CHAPTER 3

Using the Cisco IPICS System

This chapter provides tips and guidelines for using the Cisco IPICS system and includes the following sections:

Managing the RMS

The RMS enables the Cisco IPICS PMC to remotely attach to a VTG and provides support for remotely combining two or more VTGs through its loopback functionality.

To manage the RMS on Cisco IPICS, you must first configure the RMS for use with the Cisco IPICS server. The Cisco IPICS server accesses the RMS by using Secure Shell Client software and it authenticates the RMS by using the credentials that you configure in the RMS in the Configuration > RMS window in the Administration Console.

Note You must configure the RMS components exactly as described in "Appendix A: Configuring the Cisco IPICS RMS Component" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for the Cisco IPICS system to work correctly.

You must configure at least one RMS per Cisco IPICS server. You cannot configure the same RMS in multiple Cisco IPICS servers.

You may implement more stringent security measures and harden your system security by configuring additional security features that Cisco IOS provides. For more information about configuring authentication, password security, and additional layers of security, refer to the *Cisco IOS Security Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_book09186a008049e249.html

You must configure at least one T1 or E1 loopback in the RMS to support mixing. The configuration steps that are required to implement the loopback pairs may vary depending on card type, Cisco IOS version, and the type of supported RMS that you use.

Note For a complete list of supported interface cards and RMS routers, refer to the *Cisco IPICS Compatibility Matrix* at the following URL: http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Before adding an RMS, make sure that you meet the following conditions:

- The router must exist on the Cisco IPICS network
- You must define at least one location

For detailed information about how to configure an RMS and locations, refer to the "Managing the RMS" section and the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

You can view and edit information for any RMS in your Cisco IPICS network. You can also deactivate an RMS, which makes it unavailable for use by Cisco IPICS, or reactivate an RMS by pressing the **Activate** or **Deactivate** button.

You can merge, update, and show RMS configuration information by using the Configuration drop-down list box in the RMS window in the Administration Console.

Note By default, Cisco IPICS polls the RMS every ten minutes by using the RMS comparator mechanism. The RMS comparator checks the responsiveness of the RMS. If there have been any changes made to the configuration, and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. You can change the polling period by entering a new value in the **RMS Polling Frequency** field in the Options window in the Administration drawer. This setting specifies how often the Cisco IPICS polling mechanism checks whether the server can reach all RMS components that are listed in the RMS window.

Tip Because the RMS comparator mechanism can interject delays, you can disable it by navigating to **Administration > Options** and checking the **Disable RMS Comparator** check box. You should check this check box if you connect via a high latency, low bandwidth connection, such as a satellite link.

For more detailed information about managing the RMS, refer to "Managing the RMS" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing Radios

This release of Cisco IPICS provides support to define radio channels in the Cisco IPICS server and implements a radio console skin for the PMC that enables the PMC to send RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis. At the LMR gateway, the packets gets converted into audible tones via the configured ear and mouth (E&M) interface to the physical radio to provide tone control for radios.

You perform radio management in the Configuration > Radios window.

Tone control (also referred to as *Tone Remote Control* (TRC)) refers to the use of inband tone sequences to control a radio that is connected to an LMR gateway (typically a base station). In Cisco IPICS, you can use tone control to modify or

tune to a different radio frequency (RF) channel, change the transmit power level, and to enable or disable radio built-in encryption, as well as other uses. TRC uses well-defined audio sounds (also referred to as *tones*) to change the behavior of a device. A tone-keyed radio system requires that a specific tone be present on the incoming analog (e-lead) port. If this tone is not present, the radio does not transmit audio.

The PMC includes a radio console skin that provides support for channel selector buttons. The PMC can display up to nine channel selector buttons that PMC users can use for signaling, changing channels, or controlling tone sequences. The PMC generates the necessary radio control tone sequences when users press the associated button.

For more detailed information about channel selectors, refer to "Manging Radios" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Note For information about various Requests for Comment (RFCs), access the RFC repository that is maintained by the Internet Engineering Task Force (IETF) at the following URL: http://www.ietf.org/rfc.html.

