



## System Settings

---

### Overview: System Settings

Before Cisco Unity can be set up to handle calls and messages, some basic system settings must be entered.

See the following sections in this chapter for more information:

- [Configuration Settings, page 28-2](#)—This section provides information about the configuration settings.
- [Software Versions, page 28-4](#)—This section details where to find version numbers for Cisco Unity and other software components.
- [Recording Settings, page 28-4](#)—This section provides information about recording settings.
- [Contacts, page 28-6](#)—This section details where you can enter the names and phone numbers of the people responsible for maintaining or administering the Cisco Unity server.
- [Phone Languages Settings, page 28-6](#)—This section provides information about the language played for subscribers and unidentified callers.
- [GUI Languages Settings, page 28-7](#)—This section provides information about the language in which the Cisco Unity Administrator and Cisco Personal Communications Assistant are displayed.
- [Schedule Settings, page 28-8](#)—This section explains how to set up system schedules.
- [Holiday Settings, page 28-10](#)—This section explains how to set up holidays to work with Cisco Unity schedules.
- [Authentication Settings, page 28-11](#)—This section provides information about logon, password, and account lockout policy settings for subscribers accessing Cisco Unity web clients.
- [Voice Messaging Port Settings, page 28-13](#)—This section provides information about setting up voice ports.
- [Cisco CallManager Integration, page 28-15](#)—This section provides information on the Cisco CallManager integration settings that are displayed.
- [SIP Integration, page 28-16](#)—This section provides information on the SIP integration settings that are displayed.
- [Circuit-Switched Integration, page 28-17](#)—This section provides information on the circuit-switched integration settings that are displayed.
- [Enabling a Warning Tone for End of Recording, page 28-19](#)—This section how to enable a warning tone to play before the maximum allowable message length of a recording is reached.

# Configuration Settings

Configuration settings contain general Cisco Unity settings such as the default schedule, system security, and the cleanup interval for log files, as well as information about the Cisco Unity server.



## Caution

If you have a Cisco Unity failover system, configuration settings (except schedules and holidays) are not replicated between the primary and secondary servers. You must change values manually on both servers.

Use [Table 28-1](#) to learn more about configuration settings. See the following for additional information on these related topics:

- Offering subscribers the Cisco Unity Inbox—See the “[Setting Up the Cisco Personal Communications Assistant](#)” section on page 7-6.
- Setting up enhanced phone security—See the “[Overview: Enhanced Phone Security](#)” section on page 10-1.
- Identifying the default system schedule—See the “[Schedule Settings](#)” section on page 28-8.
- Log-based Cisco Unity reports—See the “[About Report Data](#)” section on page 26-2.

**Table 28-1 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.<br><br>Default: Weekdays.   |
| Use 24-Hour Time Format for Conversation and Schedules conversation | 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 over the phone.<br><br>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 over the phone. In addition, when this check box is checked, subscribers who are editing private lists can search for subscribers by spelling the subscriber name over the phone. Addressing by name requires lettered keypads on subscriber phones.<br><br>Note that checking this check box does not prevent subscribers from searching for subscribers by entering subscriber extensions over the 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 the # key twice.<br><br>When this check box is unchecked, subscribers can search for subscribers over the phone only by entering subscriber extensions. In addition, the option to address by spelled name cannot be used on the Subscribers > Conversation page and in the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)<br><br>Default: check box is checked. |

Table 28-1 System &gt; Configuration &gt; Settings Page (continued)

| Field   | Considerations  |
|---|---|
| RSA Two Factor  | <p>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.</p> <p>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.</p> <p>Default: check box not checked.</p>  |
| Subscribers Are Identified as Message Senders Only if They Log On | <p>Check this check box to disable identified subscriber messaging system-wide.</p> <p>When identified subscriber messaging is enabled, Cisco Unity automatically identifies a message left during an internal call as originating from the extension from which the call was made.</p> <p>When identified subscriber messaging is disabled, Cisco Unity does not identify the originating extension of a message left during an internal call, unless the calling subscriber logs on to Cisco Unity before leaving the message.</p> <p>Regardless of enabled or disabled status, if a subscriber logs on before leaving a message from an internal location other than the extension assigned to the subscriber (such as from a conference room), Cisco Unity identifies the call as originating from the extension of the logged-on subscriber, rather than the extension from which the call is placed.</p> <p>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.</p> <p>Default: check box not checked.</p> |
| Cisco Personal Communications Assistant (PCA)                     | <p>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 the subscriber. (Subscribers use the Cisco PCA to access their Cisco Unity Inboxes.)</p> <p>You can set up Cisco Unity Inbox notification on the Message Notification page for an individual subscriber or a subscriber template.</p>   |
| Cleanup Interval for Logger Data Files in Days                    | <p>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.</p> <p>Default: 7 days.</p>  |
| Cleanup Interval for Logger Diagnostic Files in Days              | <p>Indicate how often diagnostic files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files.</p> <p>Default: 7 days.</p>   |
| Cleanup Interval for Report Files in Days                         | <p>Indicate how often report files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files.</p> <p>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.</p> <p>Default: 7 days.</p>  |

