CHAPTER 8

Configuring and Managing the Cisco IPICS Policy Engine

The Cisco IPICS policy engine includes the dial engine, which enables the TUI and its associated features. Configuring and managing the policy engine includes the following activities:

- Managing the dial engine—Includes monitoring system status and logs, as needed, and configuring several features such as spoken names and direct dial. Also involves managing system and custom scripts and prompts. Scripts enable the TUI to handle incoming and outgoing calls. An executing script plays prompts, which provide audio instructions to users.
- Configuring Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider for use with the policy engine.

You perform the policy engine activities that are described in this chapter from the Dial Engine drawer in the Cisco IPICS Administration Console. To access this drawer, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-15, then choose the **Dial Engine** drawer in the Policy Engine tab.

To access the Dial Engine drawer, you must be assigned one of these Cisco IPICS roles: system administrator, dispatcher, operator role, or all. A system administrator or user with the all role can perform any activity in this drawer. A dispatcher or operator can perform only activities that relate to managing spoken names prompts, managing standard script prompts, and managing customized script prompts.

For additional information about using many of the policy engine features, see Chapter 6, "Using the Cisco IPICS Policy Engine."

Note

- The policy engine requires that dial ports be configured before users can dial in to Cisco IPICS and before the policy engine can dial out to users. For information about configuring dial ports, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 7-29.
- The dial-in and dial-out functionality also requires addresses be available in the multicast pool. For information about configuring the multicast pool, see the "Managing the Multicast Pool" section on page 2-51.

This chapter includes these topics:

Obtaining Information about Dial Engine Services

To operate properly, the dial engine requires a variety of services. You can check the status of these services and view related information, such as the date and time that the service last started. You can also obtain log files, if needed for troubleshooting purposes.

To obtain information about the dial engine service, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Status**.

The Status window displays. This window shows the following information for each service:

- Service Name—Name of the service
- Status—Current state of the service:
  - IN_SERVICE—The SIP subsystem and SIP provider are configured in Cisco IPICS. When the service is in this state, the dial engine can receive calls. However, if the configuration is not correct, for example, if the SIP Provider user name or password is not correct, the dial engine cannot place calls to a SIP provider that requires authentication.
  - OUT_OF_SERVICE—The SIP subsystem is in the process of shutting down.
  - PARTIAL_SERVICE—The SIP subsystem is in the process of shutting down.
  - SHUTDOWN—The SIP subsystem and SIP provider are not configured in Cisco IPICS.
- Description—Brief description of the service

Tip To make sure that the Status window shows the most current information, click **Refresh**.

Step 2 To see a list of subservices for a service, click **+** next to the service name.

To close this expanded view, click **-**.

Step 3 To see additional information or to obtain log files for a service, click the link for the service in the Service Name column.

The Status Details window displays. You can take the following actions in this window:

- View the following information about the service:
  - Service Name—Name of the service
  - Description—Brief description of the service
  - Status—Current state of the service
  - Last Failure—Date and time that the service last failed
  - Last Start Time—Date and time that the service last started
  - Latest Log File—Name of the most current log file that contains information that relates to the service
- Obtain the latest log file for the service. To do so, click the link for the log file and follow the on-screen prompts. (The Latest Log File line in the top part of the window shows the name of the most current log file.)
- Click **Refresh** to make sure that the Status Details window shows the most current information.
- Click **Done** to exit the window.

Managing Tracing for the Policy Engine

The policy engine tracing feature lets you obtain information that can be useful for troubleshooting your system. This feature logs the dial engine and cluster view daemon activities in various trace files. You can configure certain trace facilities and different trace levels to obtain the information that you need.

The policy engine includes these trace facilities:

- Cluster view daemon trace files—Provides information that relates to the cluster view daemon. The files are named Cisco*n*MCVD*n*.log, where *n* is a number that varies depending on your configuration.
- Dial engine trace files—Provides information that relates to the dial engine. The files are named Cisco*n*MIVR*n*.log, where *n* is a number that varies depending on your configuration.
- driverManager*n*.log files—Created if tracing is enabled for the LIB-MEDIA facility. *n* is a number that the system assigns to the file. It increments by 1 when a new file is created.

- Other trace files—Various additional files that may be required by the Cisco Technical Assistance Center (TAC) if you need troubleshooting assistance.

The policy engine provides these trace levels:

- Debug—Generates detailed information.
- XDebug *n* (extended debug)—Generates more verbose detailed information. *n* is a number 1 through 5 that indicates the level of xDebug logging that is enabled.

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

- 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

Managing tracing involves these activities:

- Configuring the Number and Size of Dial Engine Trace Files, page 8-5
- Configuring Trace Levels for Dial Engine Trace Files, page 8-6
- Performing Advanced Tracing Activities, page 8-8
- Obtaining Trace Files, page 8-10
- Interpreting Trace Files, page 8-10

Configuring the Number and Size of Dial Engine Trace Files

The dial engine trace facility logs information that is related to several dial engine services. It stores information in dial engine trace files. You can specify the number of dial engine trace files and the size of each trace file.

The system begins to log information in a new trace file each time that the current one 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. The total size of all dial engine trace files that are stored on the system cannot exceed 3 GB.

To configure dial engine trace files, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Tracing**.

The Tracing window displays.

Step 2 In the Number of Trace Files field, enter the number of trace files that the system creates before starting to overwrite existing files.

This entry is required. The default number of trace files is 100.

Step 3 In the Trace File Size field, enter the maximum size, in KB, of each trace file.

The system starts a new trace file when the current one reaches this maximum size. The default file size is 3145 KB.

This entry is required. The default number of trace files multiplied by the trace file size should not exceed 3 GB.

Step 4 In the Trace File configuration area, click **Save**.

If you do not want to save your changes, click **Cancel**.

Configuring Trace Levels for Dial Engine Trace Files

Trace levels specify what information Cisco IPICS logs in the dial engine trace files.

Cisco IPICS provides default trace levels that are designed to log important information while ensuring optimal system performance. You can change tracing levels if you need additional tracing information. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Tracing**.

The Tracing window displays.

Step 2 In the Trace Settings area, take any of these actions:

- To enable Debug or various XDebug levels for a facility, check the appropriate check boxes. There are five XDebug levels available.
- To disable a Debug or XDebug level for a facility, uncheck its check box.
- To set the default trace levels, click **Restore Defaults**.

  This action enables Debug tracing for the ENG and the SS_SIP facilities in the Trace settings area. It also enables tracing for the CVD and the CLUSTER_MGR facilities (under the CVD category) in the Advanced Trace settings area. All other tracing in both areas is disabled.