Tip When you configure channel selectors, you should consider the different actions that users may want to perform on the channel and what commands need to be sent to the radio when those actions are being performed.

Tone control sequences, which are defined in either a tone descriptor file or in the radio descriptor file, contain information about how to tune the radio to another frequency within that radio. For more information about tone and radio descriptor files, see the "Managing Radio and Tone Descriptors" section on page 3-5.

A tone control can be either a stateful operation or a momentary operation. If a control is stateful, the PMC displays the button.

For example, Encryption is a stateful operation and the PMC monitors its setting. Another example of a stateful operation is a Transmit Power setting that can be toggled between High, Medium, and Low.

A momentary control is one in which the functional state is not monitored or remembered. Most signals are momentary, meaning that they are sent without being monitored by the system.

For information about tone and radio descriptors, see the "Managing Radio and Tone Descriptors" section on page 3-5. For detailed information, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing Radio and Tone Descriptors

Cisco IPICS allows you to create and/or update radio and tone descriptor files. Radio and tone descriptors are .xml files that define the capabilities for specific radio types, and over-the-air signals that can be associated to one or more Cisco IPICS channels.

You can add and update radio and tone descriptors in the Administration Console by navigating to **Configuration > Descriptors.**

This section contains the following topics:

Radio Descriptors

Radio descriptors are .xml files that contain commands that are used to control functions on a radio. These files contain the following elements:

- Channel selectors—Used to change the frequency on a radio
- Control functions—Stateful controls, such as power settings and encryption on/off, and simple (momentary) controls, such as monitor and scan

For each radio capability, the radio descriptor defines the tones (events) that need to be sent to the radio to enable/disable that capability.

Note For channel selectors and control functions, Cisco IPICS supports only RFC 2833 tones. Refer to "Managing Radios" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more detailed information.

The tone control sequences, that define the control functions, can be included directly in the radio descriptor or can be referenced by name in a tone descriptor file. For more information about tone descriptors, see the "Tone Descriptors" section on page 3-6.

You can add and/or update radio descriptors in Cisco IPICS in the Descriptors window by navigating to the **Configuration > Descriptors** window in the Administration Console.

Note If you must modify or create radio descriptors, refer to the documentation that came with your radio, or other device that is being controlled, for the specific tone sequences that it supports.

Caution Because improperly constructing an .xml file, removing a radio descriptor file, or removing elements from a radio descriptor file may have unpredictable results, Cisco recommends that you only modify the radio descriptor file when absolutely necessary.

For detailed information about adding or updating descriptor files, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*. To see examples of valid and invalid descriptor file .xml entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1).*

Tone Descriptors

A tone descriptor is an .xml file that defines a sequence of momentary controls and over-the-air signals that can be associated to one or more Cisco IPICS channels. Commands can be referenced by any radio descriptor and signals can be associated to any channel.

The maximum number of consecutive control and signaling tones is six.

Note Simple control functions can reference only RFC 2833 tone events. However, momentary signals can reference both RFC 2833 tone and RFC 2833 event (DTMF) commands. For more information, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).* For some examples of valid and invalid descriptor file entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1).*

Unlike momentary controls, signals do not cause the radio to change configuration; rather, signals are treated like voice and are transmitted over the currently-tuned radio channel frequency.

Each tone in a sequence is specified by the frequency (from zero to 3999 Hz), a decibel (db) level (0 to -63), and a duration in milliseconds (ms).

Note An RFC 2833 tone or event has a maximum duration of eight seconds. Refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more information.

You can add and/or update tone descriptors in Cisco IPICS in the Descriptors window by navigating to the **Configuration > Descriptors** window in the Administration Console.

Note If you must modify or create tone descriptor files, refer to the documentation that came with your radio, for the specific control and signaling sequences that it supports.

Caution Improperly constructing a .xml file, removing a tone descriptor file, or removing elements from a tone descriptor file, that is reference by a radio descriptor file, may have unpredictable results. Cisco recommends that you only modify the tone descriptor file when absolutely necessary.