Table 28-1 System &gt; Configuration &gt; Settings Page (continued)

| Field                                   | Considerations  |
|---|---|
| Replicate Cisco Unity Directory Objects | Choose Changed Objects to manually synchronize changes from the Active Directory or Exchange 5.5 Directory into the Cisco Unity SQL database. For example, changing the distribution list by which the directory handler is scoped requires a synchronization. This 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 database, which usually occurs within 15 to 20 minutes after the directory handler scope change is made in the Cisco Unity Administrator, or can be done immediately by choosing Changed Objects.<br><br>Choose All Objects only if Cisco Unity has been down for a considerable length of time. |
| Cisco Unity Computer Settings           | <i>Display only.</i> This setting shows the name of the Cisco Unity server and the Windows Domain name.   |
| Fax Settings                            | This setting shows the name of the fax domain.  |
| Disk Usage                              | <i>Display only.</i> This setting shows, in megabytes, the total, used, and free disk space on the Cisco Unity server.  |

## Software Versions

The System > Configuration > Software Versions page displays the Cisco Unity serial and build numbers, and the version numbers for several Cisco Unity components and for the Microsoft Windows 2000 Server. If you ever contact the Cisco Technical Assistance Center (TAC), you may need to refer to this information.

## Recording Settings

The Recordings page contains settings for recording time limits and for silence thresholds (the amount of silence before Cisco Unity assumes the caller is no longer on the line) before, during, and after recordings.

## Audio Codecs

Cisco Unity supports the following audio codecs:

| Audio Codec             | Approximate File Size, 1-Minute Message | Quality Rating |
|-------------------------|---|----------------|
| G.711 Mu-Law and A-Law  | 480 KB                                  | Excellent      |
| G726 32 Kbps            | 240 KB                                  | Fine           |
| Dialogic OKI ADPCM 8Khz | 240 KB                                  | Fine           |
| Dialogic OKI ADPCM 6Khz | 180 KB                                  | Fine           |
| GSM 6.10                | 98 KB                                   | Fine           |
| G.729a                  | 60 KB                                   | Good           |

**Note**

GSM 6.10 is supported for playback on a Pocket PC, and is a higher quality recording format than MP3.

For information on choosing and implementing audio codecs, refer to the *White Paper: Audio Codecs and Cisco Unity*, which is available on Cisco.com at

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_reference_list.html).

**Caution**

If you have a Cisco Unity failover system, recordings settings are not replicated between the primary and secondary servers. You must change values manually on both servers.

Use the following table to learn more about recording settings.

**Table 28-2 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.<br>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.<br>Default: 10 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 2 or 3 seconds may not give the subscriber or caller enough time to begin speaking.<br>Default: 5 seconds.   |
| Discard Any Recording Less Than in Seconds            | Select the minimum length of recordings, in seconds, for messages or greetings. Note that this setting is not applied to recorded names.<br>Default: 1 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, Cisco Unity 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.<br>Default: 2 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, Cisco Unity 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.<br>Default: 3 seconds.  |

# Contacts

The System > Configuration > Contacts page is where you enter the names and phone numbers of the people responsible for maintaining or administering the Cisco Unity server. This information might be useful to a technician who is accessing Cisco Unity from off-site.

## Phone Languages Settings

Phone languages are the languages in which Cisco Unity can play system prompts to subscribers and callers. You specify a default phone language and other system-wide phone language settings, as well as the default text-to-speech (TTS) language, which is the language that subscribers hear when their e-mail is read to them over the phone. Note that to use TTS languages, your organization must have text-to-speech e-mail and the appropriate languages installed. See the [“Installing Languages” section on page 11-1](#) for more information about installing multiple languages.

