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, page 3-1
- Managing and Using the Cisco IPICS Policy Engine, page 3-3
- Managing the Cisco IPICS PMC, page 3-10
- Using Cisco Unified IP Phones with Cisco IPICS, page 3-13
- Maintaining User Passwords, page 3-15

Managing the RMS

An RMS is a component that 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* 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/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/index.htm

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/univercd/cc/td/doc/product/cis/c_ipics/index.htm

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 *Cisco IPICS Server Administration Guide.*

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 show, update, and merge 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 10 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. If there have been changes to the RMS 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.

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 detailed information about managing the RMS, refer to the *Cisco IPICS Server Administration Guide.*

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 TUI interaction and incoming and outgoing calls.

Note Only the system administrator, dispatcher, or operator can use the Cisco IPICS dial engine functionality. A system administrator can perform any activity in the Dial Engine drawer. A dispatcher or operator can only perform 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, access 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:

- Only increase the number or the size of trace files if necessary, or as directed by Cisco support personnel.
- 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 to use them.

  The system begins to log information in a new trace file each time 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, the script may not be able to access a prompt that it requires.

- To display the Standard Script Prompts window, choose **Dial Engine > Prompt Management > Standard Script Prompts**. By default, the Standard Script Prompts window lists all standard script prompts. To see a list only of 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 used by a script.

- The dial engine includes the following system scripts, which cannot be modified or deleted:
  - IppeDialin—TUI main menu
  - IppeDialout—Used to place outbound calls
  - IppeRecording—Used to record spoken names

  You can add other scripts, if needed.
- The policy engine 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 CallManager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider. You configure Cisco Unified CallManager for the policy engine in Cisco Unified CallManager Administration. Refer to the *Cisco IPICS Server Administration Guide* for detailed information about configuring Cisco Unified CallManager as the SIP provider.

- When you configure SIP for the policy engine in the **Dial Engine > SIP Configuration** window, you configure several fields including the following:
  - Maximum Retransmission—Enter the maximum number of times that SIP requests and responses are transmitted (the default value is 2; valid values are 0 through 10)
  - First Retransmission—Enter the number of milliseconds to wait before performing the first retransmission (the default value is 500; valid values are 100 through 4000)

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.

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 the following types:

- Invitation—Policy that causes the TUI to call designated users and invite them to join designated VTGs. This policy type is activated only through the TUI.
- Multi-purpose—Policy that performs any one of the following activities:
  - Activates designated VTGs
  - Adds participants to a VTG
  - Contacts designated users in sequence at each e-mail, Short Message Service (SMS), or pager address that is associated with the user
  - Provides the specified message to designated users by causing the TUI to call them according to the dial preferences that are configured

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 a policy would over-commit system resources when it activates VTGs.

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 3-7
- Menu Guidelines, page 3-8

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 channels, VTGs, 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), Norwegain (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 channel or VTG, press 1. Then, you can press 1 to select an assigned channel or VTG to join by spelling out the channel/VTG name, or press 2 to listen to the list of assigned channels/VTGs and then selecting from that list. (If you know the name of the channel or VTG that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available channels/VTGs.) 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 VTG or channel. 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 VTG or channel, 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, in the PMC Management window in the Administration Console.

This section contains the following topics:

- Managing the PMC Installer, page 3-11
- Managing PMC Versions, page 3-11
- Managing PMC Alert Tones and Skins, page 3-12

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 hardware, or you can configure a different IP address or host name that you want the PMC to use.

Note If you choose another IP address or host name instead of the configured IP address or host name, the IP address should be tested 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 PCs.

Note If you need to change the HTTP and HTTPS values, Cisco recommends that you notify all users that they need to download and reinstall the PMC by using the new pmcsetup.exe file that is generated after you save the changes to these values.

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 PC clients.

When you upload a new PMC version package, all new PMC versions will be saved, by default, in a non-operational state. The PMC users are not able to download the version until 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 that PMC users can then download to their PC 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 is associated.

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.*

For more information about how to manage PMC alert tones and skins, refer to the *Cisco IPICS Server Administration Guide.*

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 CallManager or for Cisco Unified CallManager Express. In addition, users in a deployment that includes Cisco Unified CallManager must subscribe to the Cisco IPICS service by using the Cisco Unified CallManager User Options application.

For detailed information about configuring Cisco Unified IP Phones for use with Cisco IPICS, refer to *Appendix B: Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device* in the *Cisco IPICS Server Administration Guide.*

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 CallManager Administration and about setting up phone services, refer to the Cisco Unified IP Phone Services configuration information in the

Cisco Unified CallManager Administration Guide for your version of Cisco Unified CallManager. You can locate the Cisco Unified CallManager documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

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 into the Cisco IPICS service logs out automatically after 30 minutes of inactivity.
- 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/univercd/cc/td/doc/product/voice/c_ipphon/english/index.htm

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/univercd/cc/td/doc/product/voice/c_callmg/

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 **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.

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 using the browser to log in. The expiration warning message has options to dismiss the warning, or to change the digit password. The message only lasts for the session.

When the user password expires, the user may still log in by using the old password but is restricted to only the user profile window and is forced to change the password before being able to access other windows.

Note After password expiration, PMC and IP phone clients will receive an error message asking the user to change the password when logging in to the server. Users will not have functionality until they change the password.

- 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, then there will be no password expiration rules in effect.
- 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 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, then 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, then there will be no account lockout in effect.

Note When the operator changes the password for any user, the old password is not required to be entered and the strong password checking (except for minimum password length) is disabled.