For detailed information about descriptor management in Cisco IPICS, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing and Using the Cisco IPICS Policy Engine

The Cisco IPICS policy engine lets you create and manage policies. Policies are comprised of one or more actions that perform when the policy executes. The policy engine includes the dial engine. Using the dial engine, you can manage standard and custom scripts and prompts that enable telephony user interface (TUI) interaction and incoming and outgoing calls.

Note Only the system administrator, dispatcher, or operator can administer the Cisco IPICS dial engine functionality. A system administrator can perform any activity in the Dial Engine drawer. A dispatcher or operator can perform only those activities that relate to managing spoken name prompts for the users who belong to the same ops view as the dispatcher.

To perform policy engine and dial engine functions, navigate to the Policy Engine tab and choose either the **Policy Management** drawer or the **Dial Engine** drawer.

Note To enable the policy engine, you must install a Cisco IPICS license that includes the policy engine feature.

This section contains the following topics:

Dial Engine Considerations

As part of the dial engine functionality, Cisco IPICS provides default configuration settings for tracing. These settings are designed for optimal system performance but you can change them if needed. Tracing consumes system resources; therefore, if you require additional trace information for the dial engine, follow these guidelines to conserve system resources:

- Increase the number or the size of trace files only if necessary.

- Keep the number and the size of trace files to the minimum values that provide the information that you need.
- Enable only the trace settings that you need or that you are instructed to enable by the Cisco TAC.
- If you enable trace settings, disable them when you no longer need them.

  The system begins to log information in a new trace file each time that the current file reaches the designated maximum file size. When the number of trace files that are stored on the system reaches a designated value, each subsequent trace file overwrites the oldest existing trace file.

Note The total size of all dial engine trace files that are stored on the system cannot exceed 3 GB.

- When you delete a language, in the Dial Engine > Prompt Management > Languages window, the logical folder for that language and all contents of the folder are removed from the repository. You can delete a single language or several languages at one time.

Note If you delete a language while the policy engine is executing a dial engine script that uses that language, script execution may not be successful because the script may not be able to access a prompt that it requires.

- To display the Standard Script Prompts window, navigate to **Dial Engine > Prompt Management > Standard Script Prompts**. By default, the Standard Script Prompts window lists all standard script prompts. To see a list of only standard script prompts that are stored in a particular logical language folder, choose that language from the Language drop-down list and then click **Query**.
- When you delete a standard script prompt or a customized script prompt, it is removed from the repository. You can delete a single prompt or several prompts at one time.

Note Before you delete a prompt, make sure that it is not used by a script. The system does not warn you if the prompt is being used by a script.

- The dial engine includes the following system scripts, which cannot be modified or deleted. You can add additional scripts.
  - BulkNotifyDialer—Used to notify recipients when Cisco IPICS receives an external notification request
  - IppeDialin—TUI main menu
  - IppeDialout—Used to place outbound calls
  - IppeRecording—Used to record spoken names
- The policy engine functionality requires that a SIP provider be configured in your network. A SIP provider handles calls to and from the policy engine.

Note You must use Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider. You configure Cisco Unified Communications Manager for the policy engine in Cisco Unified Communications Manager Administration. Refer to "Configuring and Managing the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information about configuring Cisco Unified Communications Manager as the SIP provider.

- You perform the SIP configuration in the Dial Engine > SIP Configuration window.

  Table 3-1 shows the panes and fields in the SIP Configuration window, and the appropriate actions that you can take to enter required information.