The Trace Settings area lists facilities under these categories:

- Workflow Application Scripts—Module that is responsible for the policy engine dial scripts at run time.
- Call Control—Module that is responsible for telephony signalling.

You may need to click the **+** next to a category name to see its associated facilities. To close an expanded view, click **-**.

Table 8-1 describes the facilities in the Trace Settings area.

Table 8-1 Facilities in Trace Settings Area

Facility	Description
Workflow Application Scripts Category	
APP_MGR	Provides trace information for the Applications Manager, which manages loading, invoking, and executing scripts
ENG	Provides trace information for the dial engine run time

Table 8-1 Facilities in Trace Settings Area (continued)

Facility	Description
Call Control Category	
SS_SIP	Provides trace information for the SIP Subsystem, which is the interface between the dial engine and the SIP provider (Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS)
LIB_MEDIA	Provides trace information for the Media Library, which manages media traffic between the dial engine and incoming or outgoing calls

Step 3 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Performing Advanced Tracing Activities

You can perform the following advanced tracing activities for dial engine trace files.

Note Cisco recommends that you do not perform advanced tracing activities unless you are instructed to do so by the Cisco TAC.

- Configure tracing for additional policy engine facilities—You can set trace levels for facilities other than those described in the "Configuring Trace Levels for Dial Engine Trace Files" section on page 8-6.
- Dump to the threads trace file—This file contains stack trace information about all threads that are running in the dial engine. You can dump information to this file when you need it. In addition, the system may create this file if it detects a potential problem. When new information is generated, it is appended to the existing threads trace file. The threads trace file is named JVM.log.

- Dump to the memory trace file—This file contains stack trace information about memory activities in the dial engine. You can dump information to this file when you need it. When new information is generated, the system creates a new memory trace file. The memory trace file is named memory-*n*.log, where *n* is a number that varies depending on your configuration.

To configure additional tracing or to dump to a trace file, perform the following procedure.

Note You can reset all trace levels to their default values by choosing **Control Center > Tracing** from the Dial Engine drawer and clicking **Restore Defaults** at the bottom of the Trace Settings area.

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Tracing**.

The Tracing window displays.

Step 2 Click **Advanced** at the bottom of the Tracing window.

Step 3 To set trace levels, take either of these actions in the Advanced Trace Settings area:

- To enable Debug or various XDebug *n* (extended debug) levels for a facility, check the appropriate check boxes.
- To disable a Debug or XDebug level for a facility, uncheck its check box.

The Trace Settings area lists facilities under various categories. You may need to click the **+** next to a category name to see its associated facilities. To close an expanded view, click **-**.

Step 4 To dump a trace file, take either of these actions in the Advanced Trace Settings area:

- Click **Dump Threads Trace** to dump data to the threads trace file.
- Click **Dump Memory Trace** to dump data to the memory trace file.

A message indicates whether the dump was successful.

You can view or download a file that you dumped as described in the "Obtaining Trace Files" section on page 8-10.

Step 5 Click **Save** to save any changes to the trace level settings.

If you do not want to save your changes, click **Cancel**.

Obtaining Trace Files

Trace files are stored on the Cisco IPICS server. You can obtain trace files from the Cisco IPICS Administration Console. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Status**.

The Status window displays.

Step 2 Take one of these actions:

- To obtain cluster view daemon trace files, click the **Cluster View Daemon** link.
- To obtain dial engine trace files, a threads trace file or a memory trace file, click the **Dial Engine** link.

The Status Details window displays.

Step 3 In the Relate Log Files list, click the link for the desired log file and follow the on-screen prompts to open or save the file.

Interpreting Trace Files

Dial engine and cluster view daemon trace files contain information in standard Syslog format. These files include some or all of the following information for each event that they record:

- Line number
- Date and time that the event occurred
- Category and facility name

- Severity level
- Message name
- Explanation
- Parameters and values

For additional assistance with interpreting trace files, contact the Cisco TAC.

Managing Prompts

Prompts are recorded words or phrases. The policy engine TUI executes scripts, which use prompts to provide audio instructions and information to dial-in users.

Cisco IPICS stores prompts in the *repository* on the Cisco IPICS server. The repository is a logical storage medium in which prompts are contained and organized.

This section includes these topics:

- Managing Languages for Prompts, page 8-11—Describes how to add, rename, and delete logical language folders under which prompts are stored
- Managing Standard Script Prompts, page 8-14—Describes how to upload standard script prompts to the repository
- Managing Customized Script Prompts, page 8-16—Describes how to upload customized script prompts to the repository, download these prompts so that you can listen to them, view details about these prompts, rename these prompts, and delete these prompts
- Managing Spoken Names Prompts, page 8-21—Describes how to upload spoken names to the repository, download spoken names so that you can listen to them, record spoken names, and delete spoken names

Managing Languages for Prompts

Cisco IPICS stores prompts in the repository in logical folders that correspond to the languages of the prompts. When the policy engine TUI executes a script, it plays prompts from the language folder that is designated for the script. In this

way, you can control the language in which a script executes. A special logical language folder, called default, makes prompts available to any script, regardless of the language that is designated for the script.

Managing languages for prompts involves performing the following activities to manage logical language folders:

Viewing a List of Languages

The Languages window displays a list of the logical language folders that are in the repository. For each language, this window shows the following information:

- Language—Descriptive name of the language obtained automatically based on the ISO-compliant name of the logical folder for the language
- Language Name—ISO-compliant name of the logical folder for the language
- Date Modified—Date and time that the folder was last modified
- Modified By—Cisco IPICS user ID of the user who last modified the folder

To display the Languages window, choose **Dial Engine** > **Prompt Management > Languages** from the **Policy Engine** tab.

Adding a Language

When you add a language, the system creates a logical folder for the language in the repository.

To add a language, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Languages**.

The Language window displays.

Step 2 Click **Add** at the bottom of the list of actions.

Step 3 In the Language Name field, enter a name for the logical folder.

This entry is required. The name must be ISO-compliant. For example, enter **en_US** for U.S. English, or enter **en** to use English as a base language if you will use several versions English.

Step 4 Click **Save** to save the new language.

If you do not want to save the new language, click **Cancel**.

Renaming a Language

When you rename a language, you change the name of a logical folder for the language.

If you rename 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 rename a language, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Languages**.

The Language window displays.

Step 2 Check the check box next to the language that you want to rename.

Step 3 Click **Rename** at the bottom of the Language window.

Step 4 In the New Name field, enter the new name for the language.

This entry is required. The name must be ISO-compliant. For example, enter **en_US** for U.S. English or enter **en** to use U.S. English as the base language.

Step 5 Click **Save** to save your change.

If you do not want to save your change, click **Cancel**.

