CHAPTER 6

Using the Cisco IPICS Policy Engine

The Cisco IPICS policy engine provides you with the ability to create and manage policies. A policy comprises one or more actions, which are discrete functions that perform when the policy executes. For example, you could create a policy that starts a VTG and invites designated users to join the VTG. Some policies can also include one or more triggers, which cause the policy to execute automatically and, optionally, to repeat according to a specified scheduled.

To enable the policy engine, you must install a Cisco IPICS license that includes a license for the policy engine and then restart the Cisco IPICS server. For more information about licenses, see the "Managing Licenses" section on page 2-76.

You perform the policy engine activities that are described in this chapter from the Policy Management 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 1-11, then choose the **Policy Management** drawer in the Policy Engine tab. Any Cisco IPICS user can access this drawer, but some activities that are available from this drawer require that you be assigned certain Cisco IPICS roles, as explained in the "Policy Activities Available for Cisco IPICS Roles" section on page 6-2.

Before you can perform many of the activities that are described in this chapter, you must configure the policy engine. For details, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

This chapter includes the following topics:

Policy Engine Overview

The policy engine enables the creation of policies, which specify actions that the system executes according to instructions that you provide. You can create an invitation policy that causes the telephony user interface (TUI) to call designated users and invite them to join a VTG or channel. You can also create a Multi-Purpose policy that activates designated VTGs, adds participants to a VTG, and contacts designated recipients according to notification instructions that you specify.

You can configure triggers to activate a Multi-Purpose policy according to a schedule that you specify. A trigger can be configured to activate a policy one time at a designated start date and time, or it can be configured to execute the policy repeatedly according to a designated schedule.

The policy engine includes the dial engine, which enables the TUI and its associated features. The TUI lets you use a touch-tone telephone to receive information from and provide instructions to the policy engine.

Calls arrive at the Cisco IPICS dial engine as SIP calls from the configured SIP provider and establish a unicast media connection to the Cisco IPICS server. When a caller joins a channel or VTG, the Cisco IPICS server configures a T1 resource on the RMS to allow for a multicast connection from the server to a dynamically allocated loopback. The loopback facilitates a multicast connection between the Cisco IPICS server and the selected channel or VTG on the RMS. This connection is made one time per channel or VTG, regardless of how many dial in users select the channel or VTG. When the last dial in user that is connected to that channel or VTG drops, the resource is released in the RMS.

The dynamically allocated loopback uses a multicast address from the multicast address pool. The Cisco IPICS server sends the audio that it receives from the connected call to this address. In addition, the Cisco IPICS server listens for multicast media on the multicast address for the selected channel and sends that media to the connected call.

Policy Activities Available for Cisco IPICS Roles

Table 6-1 lists the Cisco IPICS roles that are required to perform various policy engine activities.

Table 6-1 Roles Required for Policy Activities

Role	Activate Policy	Add Policy	Modify Policy	Delete Policy	View Policies	View Users	View VTGs and Channels
User	Yes	No	No	No	Associated with this user	—	—
System Administrator	Yes	No	No	No	Created by users who belong to the ops view of this system administrator[1]	All users	All VTGs and channels
Operator	Yes	Yes	Yes	Yes	Created by users who belong to the ops view of this operator[1]	Created by users who belong to or are accessible to the ops view of this operator	Created by users who belong to or are accessible to the ops view of this operator

Table 6-1 Roles Required for Policy Activities (continued)

Role	Activate Policy	Add Policy	Modify Policy	Delete Policy	View Policies	View Users	View VTGs and Channels
Dispatcher	Yes	Yes	Yes	Yes	Created by users who belong to the ops view of this dispatcher[1]	Created by users who belong to or are accessible to the ops view of this dispatcher	Created by users who belong to or are accessible to the ops view of this dispatcher
Ops View Administrator	Yes	No	No	No	Created by users who belong to the ops view of this ops view administrator[1]	Created by users who belong to or are accessible the ops view of this ops view administrator	Created by users who belong to or are accessible the ops view of this ops view administrator
All	Yes	Yes	Yes	Yes	Created by users who belong to the ops view of this user[1]	All users	All VTGs and channels

1. If this user belongs to the system ops view, this user can view all policies.

Understanding the Policies Window

The Policies window lists information about each of the policies that you have configured in Cisco IPICS. It also provides you with the capability to perform several policy management functions.

To display the Policies window, access the Policy Management drawer and click **Policies**.

Table 6-2 describes the items in the Policies window.

Table 6-2 Items in the Policies Window

Item	Description	Reference
Name field	Unique name that is assigned to the policy	See the "Adding a Policy" section on page 6-4
Type field	Type of the policy	See the "Adding a Policy" section on page 6-4
Action Names field	Actions that are associated with the policy	See the "Managing Actions for a Policy" section on page 6-5
Trigger Names field	Triggers that are associated with the policy	See the "Managing Triggers for a Policy" section on page 6-12
Ops View field	Displays the ops view to which the policy belongs	A policy is automatically assigned the ops view of the user who created the policy (for related information, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views")
Prompt field	Indicates whether a spoken name prompt is recorded for the policy	See the "Managing Prompts for a User" section on page 3-25
Add button	Provides the ability to add a new policy	See the "Adding a Policy" section on page 6-4
Delete button	Provides the ability to delete a policy	See the "Deleting a Policy" section on page 6-16

Table 6-2 Items in the Policies Window (continued)

Item	Description	Reference
Activate button	Provides the ability to activate a policy	See the "Activating a Policy Manually" section on page 6-16
Associations button	Provides the ability to associate users with a policy	See the "Associating Users with a Policy" section on page 6-15

Only the operator, dispatcher, or all role users who belong to a certain ops view should add, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are associated with that ops view. This situation can cause inconsistencies when users view policies. Operators or dispatchers who belong to the SYSTEM ops view should add, edit, or delete policies for that ops view only.