If desired, you can customize the language settings for specific Cisco Unity components such as subscriber accounts, routing rules, call handlers, interview handlers, and the directory handler. See the [“Specifying Phone Languages” section on page 11-2](#) for information about customizing language settings for individual Cisco Unity components.



### Caution

If you have a Cisco Unity failover system, phone languages settings are not replicated between the primary and secondary servers. You must change values manually on both servers.

Use the following table to learn more about phone languages settings.

**Table 28-3 System > Configuration > Phone Languages Page**

| Field                   | Considerations  |
|-------------------------|---|
| License Counts – Total  | <i>Display only.</i> This setting 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 | <i>Display only.</i> This setting shows the number of languages in the Loaded list.   |
| License Counts – Unused | <i>Display only.</i> This setting 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               | This list displays the languages that have been installed on the Cisco Unity server but that are not currently loaded.<br><br>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                  | This list displays the languages that can be selected for use by the subscriber conversation and various Cisco Unity components such as call handlers.<br><br>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 28-3** 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 over the phone. This is typically the same language that you selected in the Default Phone Language field with the following exceptions: <ul style="list-style-type: none"> <li>• 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.</li> <li>• There is no appropriate text to speech language available for Brazilian Portuguese or Korean.</li> </ul> |

## GUI Languages Settings

The settings on the GUI Languages page determine the languages in which the Cisco Unity Administrator pages can be displayed. You specify a default GUI language and other system-wide GUI language settings.

To change the GUI language used in the Cisco Unity Administrator or the Cisco Personal Communications Assistant, select a language in the browser. (Subscribers use the Cisco PCA website to access the Cisco Unity Assistant and the Cisco Unity Inbox. Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA; the Cisco Unity Inbox was known as the Visual Messaging Interface, or VMI.)

For the Cisco Unity Administrator, note that the language selected in the browser must be one of the languages in the Loaded list on the GUI Languages page. If the language that you select in the browser is not among the loaded languages, Cisco Unity uses the default GUI language. For the Cisco PCA, the language selected in the browser must be one of the languages that the Cisco PCA offers.



### Caution

If you have a Cisco Unity failover system, GUI languages settings are not replicated between the primary and secondary servers. You must change values manually on both servers.

Use the following table to learn more about GUI languages settings.

**Table 28-4** System > Configuration > GUI Languages Page

| Field                   | Considerations   |
|-------------------------|--|
| License Counts – Total  | <i>Display only.</i> This setting 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 | <i>Display only.</i> This setting shows the number of languages in the Loaded list.  |
| License Counts – Unused | <i>Display only.</i> This setting 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.  |

Table 28-4 System &gt; Configuration &gt; GUI Languages Page (continued)

| Field                | Considerations  |
|----------------------|---|
| Available            | This displays the languages that have been installed on the Cisco Unity server but that are not currently loaded.<br><br>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               | This displays the languages that can be used in the browser display of the Cisco Unity Administrator.<br><br>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.   |

## Schedule Settings

Schedules are one of the variables that Cisco Unity uses to manage calls. The standard and closed subscriber and call handler greetings play according to the days and times that you specify in a schedule.

Cisco Unity offers two predefined schedules: All Hours – All Days, and Weekdays, both of which can be modified. In addition, you can create up to 64 schedules for your organization to accommodate the standard working hours of different groups of employees. You can use either of the predefined schedules, or a new schedule that you create, as the default schedule for Cisco Unity. The default schedule is used for all call handlers, subscriber templates, and call routing tables, unless you specify a different schedule for each call handler, subscriber account, or call routing table to follow.

For each schedule that you create or modify, you identify the hours and days that make up the standard and closed hours, and whether the schedule changes for holidays:

|                       |   |
|-----------------------|---|
| <b>Standard hours</b> | The hours and days that make up the normal business hours, when the organization is open. Standard hours can include multiple time ranges and different time ranges on different days. (For example, standard hours for an organization might be Monday through Friday from 8 A.M. to 12 P.M. and 1 P.M. to 5 P.M., to accommodate a lunch break, and Saturday from 9 A.M. to 1 P.M.) |
| <b>Closed hours</b>   | The hours and days not identified as standard hours are considered nonbusiness hours, when the organization is closed.  |
| <b>Holidays</b>       | The time range defined on the System > Holidays page when the organization is closed. See the <a href="#">“Holiday Settings”</a> section on page 28-10 for information about identifying holidays.  |

### To Create a New Schedule

- Step 1** In the Cisco Unity Administrator, go to the **System > Schedules** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Schedule dialog box, enter information as appropriate in the Name field.