Deleting a Language

When you delete a language, the logical folder for that language and all contents of the folder are removed from the repository. You can delete a single language or you can delete several languages at one time.

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

To delete a language or languages, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Languages**.

The Language window displays.

Step 2 Check the check box next to each language that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this language, click **Cancel**.

Managing Standard Script Prompts

Standard script prompts are used by the system-provided scripts. These prompts are stored on the Cisco IPICS server as .wav files. You cannot delete these prompts.

Managing standard script prompts involves these activities:

- Viewing a list of Standard Script Prompts, page 8-15—Displays a list of prompts and related information
- Uploading Standard Script Prompts, page 8-15—Copies prompt .wav files to the repository

Viewing a list of Standard Script Prompts

The Standard Script Prompts window displays a list of the policy engine prompts. For each prompt, this window shows the following information:

- Prompt—Name of the prompt .wav file.
- Size—Size of the prompt .wav file.
- Date Modified—Date and time that the prompt .wav file was last uploaded.
- Modified By—Cisco IPICS user ID of the user who last uploaded the prompt .wav file to the policy engine.
- Language—Name of the logical folder in which the prompt is stored. The name <default> indicates a folder that contains prompts that are available to any script, regardless of the language that is designated for the script.

To display the Standard Script Prompts window, choose **Dial Engine > Prompt Management > Standard Script Prompts** from the **Policy Engine** tab.

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**.

Tip To make sure that the Standard Script Prompts window shows the most current information, click **Refresh** at the bottom of the list of prompts.

Uploading Standard Script Prompts

Uploading a standard script prompt copies the .wav file for the prompt to the designated language folder. You must upload a prompt before it can be used in a script.

You can upload an individual standard script prompt or you can upload a .zip file that contains one or more prompts. The policy engine automatically extracts the prompt files after uploading a .zip file. Cisco IPICS supports unencrypted .zip files that use the DEFLATE compression algorithm. For example, .zip files created with WinZip, if they use legacy compression, and .zip files created with Info-Zip are compatible with Cisco IPICS.

Prompts that you upload must conform to these guidelines:

- Encoding—CCITT u-law
- Bits per sample—8
- Sample rate—8 kHz
- Channels—1 (monaural)

To upload a standard script prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Standard Script Prompts**.

The Standard Script Prompts window displays.

Step 2 Click either of these buttons at the bottom of the list of prompts:

- **Upload**—Uploads a single prompt .wav file to the repository
- **Upload Zip**—Uploads a .zip file that contains one or more prompt .wav files to the repository, then extracts the files

Step 3 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 4 From the Language drop-down list, choose the logical language folder in which to store the prompt.

Step 5 Click **Save** to save to upload the prompt.

If you do not want to upload the prompt, click **Cancel**.

Managing Customized Script Prompts

Customized script prompts are prompts that you create for use in a customized script.

The following sections provide information about managing customized script prompts. For information about creating, editing, or integrating customized script prompts, contact your system integrator.

- Viewing a List of Customized Script Prompts, page 8-17—Displays a list of prompts and related information
- Uploading Customized Script Prompts, page 8-18—Copies prompt .wav files to the repository
- Downloading a Customized Script Prompt, page 8-19—Provides the capability for you to listen to a prompt
- Renaming a Customized Script Prompt, page 8-20—Changes the name of a customized script prompt
- Deleting a Customized Script Prompt, page 8-20—Removes the prompt .wav file from the repository

Viewing a List of Customized Script Prompts

The Customized Script Prompts window displays a list of customized script prompts. For each prompt, this window shows the following information:

- Prompt—Name of the prompt .wav file
- Size—Size of the prompt .wav file
- Date Modified—Date and time that the prompt .wav file was last uploaded or moved to another destination folder or language folder
- Modified By—Cisco IPICS user ID of the user who last modified the prompt .wav file
- Language—Logical language folder in which the prompt .wav file is stored

To display the Customized Script Prompts window, choose **Dial Engine > Prompt Management > Customized Script Prompts** from the **Policy Engine** tab.

By default, the Customized Script Prompts window lists all customized script prompts. To see a list of only customized script prompts that are stored in a particular logical language folder, choose that language from the Language drop-down list and then click **Query**.

Tip To make sure that the Customized Script Prompts window shows the most current information, click **Refresh** at the bottom of the list of prompts.

Uploading Customized Script Prompts

Uploading a customized script prompt copies the .wav file for the prompt to the designated language folder. You must upload a prompt before it can be used in a script.

Custom prompts files that are uploaded must be G.711 u-law encoded. The PSTN gateways must also encode the audio to G.711 u-law for the dial-in push-to-talk (PTT) functionality.

You can upload an individual customized script prompt or you can upload a .zip file that contains one or more prompts. The policy engine automatically extracts the prompt files after uploading a .zip file. Cisco IPICS supports unencrypted .zip files that use the DEFLATE compression algorithm. For example, .zip files created with WinZip, if they use legacy compression, and .zip files created with Info-Zip are compatible with Cisco IPICS.

Prompts that you upload must conform to these guidelines:

- Encoding—CCITT u-law
- Bits per sample—8
- Sample rate—8 kHz
- Channels—1 (monaural)

To upload a customized script prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Click either of these buttons at the bottom of the list of prompts:

- **Upload**—Uploads a single prompt .wav file to the repository
- **Upload Zip**—Uploads a .zip file that contains one or more prompt .wav files to the repository, then extracts the files

Step 3 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 4 (Optional) In the Destination Folder field, enter the name of a a logical folder.

A language folder can include one or more destination folders. Destination folders are logical folders that let you group prompts under a language. For example, you may find it convenient to group prompts according to the scripts in which they are used.

A destination folder cannot have the same name as a language folder for prompts.

Step 5 From the Language drop-down list, choose the logical language folder for this prompt.

If you entered a destination folder in Step 4, the script is stored in that folder under the logical language folder that you specify.

Step 6 Click **Save** to save upload the prompt.

If you do not want to upload the prompt, click **Cancel**.

Downloading a Customized Script Prompt

Downloading a customized script prompt copies the .wav file for the prompt to a location that you specify. You can listen to the prompt by using any media player that plays .wav files.

To download a customized script prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Check the check box next to the prompt that you want to download.

Step 3 Click **Download** at the bottom of the Customized Script Prompts window.

If your browser has a default media player configured, the prompt plays automatically.

Otherwise, follow the on-screen prompts to download prompt. After you download the prompt, you can use a media player to listen to it.

Renaming a Customized Script Prompt

You can change the name of a customized script prompt, if necessary. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Check the check box next to the prompt that you want to rename.

Step 3 Click **Rename** at the bottom of the Customized Script Prompts window.