Table 3-1 Fields in the SIP Configuration Window

Pane	Field and Action
SIP Subsystems Configuration	• Port—Enter the SIP port that the policy engine uses. • User Agent—Enter the user agent that the policy engine uses. • Maximum Retransmissions—Enter the maximum number of times that SIP requests and responses are transmitted. • First Retransmission (in msec)—Enter the number of milliseconds to wait before performing the first retransmission. **Note** The default maximum transmissions and first retransmission values are appropriate in most cases. You should not change these values unless you fully understand the characteristics of the network on which Cisco IPICS and the SIP provider are deployed and understand the SIP retransmission algorithms that are described in the RFC 3261 specification.
SIP Provider Configuration	• Host—Enter the IP address or the host name of the SIP provider. • Port—Enter the port number that the SIP provider uses for SIP. • Transport drop-down list—Choose the transport protocol (TCP or UDP) that matches the transport protocol of the SIP provider. **Note** If both protocols are configured on the SIP provider, choose either protocol. • Username—Enter the appropriate information. – If Cisco Unified Communications Manager is the SIP provider, enter the Cisco Unified Communications Manager user name for the SIP trunk. – If a Cisco router that is running a supported version of Cisco IOS is the SIP provider, enter any value in this field. • Password—Enter the appropriate information. – If Cisco Unified Communications Manager is the SIP provider, enter the Cisco Unified Communications Manager password for the SIP trunk. – If a Cisco router that is running a supported version of Cisco IOS is the SIP provider, enter any value in this field.

Table 3-1 Fields in the SIP Configuration Window (continued)

Pane	Field and Action
Cisco Unified Communications Manager Configuration for IP Phone Notifications	**Note** The fields in this pane are optional and are required only to execute policies that use the IP Phone Text Notification action, or that use the dial notification action to send a message to a Cisco Unified IP Phone. • Host Name or IP Address—Enter the host name or the IP address of the Cisco Unified Communications Manager server. • Administrator User Name—Enter the name of the Application User in Cisco Unified Communications Manager who has administrator privileges. • Administrator Password—Enter the password of the Application User in Cisco Unified Communications Manager who has administrator privileges. • End User Name—Enter the name of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated. • End User Password—Enter the password of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated. **Note** For information about Cisco Unified Communications Manager Application Users and end users, refer to your Cisco Unified Communications Manager documentation. The changes take effect only after you restart the dial engine. To restart the dial engine, follow these steps: 1. Log in to the Cisco IPICS server as the root user. 2. Enter the following command at the command prompt: [root]# **service ipics restart**

Policy Considerations

A policy defines a set of actions that the system executes according to instructions that you provide in the policy. A policy can be either of these types:

- Invitation—Policy activated only through the TUI that causes the TUI to call designated users and invite them to join a VTG or channel. You can invoke an invitation policy from the TUI breakout menu after you have joined a VTG or a channel. Users that the TUI calls are invited to join that VTG.

Note This policy type is activated only through the TUI.

- Multi-Purpose—Policy that includes any one of the following action types:
  - Activate VTG—Activates the designated, preconfigured VTGs.
  - Notification—Contacts designated recipients according to notification instructions that you specify. Notification action types include e-mail, IP Phone Text, Dial, Talk Group, and Dial Engine Script.

    For information about using notification for recipients outside of the Cisco IPICS system, see the "Using External Notifications in Cisco IPICS" section on page 3-14.
  - VTG Add Participants—Adds the designated participants to the designated VTG.
  - Dial Out—Calls the designated users according to their configured dial preferences to invite them to join the designated VTG.

Note A Multi-Purpose type policy can be activated by a trigger, by reactivating it in the Policy Management > Execution Status window, or through the TUI. An Invitation Type policy can be activated only through the TUI.

Tip When you create a policy, make sure that your system has sufficient resources (multicast addresses and dial ports) to accommodate the associated VTGs when they execute. Cisco IPICS does not warn you that the execution of a policy may over-commit system resources when it activates VTGs.

Using External Notifications in Cisco IPICS

You can also use Cisco IPICS to send notifications to recipients who are not configured in Cisco IPICS. This type of notification is called an *external notification* and performs the following functionality:

1. Simultaneously calls many external users at telephone numbers that Cisco IPICS obtains from a file that you specify.
2. Plays a designated message to each user who answers the call.
3. Captures results of each call in a log file that you can review at any time.

You invoke an external notification by sending an HTTP request or by posting a Common Alerting Protocol (CAP) .xml file to the appropriate server.