- Step 4** Select **New Schedule** or **Based on Existing Schedule**. If you select Based on Existing Schedule, select the appropriate schedule in the Based On field.
- Step 5** Click the **Add** button.
- Step 6** Check the **Observe Holidays** check box, if appropriate.
- Step 7** Click boxes on the schedule grid until all open (standard) half hours are white and all closed half hours are gray. Note that you can use the Copy Day's Schedule field and >> functions to avoid clicking the same blocks for more than one day.
- Step 8** Click the **Save** icon.
- Step 9** To use this new schedule as the Cisco Unity default schedule, see the following [“To Specify the Default Schedule”](#) procedure.

---

#### To Specify the Default Schedule

- Step 1** In the Cisco Unity Administrator, go to the **System > Schedules** page, and click **Change Default Schedule** from any schedule page. Note that when you click the link, you leave the schedule page, and move to the System > Configuration > Settings page.
- Step 2** In the Default Schedule field, click the schedule you want to use as the default for new call handlers, subscriber templates, and call routing tables.
- Step 3** Check the **Use 24-Hour Time Format for Conversation and Schedules** check box to use a 24-hour time format for all schedules, if desired.
- Step 4** Click the **Save** icon.

---

#### To Modify an Existing Schedule

- Step 1** In the Cisco Unity Administrator, go to the **System > Schedules** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the schedule that you want to modify.
- Step 4** Change settings as appropriate, and then click the **Save** icon.
- Step 5** To use this new schedule as the system default schedule, see the preceding procedure.

Use the following table to learn more about schedule settings.

**Table 28-5** 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 defined on the System > Holidays page. |

Table 28-5 System &gt; Schedules Page (continued)

| Field                                | Considerations   |
|--------------------------------------|--|
| 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. |
| 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.   |

## Holiday Settings

When a Holiday setting is in effect, Cisco Unity plays closed greetings and observes closed transfer rules. You can set up several years of holidays at a time, and you can copy the holidays from one year to the next, adjusting dates as necessary. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.

### To Identify Days as Holidays

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Holidays** page.
  - Step 2** Click the **Add** icon.
  - Step 3** In the Add a Holiday dialog box, select the month, day, and year of the holiday.
  - Step 4** Click the **Add** button.
- 

### To Modify a Holiday

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Holidays** page.
  - Step 2** Click the date of the holiday listed for the appropriate year.
  - Step 3** In the Edit Holiday For field, change settings as appropriate, and then click the **Save** icon.
- 

Use the following table to learn more about holiday settings.

Table 28-6 System &gt; Holidays Page

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

# Authentication Settings

Authentication settings dictate the logon and lockout policy which applies when subscribers access Cisco Unity by using the Cisco Personal Communications Assistant (PCA). If the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, the policy that you specify on the System > Configuration > Authentication Provider page also applies when subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity.

It is important to consider that when subscribers log on to the Cisco PCA, their credentials are sent across the network to Cisco Unity in clear text. The same is true if the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method. For increased security, it is therefore recommended that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol (see the [“Setting Up Cisco Unity to Use SSL”](#) section on page 4-1 for details). As best practice, it is also recommended that Cisco Unity administrators not use the same subscriber account to log on to the Cisco Unity Administrator and the Status Monitor, as they do to log on to the Cisco PCA.

Changes to authentication settings affect all Cisco Unity subscribers. You cannot change authentication settings for individual subscriber accounts, though you can lockout individual subscriber accounts to prevent subscribers from using the Cisco PCA, Cisco Unity Administrator, or Status Monitor to access Cisco Unity. (For details, see the [“Subscriber Account Settings”](#) section on page 17-5.)

Authentication settings represent a different logon and lockout policy from the one that applies when subscribers access Cisco Unity by phone. For information on setting up the account policy that applies when subscribers access to Cisco Unity by phone, see the [“Account Policy Settings”](#) chapter.

Use the following table to learn more about authentication settings.