Step 4 In the New Name field, enter the new name for the prompt.

This entry is required.

Step 5 Click **Save** to save your changes.

If you do not want to save your change, click **Cancel**.

Deleting a Customized Script Prompt

When you delete a customized script prompt, it is removed from the repository. You can delete a single prompt or you can delete several prompts at one time.

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

To delete a prompt or prompts, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Check the check box next to each prompt that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this prompt, click **Cancel**.

Managing Spoken Names Prompts

The TUI uses spoken names prompts to play the names of various Cisco IPICS resources to callers. You can record spoken names prompts for channels, channel groups, locations, policies, users, user groups, ops views, VTGs, and the main TUI greeting.

Note The TUI main greeting is the spoken names prompt for the ops view with which the dial-in number that you called is associated.

Managing spoken names prompts involves these activities:

- Viewing a List of Spoken Names Prompts, page 8-22—Displays a list of prompts and related information
- Uploading Spoken Names Prompts, page 8-23—Copies prompt .wav files to the repository
- Downloading a Spoken Names Prompt, page 8-25—Provides you with the capability to listen to a prompt
- Recording a Spoken Name Prompt, page 8-26—Lets you record a prompt
- Changing Information about a Spoken Names Prompt, page 8-29—Lets you change the name, language, resource type, and associated resource of a prompt
- Deleting a Spoken Names Prompt, page 8-30—Removes the prompt .wav file from the repository

Viewing a List of Spoken Names Prompts

The Spoken Names window displays a list of spoken names prompts that have been uploaded. For each prompt, this window shows the following information:

- Resource Type—Cisco IPICS resource type for which the prompt is recorded (channel, channel group, location, ops view, policy, user, user group, ops view, or VTG)
- Associated Resource—Name of the channel, channel group, location, ops view, policy, user, user group, ops view, or VTG for which the prompt is recorded
- Language—Logical language folder in which the prompt .wav file is stored
- Prompt—Shows *resource-language*, where resource is the resource that is associated with the prompt and language is the logical language folder in which the prompt .wav file is stored
- Size—Size of the prompt .wav file
- Date Modified—Date and time that the prompt .wav file was last uploaded, moved to another language folder, or updated with another associated resource
- Modified By—Cisco IPICS user ID of the user who last modified the prompt .wav file

To display the Spoken Names window, choose **Dial Engine > Prompt Management > Spoken Names** from the **Policy Engine** tab.

To see a list of specific prompts, make the desired choices from the following drop-down list and then click **Query**:

- Language—Displays prompts from the designated logical language folder. To display prompts in all language folders, choose **All**.
- Resource Type—Displays prompts for the designated resource. To display prompts for all resources, choose **All**.
- Associated Resource—Displays prompts for the designated channel, channel group, location, ops view, policy, user, user group, ops view, or VTG. The names that appear in this list depend on the resource type that you selected. This drop-down list is dimmed if you choose **All** for the resource type.

Tip To make sure that the Spoken Names window shows the most current information, click **Refresh** at the bottom of the list of prompts.

Uploading Spoken Names Prompts

Uploading a spoken names prompt copies the .wav file for the prompt to the designated language folder. You must upload a prompt before it can be used in a script.

You can upload an individual spoken names prompt or you can upload a .zip file that contains one or more prompts. The .zip file can be up to 1 GB (1,024 MB) in size. The policy engine automatically extracts the prompt files after uploading a .zip file. Cisco IPICS supports unencrypted .zip files that use the DEFLATE compression algorithm. For example, .zip files created with WinZip, if they use legacy compression, and .zip files created with Info-Zip are compatible with Cisco IPICS.

Prompts that you upload must conform to these guidelines:

- Encoding—CCITT u-law
- Bits per sample—8
- Sample rate—8 kHz
- Channels—1 (monaural)

To upload a spoken names prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

Step 2 If you want to upload a .zip file that contains one or more prompt .wav files to the repository, click **Upload Zip**, and then go to Step 3.

If you want to upload a single .wav file, take these actions:

a. From the Resource Type drop-down list, choose the type of resource for which this prompt is to be associated (channel, channel groups location, ops view, policy, user, user group, or VTG).

b. Click **Search** and, in the Search Results window, locate and choose the resource or resources for which this prompt is to be associated.

   For information about using the Search Results window, see the "Using Search Windows" section on page 1-17.

c. From the Associated Resource drop-down list, choose a resource for which this prompt is to be associated.

   This list shows the items that you chose in the Search Results window.

Step 3 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 4 From the Language drop-down list, choose the logical language folder in which to store the prompt or prompts.

Step 5 If you are uploading a .zip file, take the following actions to associate the prompts in that file with the appropriate Cisco IPICS resources.

When you associate prompts with a resource, you make the prompts available to resources of the designated type.

a. Click **Associate**.

   The Prompt Association window displays.

b. In the Prompts Available list, click the prompt to associate with the resource.

c. In the Resources Available list, click the resource to associate with the prompt.

   If the resource that you want does not appear in the Resources Available list, from the Resources drop-down list, choose the Cisco IPICS resource type (channel, channel group, location, ops view, policy, user, user group, or VTG) that you want, click **Search** and, in the Search Results window, locate and choose the resource or resources with which to associate the prompt.

   For information about using the Search Results window, see the "Using Search Windows" section on page 1-17.

d. Click **Associate**.

The Prompt Association area displays the prompt name and its associated resource.

If you want to undo one or more associations, in the Prompt Association area, check the check box next to each prompt name to disassociate and click **Remove**.

e. Repeat Step 5 b, c, and d as needed to associate other prompts in the .zip file with resources.

f. To save associations that you made, click **Save**.

If you do not want to save the associations, click **Cancel**.

Step 6 If you are uploading a single file, click **Save** to upload the prompt.

If you do not want to upload the prompt, click **Cancel**.

Downloading a Spoken Names Prompt

Downloading a spoken names prompt copies the .wav file for the prompt to a location that you specify. You can listen to the prompt by using any media player that plays .wav files.

To download a spoken names prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

The Spoken Names window displays.

Step 2 Check the check box next to the prompt that you want to download.

Step 3 Click **Download** at the bottom of the Spoken Names window.

Step 4 Follow the on-screen prompts to download the prompt.

If your browser has a default media player configured, the prompt plays automatically.

Otherwise, follow the on-screen prompts to download prompt. After you download the prompt, you can use a media player to listen to it.

Recording a Spoken Name Prompt

You can use either of the following methods to record a spoken names prompts:

- Recording a Spoken Names Prompt by Using the Dial Engine, page 8-26
- Recording a Spoken Names Prompt by Using the Windows Sound Recorder, page 8-28

You can also record a spoken names prompt by calling the TUI and following the prompts to record the name. For more information, see the "Using the Policy Engine Telephony User Interface" section on page 6-30.