For more detailed information about external notifications, refer to "Using Cisco IPICS for External Notifications" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Guidelines for Using the TUI

When you use the TUI, be aware of the guidelines that are listed in the following sections:

- General Guidelines, page 3-14
- Menu Guidelines, page 3-16

General Guidelines

The following general guidelines apply when you use the TUI:

- After you dial in to the TUI, the system prompts you to enter your user ID and PIN (password). You must authenticate before you can continue to use the system.
- When you call the system, the language in which you hear prompts is the default language that is configured for the ops view with which you are associated.
- The system spells out your user name if you do not have a recorded spoken name.

- After you authenticate, the system announces the available menu options, such as joining a channel or VTG, invoking a policy, or accessing the system menu.
- The TUI allows you to interrupt a prompt and dial ahead by entering your next option before the prompt has finished.
- A menu times out if you do not respond within the predefined allowable period of time. In most instances, this period of time is 3 seconds and includes a maximum retry limit of 3. When the allowable period of time has expired, the TUI responds with “Are you still there?” and the menu repeats. When the maximum retry limit has been exceeded, the TUI responds with a warning prompt to inform you that the call will be disconnected and then it terminates the call.
- If the system does not detect a response to the prompts after a predefined number of consecutive attempts, the system returns you to the previous menu or terminates the call, if you are using the main menu.
- When you enter an incorrect key option, the TUI responds with “Please try again” and the menu repeats.
- When you dial out to invite a party in to a call, the called user must press any key to authenticate before the call is connected to the channel or VTG. (As the call is being dialed out, the system does not play any audible sounds.)
- To terminate your input, press #.
- To return to the previous menu, except when you are using the main menu, press *.
- To select resources, such as groups or policies, from a menu, press the number that corresponds to your selection when the number of entries is 9 or less. When 10 or more entries exist, you must press the number that corresponds to your selection followed by #.
- The option to select a resource by spelling its name depends on your locale:
  - The TUI supports the following locales: Afrikaans (af), Albanian (sq), Basque (eu), Catalan (ca), Danish (da), Dutch (nl), English (en), Faroese (fo), Finnish (fi), French (fr), German (de), Icelandic (is), Irish (ga), Italian (it), Norwegian (no), Portuguese (pt), Rhaeto-Romanic (rm), Scottish (gd), Spanish (es), Swedish (sv)

  - If you use a locale that does not support dial by name, such as locales that do not have equivalent characters available on the phone keypad to enable dial by name, you must make your selection from the list of available resources.

Menu Guidelines

The following guidelines apply when you use the TUI menus:

- Transfer and conference features are not supported on a phone when the phone is connected to the TUI.
- From the TUI main menu, you can take the following actions:
  - To join a group, press 1. Then, you can press 1 to select an assigned group to join by spelling out the group name, or press 2 to listen to the list of assigned groups and then selecting from that list. (If you know the name of the group that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available groups.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke a general purpose policy, press 2. Then, you can press 1 to select a policy by spelling its name, or press 2 to listen to the list of available policies. (If you know the name of the policy that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available policies.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke the system menu, press 0. From this menu, you can take the following actions:

    - To access system help, press 1. This option provides an overview of the system menu.

    - To manage your user profile, press 2. To change your PIN, or password, press 1. To change your recorded name, press 2.

    - To obtain policy status, press 3. To replay the information, press 1.

    - To return to the previous menu from these menus, press *.
- The TUI provides a dial-in floor control feature to support dial-in users:
  - From the TUI call menu, you can take the following actions:

- To request the floor, press 1. You hear a single beep if you obtain the floor. You hear a busy tone if the floor is not available to you.

- To release the floor, press 2. You hear a double-beep to confirm that the floor is released.

  - The dial-in floor allows one dial-in user at a time to speak in a group. It does not control whether other PTT users can speak.
  - When you have the dial-in floor, you can speak and be heard by other users in a group, but you cannot hear other users talking.
  - When you have the dial-in floor, the TUI prompts every two minutes to confirm that you want to keep the floor. Press 1 to keep the floor or press 2 to release the floor.

- From the TUI breakout menu, you can take the following actions:
  - To access system help, press 1. This option provides an overview of the system menu.
  - To invite a dial user to join the call by using an ad-hoc invitation or by using an invitation policy, press 2.