**Table 28-7 System > Configuration > Authentication Provider Page**

| Field                           | Considerations  |
|---------------------------------|---|
| Remember Logons for ___ Days    | <p>If desired, check this check box and enter the number of days that Cisco Unity will store logon information. When you check this check box, logons are stored as encrypted as cookies on the subscriber computer.</p> <p>When Cisco Unity remembers logon information, subscribers do not have to enter it to log on to the Cisco Personal Communications Assistant (PCA). Instead, the logon credentials for a subscriber are automatically populated in the Log On page.</p> <p>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 the Status Monitor.</p> <p>Default: blank.</p> |
| Remember Passwords for ___ Days | <p>If desired, check this check box and enter the number of days that Cisco Unity will store password information. When you check this check box, passwords are stored as encrypted as cookies on the subscriber computer.</p> <p>When Cisco Unity remembers subscriber passwords, subscribers do not have to enter it to log on to the Cisco Personal Communications Assistant (PCA). Instead, a subscriber password is automatically populated in the Log On page.</p> <p>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 the Status Monitor.</p> <p>Default: blank.</p>          |

Table 28-7 System &gt; Configuration &gt; Authentication Provider Page (continued)

| Field                                  | Considerations   |
|--|--|
| Session Key Duration                   | <p>This field indicates the length of time that the browser can be left unattended before Cisco Unity automatically logs the subscriber off.</p> <p>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.</p> <p>Regardless of whether you update the session duration here or directly in IIS, the new timeout value applies the next new browser session.</p> <p>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 the Status Monitor.</p> <p>Default: 20 minutes.</p> |
| Disallow Blank Passwords               | <p>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 Windows account policy allows blank passwords.</p> <p>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 the Status Monitor.</p>  |
| Lock Out Accounts                      | <p>Check this check box if you want to specify an account lockout policy for the subscribers using the Cisco Personal Communications Assistant (PCA).</p> <p>When this check box is checked, enter the appropriate values in the following fields:</p> <ul style="list-style-type: none"> <li>• Accounts Are Locked Out For __ Minutes</li> <li>• Accounts Will Lock Out After __ Logon Attempts</li> <li>• Reset Account Lockout Counters After __ Minutes</li> </ul> <p>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 the Status Monitor.</p> <p>Default: check box checked.</p>   |
| Accounts Are Locked Out For __ Minutes | <p>Enter the number of minutes that Cisco Unity will prevent subscribers from accessing Cisco Unity by using the Cisco Personal Communications Assistant (PCA).</p> <p>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 the Status Monitor.</p> <p>This option is unavailable when the Lock Out Accounts check box is unchecked.</p> <p>Default: 30 minutes.</p>  |

**Table 28-7 System > Configuration > Authentication Provider Page (continued)**

| Field   | Considerations   |
|---|--|
| Accounts Will Lock Out After __ Logon Attempts  | <p>Enter the number of failed logon attempts after which subscribers cannot access Cisco Unity by using the Cisco Personal Communications Assistant (PCA).</p> <p>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 the Status Monitor.</p> <p>This option is unavailable when the Lock Out Accounts check box is unchecked.</p> <p>Default: 5 attempts.</p>   |
| Reset Account Lockout Counters After __ Minutes | <p>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.</p> <p>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 the Status Monitor.</p> <p>This option is unavailable when the Lock Out Accounts check box is unchecked.</p> <p>Default: 30 minutes.</p> |

## Voice Messaging Port Settings

Each voice messaging port on the Cisco Unity server can be set to perform one or more of these functions:

- Answer incoming calls from unidentified callers and from subscribers dialing in to Cisco Unity.
- Dial out to notify subscribers of voice, fax, and e-mail messages.
- Dial out to allow system administrators and subscribers to use the phone as a recording and playback device in Cisco Unity applications. (The phone is offered as a recording and playback device in the Media Master, which appears on pages of the Cisco Unity Administrator, Cisco Unity Assistant, and Cisco Unity Inbox, and in ViewMail.)

(Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA; the Cisco Unity Inbox was known as the Visual Messaging Interface, or VMI.)

- Dial out to turn message waiting indicators (MWIs) on and off.
- Dial out to deliver outbound AMIS messages (some systems may not have this feature).

The number of voice messaging ports set for each of these functions depends on many factors, such as:

- The total number of voice messaging ports available.
- The number of subscribers who will use message notification and how often they will receive notifications.
- For circuit-switched phone systems, whether your integration is serial or analog (analog integrations use a voice messaging port to turn MWIs on and off, while serial integrations do not).
- Whether your organization communicates primarily through e-mail or voice mail.