Recording a Spoken Names Prompt by Using the Dial Engine

When you record a spoken names prompt by using the dial engine, you instruct the dial engine to call you at a telephone number that you specify. When you answer the call, the TUI guides you through recording the prompt. Then the policy engine automatically uploads the prompt to the repository.

To record or rerecord a spoken names prompt by using the dial engine, perform the following procedure. If you use this procedure to rerecord an existing spoken names prompt, the system creates a new .wav file for the prompt.

Note If you want to replace the .wav file for an existing prompt with a new .wav file, perform Step 1 through Step 5 in the following procedure. Then click the link for the prompt. In the Prompt Information window, click the **Browse** button to enter, the path and file name of the file to upload; then, click **Save**.

Procedure

Step 1 Take one of these actions to display the Spoken Names window:

- In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.
- From the management window for a Cisco IPICS resource, click the **Recorded** or the **Not Recorded** link in the Prompt column.

  If you take this action, Cisco IPICS automatically populates the Resource Type, Associated Resource, and Language fields with the information that is needed to record the prompt for the resource. You can change this information as described in the next four steps, if needed. If the information is correct, go to Step 6.

Step 2 From the Resource Type drop-down list, choose the type of resource for which this prompt is to be recorded (channel, channel groups location, ops view, policy, user, user group, or VTG).

Step 3 Click **Search** and, in the Search Results window, locate and choose the resource or resources for which this prompt is to be recorded.

For information about using the Search Results window, see the "Using Search Windows" section on page 1-17.

Step 4 From the Associated Resource drop-down list, choose a resource for which this prompt is to be recorded.

This list shows the items that you chose in the Search Results window.

Step 5 If you want re-record an existing prompt, take these actions to locate existing prompts for this resource:

a. From the Language drop-down list, choose the logical language folder in which existing prompts are stored.

Choose **All** if you want to display prompts from all language folders.

Choose **Default** if you want to display prompts from the default language folder.

b. Click **Query**.

Step 6 Take one of these actions:

- To record a spoken names prompt for the first time, click **Record**.
- If you want to re-record an existing prompt, check the check box for the prompt in the list of prompts and then click **Rerecord**.

Step 7 From the Language drop-down list, choose the logical language folder in which to store the .wav file for the prompt.

Choose **default** if you want this prompt to be available to any script, regardless of the language that is designated for the script.

Step 8 In the Phone Number field, enter a telephone number where the system should call you.

You can include parentheses, spaces, and dashes in the telephone number.

The SIP provider must be able to route the call to the number that you enter.

Step 9 Click **Call**.

The dial engine calls the telephone number that you specified.

Step 10 Answer the telephone and follow the verbal prompts to log in to the TUI and record the prompt.

Recording a Spoken Names Prompt by Using the Windows Sound Recorder

You can record a spoken names prompt by using the Microsoft Windows Sound Recorder. To do so, perform the following procedure. (The procedure shown is for systems that are running the Microsoft Windows XP operating system.)

Procedure

Step 1 From the Windows Start menu, choose **Start > Programs > Accessories > Entertainment > Sound Recorder**.

The Sound Recorder dialog box displays.

Step 2 Click the **Record** button and speak the name that you want to record into the microphone.

Step 3 Click the **Stop** button when you finish recording.

Step 4 Check your recording by clicking the **Rewind** button or by dragging the slider to the beginning of the recording, and then clicking the **Play** button.

Step 5 When you are satisfied with the recording, choose **File > Save As**.

The Save As window opens.

Step 6 Click **Change** to set the recording options.

You can also set recording properties by choosing **Properties** from the Sound Recorder File menu.

The Sound Selection dialog box displays.

Step 7 From the Format drop-down menu, choose **CCITT u-Law**.

Step 8 From the Attributes drop-down menu, choose 8.000 kHz, 8 Bit, Mono 7 kb/sec.

Step 9 Click **Save As.**

The Save As dialog box displays.

Step 10 Enter a name for this format, and then click **OK**.

Step 11 In the Sound Selection dialog box, click **OK**.

Step 12 In the Save As window, save the recording file in the directory of your choice, and then click **Save**.

To use this prompt with the policy engine, you must upload it as described in the "Uploading Spoken Names Prompts" section on page 8-23.

Changing Information about a Spoken Names Prompt

You can change the name, language, resource type, and associated resource of a prompt. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

The Spoken Names window displays.

Step 2 Locate the desired prompt by making choices from the Language, Resource Type, and Associated Resource drop-down lists, and clicking **Query**.

For description of the drop-down lists, see the "Viewing a List of Spoken Names Prompts" section on page 8-22.

Step 3 Click the link in the Prompt column for the desired prompt.

Step 4 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 5 From the Language drop-down list, choose the logical language folder in which to store the prompt.

Step 6 From the Resource Type drop-down list, choose the Cisco IPICS resource type for which the prompt is recorded (channel, channel group, location, policy, user, user group, ops view, or VTG).

Step 7 From the Associated Resource drop-down list, choose the name of the channel, channel group, location, policy, user, user group, ops view, or VTG for which the prompt is recorded.

Step 8 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Deleting a Spoken Names Prompt

When you delete a spoken names prompt, it is removed from the repository. You can delete a single prompt or you can delete several prompts at one time.

To delete a spoken names prompt or prompts, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

The Spoken Names window displays.

Step 2 Check the check box next to each prompt that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this prompt, click **Cancel**.

Managing Dial Engine Scripts

The policy engine executes scripts that enable the TUI to communicate with users. Scripts provide instructions that the TUI follows to play prompts and perform other operations. A script plays prompts in the language that you designate for the 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

Cisco IPICS stores scripts in the *repository*, which is a logical storage medium in which scripts are contained and organized.

Managing dial engine scripts involves these activities:

- Viewing a List of Dial Engine Scripts, page 8-31
- Adding a Dial Engine Script, page 8-32
- Viewing or Changing Information about a Custom Dial Engine Script, page 8-33
- Deleting a Custom Dial Engine Script, page 8-34

Viewing a List of Dial Engine Scripts

The Dial Engine Script Management window displays a list of dial engine scripts. For each script, this window shows the following information:

- Name—Name of the script

- Script—File name of the script and its location in the logical file structure
- App Type—Type of application:
  - DIAL_IN—Script is invoked when a user calls the TUI
  - DIAL_OUT—Script is invoked when the system dials out to a user
- Trigger—Mechanism that invokes a script:
  - For DIAL-IN app type—Dial-in telephone number configured for this dial engine script
  - For DIAL-OUT app type—Not applicable

To display the Dial Engine Scripts window, choose **Dial Engine** > **Dial Engine Script Management** from the **Policy Engine** tab.