    - To perform an ad-hoc invitation, press 1. To confirm your selection, press 1 (no audible sounds play during the time that it takes for the remote party to pick up and authenticate). To try your call again, press 2. To cancel, press *.

    - To perform an invitation policy, press 2. To choose an invitation policy by spelling out the name, press 1. To listen to the list of invitation policies, press 2 and then select from that list. To confirm your selection, press 1. To cancel, press 2. To return to the previous menu, press *.
  - To invoke a general purpose policy, press 3. To choose an invitation policy by spelling out the name, press 1. To listen to the list of invitation policies, press 2 and then select from that list. To confirm your selection, press 1. To cancel, press 2. To return to the previous menu, press *.
  - To leave the call and return to the main menu, press 0.
  - To return to the call, press *.

Managing the Cisco IPICS PMC

You can manage PMC functions that include configuring the PMC installer, and uploading PMC version packages, alert tone sets, and PMC skin sets, and configuring PMC regions in the Administration > PMC Management window.

This section contains the following topics:

Managing the PMC Installer

The PMC installer installs new PMC version packages and makes them available to PMC users. When you configure the PMC installer, you can choose the IP address or host name of the server, or you can configure a different IP address or host name that you want the PMC users to use.

Note If you choose another IP address or host name instead of the configured IP address or host name, make sure that you test the IP address in the network domain that will be supported with that server.

Cisco recommends that you use the default HTTP and HTTPS ports that are listed in the PMC installer configuration area. The IP address, HTTP port, and HTTPS port fields affect only the PMC installer and do not have an immediate effect on PMC clients that have already been installed on user PMC client machines.

Note To change the HTTP and HTTPS values, Cisco recommends that you inform all PMC users to connect to the server to download and reinstall an updated version of the PMC.

Managing PMC Versions

The Cisco IPICS server maintains a repository of one or more versions of the PMC. PMC updates can be assembled into upgrade packages that add features and resolve issues. Users can then upgrade their PMC clients at any time by downloading the current version of the PMC executable file.

Note You must configure the PMC installer and upload the PMC upgrade package before users can download and install the PMC on their PMC client machines.

By default, all new PMC versions are saved to a non-operational state after you upload a new PMC version package. The PMC becomes available to users only after you change the state to one of the following states:

- Recommended—This version represents the recommended software version that should run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform the PMC user. The server then sends this version to the PMC and the PMC installs it after the PMC user responds positively to the message prompt or if other installed versions are not supported.
- Staged—This version represents the software version that the PMC downloads according to your discretion. The server sends this version to the PMC for download but the PMC does not download it until you change the state of this version to recommended or operational. At that time, the PMC may install the new version after the PMC user responds positively to the message prompt or if other installed versions are not supported.
- Operational—This version represents a version of PMC software that is operational. This version is supported for use with the server but there may be a later version that is also supported.

Note The server always extends priority to the PMC versions that it marks as recommended.

To force updates immediately, choose the **Not Supported** state from the drop-down list box. This state forces PMC users, who are running this version of the PMC, to restart and download a newer version.

Caution Forcing a PMC automatic update shuts down and then restarts a PMC without warning a user, regardless of the purpose for which the PMC is being used. For this reason, Cisco recommends that you force an update only when it is absolutely necessary.

Managing PMC Alert Tones and Skins

You create PMC alert tone sets and then upload tone sets and skin sets to the server. PMC users can then download the tone and skin sets to their PMC client machines. Alert tone sets and skin sets are associated with ops views, so each PMC user can see only one tone and skin set based on the ops view to which that user belongs.