Each voice messaging port can be set to perform more than one function (for example, to answer calls and to dial out to turn MWIs on). When the voice messaging ports perform more than one function and are very active (for example, answering many calls), the other functions may be delayed until the voice

messaging port is free (for example, MWIs cannot be turned on until there are fewer calls to answer). For guidelines on setting up the voice messaging ports, see [Table 28-8](#). For best performance, use the first voice messaging ports for incoming calls and the last ports to dial out. This helps minimize the possibility of a collision, in which an incoming call arrives on a port at the same time that Cisco Unity takes the port off-hook to dial out.

In a typical installation, the installer sets up voice messaging ports for Cisco Unity, but you can modify them on the Ports page. Before changing port settings, however, monitor the voice messaging port activity. See the [“Port Usage Report” section on page 26-9](#) for more information about monitoring voice messaging port activity.

**Note**

If you have a Cisco Unity failover system, voice messaging port settings are not replicated between the primary and secondary servers. You must change voice messaging port settings on both servers.

Use the following table to learn more about port settings.

**Table 28-8 System > Ports Page**

| Field   | Considerations  |
|---|---|
| Extension   | Enter the extension for the port as assigned on the phone system.   |
| Enabled   | Check this check box to enable the port. This setting is used during normal operation.<br>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. This setting is typically used only by the installer for 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. As a general guideline, set Answer Calls on approximately 75 percent of the ports.   |
| 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. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports. |
| Dialout MWI<br><i>(not used by serial or SMDI integrations)</i> | 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. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.                    |

Table 28-8 System &gt; Ports Page (continued)

| Field  | Considerations  |
|--|---|
| AMIS Delivery<br>(available with the AMIS licensed feature only) | <p>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.</p> <p>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 &gt; AMIS &gt; Schedule page so that outgoing AMIS calls are placed during closed hours or at times when Cisco Unity is not processing many calls.</p> |
| TRAP Connection  | <p>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. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.</p>   |

## Cisco CallManager Integration

The integration settings are specified during installation in the Cisco Unity Telephony Integration Manager (UTIM), which configures Cisco Unity to work with the specified phone system. Once the integration is set up, you should not need to change the integration settings, but you can review them on the Integration page or revise them in UTIM.



### Note

If you have a Cisco Unity failover system, changes to the integration settings must be made in UTIM on each server individually. Integration settings are not replicated between the primary and secondary servers.

Use the following table to learn more about the integration settings.

Table 28-9 System &gt; Integration &gt; Cisco CallManager Page

| Field  | Considerations   |
|--|--|
| Integration Name   | <i>Display only.</i> This field displays the name of the Cisco CallManager integration entered in UTIM.  |
| Manufacturer   | <i>Display only.</i> This field displays the phone system manufacturer selected in UTIM.   |
| Model  | <i>Display only.</i> This field displays the phone system model selected in UTIM.  |
| Software Version   | <i>Display only.</i> This field displays the phone system software version selected in UTIM.   |
| Trunk Access Code<br>(for dual phone system integrations only) | <i>Display only.</i> This field displays the number that Cisco Unity dials to transfer a call from one phone system to the other. This code was entered in UTIM. |
| Cluster Name   | <i>Display only.</i> This field displays the name of the Cisco CallManager cluster entered in UTIM.  |

**Table 28-9 System > Integration > Cisco CallManager Page (continued)**

| Field                          | Considerations  |
|--------------------------------|---|
| IP Address/Name                | <i>Display only.</i> This field displays the IP address of the publisher (primary) Cisco CallManager server. This address was entered in UTIM.  |
| IP Port                        | <i>Display only.</i> This field displays the TCP port used by the Cisco CallManager servers. This port was entered in UTIM.   |
| RTP/IP Port Base               | <i>Display only.</i> This field displays the first (or base) port number for RTP used by the Cisco CallManager servers. This first port number was entered in UTIM.   |
| Reconnect                      | <i>Display only.</i> This field displays whether Cisco Unity will automatically reconnect to the publisher (primary) Cisco CallManager server after failover has been corrected. The setting True indicates that automatic reconnection is enabled. This value was set in UTIM. |
| IP Addresses                   | <i>Display only.</i> This field displays the IP addresses of the subscriber (secondary) Cisco CallManager servers. These addresses were entered in UTIM.  |
| MWI On Extension               | <i>Display only.</i> This field displays the extension that Cisco CallManager uses to turn MWIs on. This extension was entered in UTIM.   |
| MWI Off Extension              | <i>Display only.</i> This field displays the extension that Cisco CallManager uses to turn MWIs off. This extension was entered in UTIM.  |
| Resynchronize At               | <i>Display only.</i> This field displays the time each day that Cisco Unity resynchronizes MWIs for every subscriber account. This time was entered in UTIM. Resynchronization occurs only when it is enabled in UTIM.  |
| Number of Ports                | <i>Display only.</i> This field displays the number of voice messaging ports set up in UTIM to connect Cisco Unity to the Cisco CallManager server.   |
| CallManager Device Name Prefix | <i>Display only.</i> This field displays the prefix Cisco CallManager adds to the device name for the voice messaging ports. This prefix was entered in UTIM and must match the prefix used by Cisco CallManager.   |