Adding a Dial Engine Script

When you add a dial engine script, you make it available for use by the policy engine. For additional information about adding a dial engine script, contact your system integrator.

To add a dial engine script, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Script Management**.

The Dial Engine Scripts window displays.

Step 2 Click **Add** at the bottom of the list of scripts.

Step 3 In the Dial Engine Script Name field, enter a name for this script.

This entry is required.

Step 4 In the Script field, enter a name for the script.

This entry is required.

Step 5 (Optional) Use the **Browse** button to enter, in the Destination Folder field, the path and file name of the file to upload.

Destination folders let you group or organize scripts. For example, if you have two scripts with the same name, put each one in a separate destination folder.

Step 6 From the Trigger Type drop-down list, choose one of these options:

- Dial In—Script is invoked by a call to the TUI
- Dial Out—Script is invoked by a call from the TUI

You must choose one of these options.

Step 7 For a Dial In trigger type, in the DN field, enter the telephony access string that is dialed to invoke the script.

This entry is required for a Dial In trigger type. This string must be configured on the SIP provider so that the SIP provider can route the directory number (DN) to the policy engine. This field can contain numbers and letters.

This field does not display if the trigger type is Dial Out.

Step 8 From the Language drop-down list, choose the logical language folder that contains the prompts to be played by this script.

This entry is required.

Step 9 To add the script, click **Add**.

If you do not want to add this script, click **Cancel**.

Viewing or Changing Information about a Custom Dial Engine Script

You can view or modify information for any custom dial engine script. You cannot view or modify information for any of the five system scripts that are listed in the "Managing Dial Engine Scripts" section on page 8-31.

To view or modify information about a custom dial engine script, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Script Management**.

The Dial Engine Scripts window displays.

Step 2 Click the link in the Name column for the custom script.

System scripts do not have a link.

Step 3 View or update the following information as needed:

- Dial Engine Script Name—Name assigned to this script
- Current Script (*display only*)—Script that is currently used for the DN
- Script—Script file that executes
- Destination Folder— Logical folder under the language folder in which the script is stored
- Trigger Type—Either of these options:
  - Dial In—Script is invoked by a call to the TUI
  - Dial Out—Script is invoked by a call from the TUI
- Language— Logical language folder in which the script is stored

Step 4 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Deleting a Custom Dial Engine Script

When you delete a dial engine script, it is removed from the repository. You can delete any custom script, but you cannot delete the system scripts that are listed in the "Managing Dial Engine Scripts" section on page 8-31.

You can delete a single script or you can delete several scripts at one time.

To delete a custom script or scripts, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Script Management**.

The Dial Engine Scripts window displays.

Step 2 Check the check box next to each custom script that you want to delete.

These check boxes are dimmed for the system scripts.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this script, click **Cancel**.

Configuring SIP

The SIP configuration process provides the policy engine with the following parameters:

- Parameters required to work with the SIP provider.
- Parameters required to use the IP Phone Text Notification action in a policy
- Parameters required to use the Dial notification action in a policy to send a message to a Cisco Unified IP Phone

For related information, see the "Configuring the SIP Provider" section on page 8-43.

To configure SIP for the policy engine, perform the following steps.

Note After you configure SIP, verify that the Dial Engine and SIP subsystem are IN_SERVICE. For more information, see the "Obtaining Information about Dial Engine Services" section on page 8-2.

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > SIP Configuration**.

The SIP Configuration window displays.

Step 2 In the SIP Subsystems Configuration pane, take these actions to enter required information:

- In the Port field, enter the SIP port that the policy engine uses.

  This entry is required. The default value is 5060.
- In the User Agent field, enter the user agent that the policy engine uses.

  This entry is required. The default value is Cisco-IPPE/2.0.

- In the Maximum Retransmissions field, enter the maximum number of times that SIP requests and responses are transmitted.

  This entry is required. The default value is 2. Valid values are 0 through 10.

- In the First Retransmission field, enter the number of milliseconds to wait before performing the first retransmission.

  This entry is required. 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.

Step 3 In the SIP Provider Configuration pane, take these actions:

- In the Host field, enter the IP address or the host name of the SIP provider. This entry is required.
- In the Port field, enter the port number that the SIP provider uses for SIP. This entry is required.
- From the Transport drop-down list, choose the transport protocol (TCP or UDP) that matches the transport protocol of the SIP provider.

  If both protocols are configured on the SIP provider, choose either protocol.

- In the Username field, enter the appropriate information. This information is required.
  - 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.
- In the Password field, enter the appropriate information. This information is required.
  - 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.

Step 4 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Step 5 Your changes take effect only after you restart the dial engine. To restart the dial engine, follow these steps:

a. Log in to the Cisco IPICS server as the root user.

b. Enter the following command at the command prompt:

```
[root]# service ipics restart
```

Managing Cisco Unified Communications Manager for IP Phone Notifications

If you configure policies to use the IP Phone Text Notification action or to use the Dial Notification action to send a message to a Cisco Unified IP Phone, you must configure at least one Cisco Unified Communications Manager under IP Phone Notification Configuration for these policies to execute.

When you configure a Cisco Unified Communications Manager for IP phone notification, you provide information about a Cisco Unified Communications Manager in which end users contain information about IP phones that Cisco IPICS should contact. You can provide information for up to three Cisco Unified Communications Managers. Then, when a policy that includes a IP Phone Text Notification action or to use the Dial Notification executes, Cisco IPICS contacts each of the configured Cisco Unified Communications Managers and provides all configured IP phone numbers to each one. When a provided phone number matches a phone number on a Cisco Unified Communications Manager, it returns the MAC address of the corresponding IP phone to Cisco IPICS, and Cisco IPICS contacts the phone at that MAC address.

Managing IP phone notification involves these activities:

- Viewing a List of Cisco Unified Communications Managers for IP Phone Notifications, page 8-38
- Adding a Cisco Unified Communications Manager for IP Phone Notification, page 8-38

- Viewing or Changing Information about a Cisco Unified Communications Manager Configured for IP Phone Notification, page 8-40
- Deleting a Cisco Unified Communications Manager for IP Phone Notification, page 8-41

Viewing a List of Cisco Unified Communications Managers for IP Phone Notifications

The IP Phone Notification Configuration window displays a list of Cisco Unified Communications Managers configured for IP phone notifications. For each notification, this window shows the following information:

- Name—A system-provided identifier for the notification. The name includes the designation CUCM (for Cisco Unified Communications Manager) and the IP address of the Cisco Unified Communications Manager server that the IP phone notification is configured for.
- Version—Cisco Unified Communications Manager version that is running on the configured server.
- Host Name or IP Address—Host name or IP address of the Cisco Unified Communications Manager.

