called switch.ini file) that is being used to initialize the integration.
Primary Server	*Display only.* Displays the IP address of the primary SIP proxy server. This address was entered in UTIM.
Secondary Server	*Display only.* Displays the IP address of the secondary SIP proxy server, if applicable. This address was entered in UTIM.
Cisco Unity SIP Port	*Display only.* Displays the IP port on Cisco Unity that callers and the SIP proxy server use to connect to voice mail. This port was entered in UTIM.
SIP Contact Line Name	*Display only.* Displays the voice messaging line name that subscribers use to contact Cisco Unity and that Cisco Unity uses to register with the SIP proxy server. This line name was entered in UTIM.
Preferred Codec	*Display only.* Displays the codec that Cisco Unity first attempts to use on outgoing calls. This codec was selected in UTIM.
Preferred Transport Protocol	*Display only.* Displays the preferred transport protocol that Cisco Unity uses. This value was set in UTIM.
Authenticate with SIP Proxy Server	*Display only.* Displays whether Cisco Unity authenticates with the SIP proxy server. The setting Yes indicates that authentication is enabled. This value was set in UTIM.
Authentication Name	*Display only.* Displays the name that the SIP proxy server uses for authentication. This name was entered in UTIM.

Integration <Phone System Via PIMG/TIMG> Page

Table 13-15 System > Integration > <Phone System Via PIMG/TIMG> Page

Field	Considerations
Integration Type	*Display only.* Displays the name of PIMG (PBX IP Media Gateway) integration entered in UTIM.
Switch File	*Display only.* Displays the Cisco Unity phone configuration file (also called switch.ini file) that is being used to initialize the integration.
PIMG SIP Port	*Display only.* Displays the IP port of the PIMG unit that Cisco Unity uses for SIP communication. This port was entered in UTIM.
Cisco Unity SIP Port	*Display only.* Displays the IP port on Cisco Unity that callers and the PIMG unit use to connect to voice mail. This port was entered in UTIM.
SIP Contact Line Name	*Display only.* Displays the voice messaging line name that subscribers use to contact Cisco Unity and that Cisco Unity uses to register with the SIP proxy server. This line name was entered in UTIM.
Preferred Codec	*Display only.* Displays the codec that Cisco Unity first attempts to use on outgoing calls. This codec was selected in UTIM.

Table 13-15 System > Integration > <Phone System Via PIMG/TIMG> Page (continued)

Field	Considerations
Preferred Transport Protocol	*Display only.* Displays the preferred transport protocol that Cisco Unity uses. This value was set in UTIM.
Authenticate with SIP Proxy Server	*Display only.* Displays whether Cisco Unity authenticates with the PIMG unit. The setting Yes indicates that authentication is enabled. This value was set in UTIM.
Authentication Name	*Display only.* Displays the name that the PIMG unit uses for authentication. This name was entered in UTIM.

Integration <Phone System Via Voice Cards> Page

Table 13-16 System > Integration > <Phone System Via Voice Cards> Page

Field	Considerations
Integration Type	*Display only.* Displays the name of integration entered in UTIM.
Switch File	*Display only.* Displays the Cisco Unity phone configuration file (also called switch.ini file) that is being used to initialize the integration.
PBX Manufacturer	*Display only.* Displays the phone system manufacturer selected in UTIM.
PBX Model	*Display only.* Displays the phone system model selected in UTIM.
PBX Software Version	*Display only.* Displays the phone system software version selected in UTIM.