Note The PMC alert tone feature requires the use of compatible alerting tone files. These files must be .wav files that are encoded in Pulse Code modulation (PCM), which is a sampling technique that digitizes analog signals. These .wav files must be encoded in PCM format with 8 bits monaural samples at 8000 Hz sampling rate for a total of 64 kbps. While higher and lower rates may seem to work, Cisco IPICS does not support the use of any other encoding or bit rates, as they may produce inferior sound quality. Any file that is used with the G.729 codec may sound inferior due to its encoding algorithms. In addition, all alerting tones should be encoded to a nominal value of -20 decibels relative to one milliwatt (dBm) and begin and end with zero deflection to eliminate or minimize "popping" or clicking sounds. For more detailed information, refer to the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1).*

For more information about how to manage PMC alert tones and skins, refer to "Managing PMC Alert Tones" and "Managing PMC Skins" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing PMC Regions

You can configure regions (views) that the PMC displays to the user. A PMC region is a grouping of channels on the PMC. Channels (including radio channels) are divided among regions. Channels, radios, and VTGs are configured to belong to a particular region when they are created.

Note PMC regions display only when you use the 36-channel radio console skin.

When you configure new regions in the Cisco IPICS server, they are represented by tabs that display along the right side of the PMC display. The position of the region determines where the region displays on the PMC.

You can add new PMC regions, view and edit existing regions, and delete regions in the PMC Management > PMC Regions window.

For more information about how to manage PMC regions, refer to "Managing PMC Regions" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Using Cisco Unified IP Phones with Cisco IPICS

The Cisco IPICS service allows several Cisco Unified IP Phone models to communicate and participate in PTT channels and VTGs. Before a user can access the Cisco IPICS service, Cisco IPICS must be configured as a phone service for Cisco Unified Communications Manager or for Cisco Unified Communications Manager Express. In addition, users in a deployment that includes Cisco Unified Communications Manager must subscribe to the Cisco IPICS service by using the Cisco Unified Communications Manager User Options application.

For detailed information about configuring Cisco Unified IP Phones for use with Cisco IPICS, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

After you configure Cisco IPICS as an available service, and IP phone users have subscribed to the service, the Cisco Unified IP Phone Services menu displays Cisco IPICS as an option.

For additional information about Cisco Unified Communications Manager Administration and about setting up phone services, refer to the Cisco Unified IP Phone Services configuration information in the Cisco Unified Communications Manager Administration Guide for your version of Cisco Unified Communications Manager. You can locate the Cisco Unified Communications Manager documentation at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Users should be aware of the following guidelines when using Cisco Unified IP Phones with Cisco IPICS:

- To obtain help with using the Cisco IPICS service on a Cisco Unified IP Phone, press the **Help** softkey.
- A phone that is logged in to the Cisco IPICS service logs out automatically after 30 minutes of inactivity. You can configure a different timeout period in the Administration > Options window.
- You can configure whether the Cisco IPICS service requires users to log in before accessing the service from a Cisco Unified IP Phone. If there are users who you do not want to require to log on, you can configure a separate service in Cisco Unified Communications Manager that bypasses the login for each of these users.

  When you configure the Cisco IPICS service so that it does not prompt for user login credentials on the Cisco Unified IP Phone, the service automatically activates a channel or VTG if only one channel or VTG is assigned.

  If you configure the Cisco IPICS service to bypass the user login and if there are more than one channel or VTG that is assigned, Cisco IPICS displays the list of these channels and VTGs on the IP phone.

  For detailed information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*
- On some model IP phones, you can add a special parameter to the Cisco IPICS Service URL configuration to enable the display of the Logout softkey on the main display while IP phone users are connected to a channel or VTG. For more information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

- If a phone loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service, the service retains its current state and the user can continue to use the PTT functionality for the channel or VTG that is currently selected. However, the phone cannot connect to other channels or VTGs until connectivity to the server is re-established.
- A Cisco IPICS user can be logged in to the Cisco IPICS service with the same login credentials on more than one phone simultaneously. In this case, the following information applies:
  - The user can send and receive audio on all of the phones
  - If the user presses a key on any phone that causes the phone to interact with the server (for example, the **Back**, **Latch**, or **Help** softkey), all phones log out except the last one that was logged into.
- When the Cisco Unified Wireless IP Phone 7921 is connected to an active Cisco IPICS channel or VTG, the phone goes into continuous listening mode. In this mode, the phone remains in an active receive state even if Cisco IPICS is not transmitting audio. In this state, the phone continues to draw power from the battery, which limits the battery life to approximately eight hours of talk time. (When the channel or VTG is deactivated, the phone enters standby mode to conserve power.) To ensure that you have an adequate power supply for your Cisco Unified Wireless IP Phone 7921, Cisco recommends that you maintain a backup battery for use with your phone. For more information about the Cisco Unified Wireless IP Phone 7921, refer to the Cisco Unified IP Phone documentation that is available at the following URL:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