To display the IP Phone Notification Configuration window, choose **Dial Engine > IP Phone Notification Configuration** from the **Policy Engine** tab.

Adding a Cisco Unified Communications Manager for IP Phone Notification

When you add a Cisco Unified Communications Manager for IP phone notification, you make it available for use by policies that include the IP Phone Text Notification action or the Dial notification action to send a message to a Cisco Unified IP Phone.

To add a Cisco Unified Communications Manager for IP phone notification, perform the following procedure.

Note For information about Cisco Unified Communications Manager Application Users and end users, see your Cisco Unified Communications Manager documentation.

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > IP Phone Notification Configuration**.

The IP Phone Notification Configuration window displays.

Step 2 Click **Add** at the bottom of the list of notifications.

Step 3 From the Version drop-down list, choose the version of Cisco Unified Communications Manager that is running on the server that Cisco IPICS should contact for this notification.

This entry is required.

Step 4 In the Host Name or IP Address field, enter the host name or the IP address of the Cisco Unified Communications Manager server.

This entry is required.

Step 5 In the Administrator User Name field, enter the name of the Application User in Cisco Unified Communications Manager who has administrator privileges.

This entry is required.

Step 6 In the Administrator Password field, enter the password of the Application User in Cisco Unified Communications Manager who has administrator privileges

This entry is required.

Step 7 In the End User Name field, enter the name of the end user in Cisco Unified Communications Manager to which IP Phones are associated.

This entry is required.

Step 8 In the End User Password field, enter the password of the end user in Cisco Unified Communications Manager to which IP Phones are associated.

This entry is required.

Step 9 To add the notification, click **Save**.

If you do not want to add this notification, click **Cancel**.

Viewing or Changing Information about a Cisco Unified Communications Manager Configured for IP Phone Notification

You can view or modify information about any Cisco Unified Communications Manager configured for IP phone notification. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > IP Phone Notification Configuration**.

The IP Phone Notification Configuration window displays.

Step 2 Click the link in the Name column of the Cisco Unified Communications Manager for IP phone notification.

Step 3 View or update the following information as needed:

- Version—Version of Cisco Unified Communications Manager that is running on the server that Cisco IPICS should contact for this notification
- Host Name or IP Address field—Host name or the IP address of the Cisco Unified Communications Manager server
- Administrator User Name—Name of the Application User in Cisco Unified Communications Manager who has administrator privileges.
- Administrator Password—Password of the Application User in Cisco Unified Communications Manager who has administrator privileges
- End User Name—Name of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated.
- End User Password—Password of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated.

Step 4 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Deleting a Cisco Unified Communications Manager for IP Phone Notification

To delete a Cisco Unified Communications Manager configured for IP phone notification perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > IP Phone Notification Configuration**.

The IP Phone Notification Configuration window displays.

Step 2 Check the check box next to the Cisco Unified Communications Manager name that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this Cisco Unified Communications Manager configured for IP phone notification, click **Cancel**.

Configuring Dial Engine Parameters

The dial engine parameters configuration process provides system settings for the dial engine.

To configure dial engine parameters, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Dial Engine Parameters**.

The Dial Engine Parameters window appears.

Step 2 In the SMTP Server field, enter the IP address or the host name of the SMTP server that is used by the dial engine.

Leave this field blank if there is no SMTP server configured for the dial engine.

Step 3 In the Sender Email Address field, enter the e-mail address that appears as the "From" address when the policy engine sends e-mail notifications to users.

If you specify a sender e-mail address when configuring an ops view, that value overrides the value in this field.

Step 4 In the Outbound Dial Number field, enter the telephone number that appears as the caller ID number when the policy engine calls a user.

This entry is required. The number must not be the same as a dial-in number that is used to call the policy engine.

If this number is not configured, the policy engine is not able to dial out.

Note If the policy engine call goes through more than one voice gateway, the caller ID of the last gateway appears as the caller ID, regardless of the value that is configured in the Outbound Dial Number field.

Step 5 From the Default Language drop-down list, choose the logical language folder that the TUI uses at run time.

Step 6 In the Default Session Timeout field, enter the number of seconds that a call session is kept in memory after the call completes.

This entry is required. The default value is 500.

Note You should change the Default Session Timeout value only if you are instructed to do so by the Cisco TAC.

The Dial Engine Parameters window displays the codec that the policy engine uses. This codec is G.711 u-law and cannot be changed.

Step 7 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Configuring the SIP Provider

The policy engine requires that a SIP provider be configured in your network if you use the dial-in or dial-out features. A SIP provider handles calls to and from the policy engine.

You must use Cisco Unified Communications Manager or a Cisco Unified Communications Manager Express as the SIP provider, enter any value in this field as the SIP provider. To do so, configure the application as described in the following sections.

These sections assume that Cisco Unified Communications Manager or a supported router with Cisco IOS software is installed and running in your network.

- Configuring Cisco Unified Communications Manager as the SIP Provider, page 8-43
- Configuring a Cisco Unified Communications Manager Express as the SIP Provider, page 8-48

Configuring Cisco Unified Communications Manager as the SIP Provider

Assuming that Cisco Unified Communications Manager is configured and running in your network, this section describes additional configuration that is required for Cisco Unified Communications Manager to function as the SIP provider for the policy engine.

Before you configure Cisco Unified Communications Manager for the policy engine, you must provide SIP configuration information as described in the "Configuring SIP" section on page 8-35.

When you perform the procedure in this section, you must provide the information that is listed Table 8-2. You may find it convenient to gather this information before you start the procedure.

Table 8-2 Information Required for Cisco Unified Communications Manager Configuration

Information	Your Value
User ID that you entered when you configured SIP as described in the "Configuring SIP" section on page 8-35	
Password that you entered when you configured SIP as described in the "Configuring SIP" section on page 8-35	
Incoming port, if other than the default 5060	
Partitions, if configured for Cisco Unified IP Phones	
Calling search spaces, if configured for Cisco Unified IP Phones	
IP address of the Cisco IPICS server	
DNs for ops views and custom dial engine scripts	
User name that you entered when you configured the RMS (required only if you are using the direct dial feature)	
Password that you entered when you configured the RMS (required only if you are using the direct dial feature)	

To configure Cisco Unified Communications Manager for the policy engine, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, take the following actions to configure an Application User for the policy engine.