## SIP Integration

The integration settings are specified during installation in the Cisco Unity Telephony Integration Manager (UTIM), which configures Cisco Unity to work with the specified phone system. Once the integration is set up, you should not need to change the integration settings, but you can review them on the Integration page or revise them in UTIM.



### Note

If you have a Cisco Unity failover system, changes to the integration settings must be made in UTIM on each server individually. Integration settings are not replicated between the primary and secondary servers.

Use the following table to learn more about the integration settings.

**Table 28-10 System > Integration > SIP Page**

| Field            | Considerations   |
|------------------|--|
| Integration Name | <i>Display only.</i> This field displays the name of SIP integration entered in UTIM.    |
| Manufacturer     | <i>Display only.</i> This field displays the phone system manufacturer selected in UTIM. |

**Table 28-10 System > Integration > SIP Page (continued)**

| Field   | Considerations   |
|---|--|
| Model   | <i>Display only.</i> This field displays the phone system model selected in UTIM.  |
| Software Version  | <i>Display only.</i> This field displays the phone system software version selected in UTIM.   |
| Trunk Access Code<br><i>(for dual phone system integrations only)</i> | <i>Display only.</i> This field displays the number that Cisco Unity dials to transfer a call from one phone system to the other. This code was entered in UTIM.                             |
| Cluster Name  | <i>Display only.</i> This field displays the name of the SIP cluster entered in UTIM.  |
| IP Address/Name   | <i>Display only.</i> This field displays the IP address of the primary SIP proxy server. This address was entered in UTIM.   |
| IP Port   | <i>Display only.</i> This field displays the IP port used by the primary SIP proxy server. This port was entered in UTIM.  |
| IP Addresses  | <i>Display only.</i> This field displays the IP addresses of the secondary SIP proxy servers. These addresses were entered in UTIM.  |
| Authentication<br><i>(only when authentication is enabled)</i>        | <i>Display only.</i> This field displays whether Cisco Unity authenticates with the SIP proxy server. The setting True indicates that authentication is enabled. This value was set in UTIM. |
| Name<br><i>(only when authentication is enabled)</i>                  | <i>Display only.</i> This field displays the name the SIP proxy server uses for authentication. This name was entered in UTIM.   |
| Contact Line Name   | <i>Display only.</i> This field displays the voice messaging line name that subscribers use to contact Cisco Unity. This line name was entered in UTIM.                                      |
| Starting RTP Audio Port   | <i>Display only.</i> This field displays the first RTP audio port that subscribers use to contact Cisco Unity. This first RTP audio port was entered in UTIM.                                |
| Preferred Codec   | <i>Display only.</i> This field displays the preferred codec that subscribers use when contacting Cisco Unity. This codec was selected in UTIM.  |
| Number of Ports   | <i>Display only.</i> This field displays the number of voice messaging ports set up in UTIM to connect Cisco Unity to the SIP proxy server.  |

## Circuit-Switched Integration

The integration settings are specified during installation in the Cisco Unity Telephony Integration Manager (UTIM), which configures Cisco Unity to work with the specified phone system. Once the integration is set up, you should not need to change the integration settings, but you can review them on the Integration page or revise them in UTIM.



### Note

If you have a Cisco Unity failover system, changes to the integration settings must be made in UTIM on each server individually. Integration settings are not replicated between the primary and secondary servers.

Use the following table to learn more about the integration settings.