  For information about how to customize the softkeys on the Cisco Unified Wireless IP Phone 7920/7921 to enable direct access to the Services menu, refer to the following URL:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Maintaining User Passwords

Cisco IPICS provides password security features that enforce password complexity (strong passwords) that must adhere to certain rules for user password creation. Cisco IPICS checks for user password length and character requirements, keeps track of password expiration settings, maintains historic passwords in the database, and locks out user accounts after a maximum number of invalid login attempts.

As a system administrator, you can manage user password settings in the Administration > Options > Passwords tab, in the Administration Console.

You can specify the following password settings in the Options window:

- Minimum password length—Specifies the minimum number of characters that a user can enter (to ensure a strong login password, configure the minimum password length to contain at least 8 characters total)
- Minimum digit password length—Specifies the minimum number of numeric characters that a user can enter when creating or changing the digit password (or PIN) in the My Profile window
- Minimum lower case letter count—Specifies the minimum number of lower case letters that a user can enter when creating or changing the login password (the total number cannot exceed the number that is set for the minimum password length)
- Minimum upper case letter count—Specifies the minimum number of upper case letters that a user can enter when creating or changing the login password (the total number cannot exceed the number that is specified for the minimum password length)
- Minimum numeric character count—Specifies the minimum numeric characters that a user can enter when creating or changing the login password (the total number cannot exceed the number that is specified for the minimum digit password)
- Minimum special character count—Specifies the minimum special characters that a user can enter when creating or changing the login password (check that the password contains at least one of the following characters: lower case letter, upper case letter, number, and special characters such as pronunciation mark, exclamation point, asterisk, etc.)
- Password history count—Specifies the number of passwords of which Cisco IPICS keeps track and that the user will not be able to use again.

- Password expiration notification—Specifies the number of days, prior to a password expiring, in which the user will be notified with a warning (if you set the number to 0, then the current password will expire on the actual password expiration date and the user will be forced to create a new password at the next Cisco IPICS login)
- Password expiration—Specifies the number of days in which the Cisco IPICS login password will expire (if you set the value to 0, then the password will never expire)

  At each login, Cisco IPICS checks if the user password is about to expire in the number of days that are configured in the password expiration field. If the date has passed, the user gets notified that the password is about to expire.

Note The notification that the user receives does not apply to digit password.

When the digit password expires, the user receives a warning message when logging in to the server. The user can either dismiss the warning or change the digit password. The message lasts only for the duration of the session.

After the user password expires, the user may still log in by using the old password but is restricted to accessing only the user profile window. Cisco IPICS forces the user to change the password before being able to access other windows.

Note After password expiration, PMC and IP phone clients receive an error message prompting the user to change the password when logging in to the server. Users must change their password before they can resume using the Cisco IPICS service.

- Apply password expiration check box—You can apply the password rules, for both the user and digit passwords, by checking this check box. If you leave the check box unchecked, no password expiration rules apply.
- Maximum invalid login attempts allowed—Specifies the maximum consecutive number of times that a user can attempt to log in to Cisco IPICS with invalid login information (user name/password) before the user account gets locked out.

  A user whose account is locked cannot log in to the Cisco IPICS system. Existing logins continue to work until the user logs out of the system.

When users get locked out of Cisco IPICS, either the system administrator or the operator can unlock the user account from the User Management > Users window.

The invalid login attempt counter resets to 0 after the configured number of expiration hours has been exceeded.

- Failed password attempt expiration—Specifies the number of hours in which Cisco IPICS resets the number of invalid login attempts back to 0 (if you set this value to 3 hours, for example, the value is set back to 0 three hours after a failed login attempt)
- Apply user account lockout check box—You can apply the account lockout rules by checking this check box. If you leave the check box unchecked, no account lockout applies.