This Application User requires digest credentials and will be used by the policy engine to authenticate calls that it makes to Cisco Unified Communications Manager.

a. Choose **User Management > Application User**.

b. Click **Add New**.

c. In the Application User Configuration Page, enter the following information:

- User ID—Enter the same user ID that you entered when you configured SIP.
- Password and Confirm Password—Enter a password that the user will use to log in to Cisco Unified Communications Manager.
- Digest Credentials and Confirm Digest Credentials—Enter the password that you entered when you configured SIP.
- Update other fields as needed for your deployment or accept the default values.

d. Click **Save**.

Step 2 In Cisco Unified Communications Manager Administration, take the following actions to define a SIP trunk security profile with digest authentication enabled.

The default SIP trunk does not provide security. This new profile enables digest authentication for calls from the policy engine to Cisco Unified Communications Manager.

a. Choose **System > Security Profile > SIP Trunk Security Profile**.

b. Click **Add New**.

c. In the Name field, enter **Digest Authenticated SIP Trunk Profile**.

d. In the Description field, enter **Digest Authenticated SIP Trunk Profile**.

e. From the Device Security Mode drop-down list, choose **Non Secure**.

f. From the Incoming Transport drop-down list, choose **TCP+UDP**.

g. From the Outgoing Transport drop-down list, choose **TCP**.

h. Check the **Enable Digest Authentication** check box.

i. In the Nonce Validity Time field, enter **5**.

j. In the **Incoming Port** field, enter the default value of 5060 or enter another value if appropriate for your deployment.

k. Click **Save**.

Step 3 In Cisco Unified Communications Manager Administration, take the following actions to create a SIP trunk for the policy engine.

The SIP trunk is used to exchange dial-in and dial-out calls between Cisco Unified Communications Manager and the policy engine.

a. Choose **Device > Trunk**.

b. Click **Add New**.

c. From the Trunk Type drop-down list, choose **SIP Trunk**.

d. From the Device Protocol drop-down list, choose **SIP**.

e. Click **Next**.

f. Enter information that is appropriate for your Cisco Unified Communications Manager deployment, making sure to follow these guidelines:

- If you configured partitions and calling search spaces for your Cisco Unified IP Phones, enter the same calling search spaces for the policy engine.
- In the Destination Address field, enter the IP address of the Cisco IPICS server.
- In the SIP Trunk Security Profile field, enter the name of the profile that you created in Step 2.

g. Click **Save**.

Step 4 In Cisco Unified Communications Manager Administration, take the following actions to create a route pattern for the new SIP trunk.

The route pattern that is associated with the SIP trunk instructs Cisco Unified Communications Manager which calls to send to the policy engine.

a. Choose **Call Routing > Route/Hunt > Route Pattern**.

b. Click **Add New**.

c. Enter information that is appropriate for your Cisco Unified Communications Manager deployment.

   In the Route Pattern field, make sure to include in the route pattern all DNs that you want to be routed to the policy engine (DNs for ops views and custom dial engine scripts).

d. From the Gateway/Route List drop-down list, choose the SIP trunk that you created in Step 3.

e. Click **Save**.

Step 5 (Optional—Required only if you are using the direct dial feature.) In Cisco Unified Communications Manager Administration, take the following actions to configure an Application User for the RMS:

a. Choose **User Management > Application User**.

b. Click **Add New**.

c. In the Application User Configuration page, enter the following information:

   - User ID—Enter the same user ID that you entered when you configured the RMS.
   - Password and Confirm Password—Enter the same password that you entered when you configured the RMS
   - Other fields—Enter information as appropriate for your deployment.

d. Click **Save**.

Step 6 (Optional—Required only if you are using the direct dial feature.) In Cisco Unified Communications Manager Administration, take the following actions to create a SIP trunk for the RMS:

a. Choose user **Device > Trunk**.

b. Click **Add New**.

c. From the Trunk Type drop-down list, choose **SIP Trunk**.

d. From the Device Protocol drop-down list, choose **SIP**.

e. Click **Next**.

f. Enter information that is appropriate for your Cisco Unified Communications Manager deployment, making sure to follow these guidelines:
   - If you configured partitions and calling search spaces for Cisco Unified IP Phones, enter those calling search spaces.
   - In the Destination Address field, enter the IP address of the RMS.
   - In the SIP Trunk Security Profile field, enter the name of the profile that you created in Step 2.

g. Click **Save**.

Configuring a Cisco Unified Communications Manager Express as the SIP Provider

Assuming that Cisco Unified Communications Manager Express is running a supported version of Cisco IOS is configured and running in your network, this section describes additional configuration required for configuring the router as the SIP provider for direct dial calls from an IDC.

Note Although Cisco IOS supports values other than those shown for some of the fields in this configuration, Cisco recommends that you configure the values that are shown to ensure consistency.

Procedure

Step 1 Enter the following command to start configuration mode:

```
Router# configure terminal
```

Step 2 Enter the following commands to allow SIP to SIP connections.

If no other SIP devices are configured, skip this step.

```
Router(config)# voice service voip
Router(con-voi-serv)# allow-connections sip to sip
Router(con-voi-serv)# exit
```

Step 3 Enter the following commands to define a voice class codec that uses the G.711 u-law codec.

```
Router(config)# voice class codec 2
Router(config-class)# codec preference 1 g711ulaw
Router(config-class)# exit
```

Step 4 Enter the following commands to define a dial-peer for each route pattern that you allocated for ops views.

Route patterns must span the DNs that are associated with each ops view and custom script. For example, if your system has ops views with the DNs 8100–8199 and 9200–9299, you could define two route patterns, 81*nn* and 92*nn*, where *n* is any digit. You would then define one dial peer for each route pattern.

```
Router(config)# dial-peer voice 554 voip
Router(config-dial-peer)# destination-pattern route-pattern
Router(config-dial-peer)# voice-class codec 2
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# session target ipv4:ip-address
```

(replace *ip-address* with the IP address of the Cisco IPICS server)

```
Router(config-dial-peer)# session transport transport-protocol
```

(replace *transport-protocol* with UDP or TCP, depending on which value is configured for SIP as described in the "Configuring SIP" section on page 8-35)

```
Router(config-dial-peer)# dtmf-relay rtp-nte
Router(config-dial-peer)# exit
```

Step 5 (Optional—Skip this step if the SIP provider and RMS are configured on the same router.) Enter the following commands to configure the incoming voice dial peer to turn off voice activity detection (VAD) and use RFC 2833 for DTMF for calls from Cisco IPICS):

```
Router(config)# dial-peer voice 555 voip
Router(config-dial-peer)# voice-class codec 2
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# incoming called number .
Router(config-dial-peer)# no vad
Router(config-dial-peer)# dtmf-relay rtp-nte
```

Step 6 To exit, enter this command:

```
Router(config)# end
```