**Table 28-11 System > Integration > Circuit-Switched Page**

| Field   | Considerations  |
|---|---|
| Integration Name  | <i>Display only.</i> This field displays the name of integration entered in UTIM.   |
| Manufacturer  | <i>Display only.</i> This field displays the phone system manufacturer selected in UTIM.  |
| Model   | <i>Display only.</i> This field displays the phone system model selected in UTIM.   |
| Software Version  | <i>Display only.</i> This field displays the phone system software version selected in UTIM.  |
| Trunk Access Code<br><i>(for dual phone system integrations only)</i>   | <i>Display only.</i> This field displays the number that Cisco Unity dials to transfer a call from one phone system to the other. This code was entered in UTIM.  |
| MWI On Code<br><i>(for analog or DTMF integrations only)</i>  | <i>Display only.</i> This field displays the code that the phone system uses to turn MWIs on. This code was entered in UTIM.  |
| MWI Off Code<br><i>(for analog or DTMF integrations only)</i>   | <i>Display only.</i> This field displays the code that the phone system uses to turn MWIs off. This code was entered in UTIM.   |
| SMDI Field Length<br><i>(for serial or SMDI integrations only)</i>  | <i>Display only.</i> This field displays the SMDI or station field length for the phone system. The SMDI field length is the length of the SMDI or station prefix plus the default extension length. The length is either 10 or 7. This value was entered in UTIM and must match the settings used by the phone system.<br><br>SMDI serial integrations use SMDI packets to send information about the call. The information in an SMDI packet varies according to the phone system, but the packet may include ANI, DNIS, call type (forward or direct), and forwarding station. |
| Default Extension Length<br><i>(for serial or SMDI integrations only)</i>   | <i>Display only.</i> This field displays the default length of extensions on the phone system. This length was selected in UTIM.  |
| Resynchronize At  | <i>Display only.</i> This field displays the time each day that Cisco Unity resynchronizes MWIs for every subscriber account. This time was entered in UTIM. Resynchronization occurs only when it is enabled in UTIM.  |
| Serial Communication Settings:<br><ul style="list-style-type: none"> <li>• COM Port</li> <li>• Baud Rate</li> <li>• Data Bits</li> <li>• Stop Bits</li> <li>• Parity</li> </ul> <i>(for serial or SMDI integrations only)</i> | <i>Display only.</i> The fields in this section show the serial communication settings used in SMDI serial integrations. These settings are disabled for other types of integrations.<br><br>The COM Port field setting specifies the communications port on the Cisco Unity server. The Baud, Data Bits, Stop Bits, and Parity field settings must match the serial communication settings used by the phone system.   |
| Number of Ports   | <i>Display only.</i> This field displays the number of voice messaging ports set up in UTIM to connect Cisco Unity to the phone system.   |

# Enabling a Warning Tone for End of Recording

This feature applies only to integrations with Cisco CallManager and SIP phone systems.

Cisco Unity can be set to sound a warning tone before reaching the maximum allowable message length while callers record their messages. By default, the warning tone is disabled. There are two settings that can be customized:

- The number of milliseconds before reaching the maximum message length when the warning tone will sound. Any setting greater than 0 enables the warning tone.
- The maximum recording length in milliseconds for which no warning tone will sound. This setting prevents the warning tone from sounding for shorter recordings such as voice names.

For example, if the maximum message length is set for 300 seconds and the first setting is set for 10 seconds, the warning tone will sound after 290 seconds of recording—10 seconds before the recording limit is reached and the recording session is terminated.

To enable the warning tone, do the following procedure.

## To Enable the Warning Tone for the End of Recording

---

- Step 1** On the Cisco Unity server, browse to the `CommServer\Utilities\AdvancedSettingsTool` directory and double-click **UnityAdvancedSettingsTool.exe**. The Unity Registry Settings window appears.
  - Step 2** In the Unity Settings box on the left, click **Record Termination Warning Time**. Information about this setting appears in the Description box.
  - Step 3** In the New Value field, enter a number of milliseconds to indicate when the warning tone will sound. The tone sounds this number of milliseconds prior to the end of the allowed recording time. We recommend entering **10000**.
  - Step 4** Click **Set**.
  - Step 5** In the Unity Settings box on the left, click **Minimum Recording Length for Termination Warning**.
  - Step 6** In the New Value field, enter the maximum recording length in milliseconds for which no warning tone will sound. We recommend entering 30000.
  - Step 7** Click **Set**.
  - Step 8** Click **Exit** to close the Unity Registry Settings window.
  - Step 9** For the settings to take effect, exit and restart the Cisco Unity software.
-