Adding a Policy

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

- Invitation—Policy activated only through the TUI that causes the TUI to call designated users and invite them to join a VTG or channel. You can invoke an invitation policy from the TUI breakout menu after you have joined a VTG or a channel. Users that the TUI calls are invited to join that VTG.
- Multi-Purpose—Policy that performs any one of the following activities:
  - Activates designated VTGs
  - Adds participants to a VTG
  - Executes a notification action. For more information, see the "Understanding Notification Actions" section on page 6-6.
  - Provides the specified message to designated users by causing the TUI to call them according to the dial preferences that are configured as described in the "Managing Communications Preferences for a User" section on page 3-13

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 that you define may over-commit system resources when it activates VTGs.

To add a policy, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

The Policy Management window displays.

Step 2 In the Policies area, click **Add**.

The New Policy window displays.

Step 3 In the **General** tab, take these actions:

a. In the Policy Name field, enter a unique name for the policy.

You might find it useful to name policies according to function, such as "Notify Emergency Team."

b. In the Policy Description field, enter a description for this policy.

c. From the Policy Type drop-down list, choose one of these types:

- Multi-Purpose—Creates a policy that activates designated VTGs, executes a notification action, adds participants to a VTG, or dials designated users based on dial preferences
- Invitation—Creates a policy that invites designated users to join a designated VTG or a channel

d. Click **Save**.

Step 4 Perform the tasks that are described in Table 6-3, as needed.

You do not need to perform these tasks now. You can enter or update this information later.

Table 6-3 Tasks for Adding a Policy

Task	Reference
Enter one or more actions for the policy.	See the "Managing Actions for a Policy" section on page 6-5.
Designate the users who can activate or deactivate this policy.	See the Associating Users with a Policy, page 6-15.

Managing Actions for a Policy

An action specifies the activity that a policy performs when it executes. The actions available for a policy depend on the policy type. Actions include the activities that are described in Table 6-4.

Table 6-4 Policy Actions

Action	Associated Policy Type	Description
Invite to VTG	Invitation	Calls designated users and invites them to join a VTG by responding to TUI prompts. This policy can be activated only through the TUI when you break out of an existing VTG. In this case, this action calls users according to their dial preferences and invites them to join the VTG from which you broke out.
Activate VTG	Multi-Purpose	Activates the designated preconfigured VTGs.
Notification	Multi-Purpose	Contacts designated recipients according to notification instructions that you specify. For more detailed information, see the "Understanding Notification Actions" section on page 6-6.

Table 6-4 Policy Actions (continued)

Action	Associated Policy Type	Description
VTG Add Participants	Multi-Purpose	Adds the designated participants to the designated VTG.
Dial Out	Multi-Purpose	Calls the designated users according to their configured dial preferences to invite them to join the designated VTG.

A policy can have an unlimited number of actions. If a policy includes more than one action, the policy engine executes the actions in the order that they are listed in the Policies window.

You can add, update, or delete actions for any policy. The procedure that you perform to add or update an action depends on the type of policy.

Managing actions for a policy involves these activities:

- Understanding Notification Actions, page 6-6
- Adding or Updating an Action for a Multi-Purpose Type Policy, page 6-8
- Adding or Updating an Action for an Invitation Type Policy, page 6-11
- Deleting an Action, page 6-12

Understanding Notification Actions

Notification actions cause Cisco IPICS to contact designated recipients and provide them with information that you specify. The policy engine notification actions that are described in this chapter can notify only recipients that are configured in Cisco IPICS.

This section describes the Email, IP Phone Text, Dial, Talk Group, Dial Engine Script, and Alert notification actions. For information about configuring these action types, see the "Adding or Updating an Action for a Multi-Purpose Type Policy" section on page 6-8.

A policy can notify any Cisco IPICS user. For information about the number of recipients that are supported for various notification actions, see *Cisco IPICS Compatibility Matrix*.

Email Notification Action

An Email notification action sends a message to the e-mail, SMS, and pager addresses that are configured as notification preferences for each user that you designate as a recipient. The policy engine can send a message that contains up to 1,000 characters. It truncates longer messages to 1,000 characters.

IP Phone Text Notification Action

An IP Phone Text notification action displays a designated message on supported Cisco Unified IP Phone models. The telephone numbers of each phone must be configured as a dial preference for the associated user.

This type of notification action requires that you configure parameters in the Cisco Unified Communications Manager Configuration for IP Phone Notifications area in the SIP Configuration menu. For instructions, see the "Configuring SIP" section on page 8-24.

Dial Notification Action

The policy engine executes a Dial notification action as follows:

- If the IP Phone Notifications parameters are configured in the IP Phone Notification Configuration window, the system checks whether each designated user has an associated Cisco Unified IP Phone configured in Cisco Unified Communications Manager. If a user does have an associated phone, the system plays the designated message on the speaker of the phone.
- If IP Phone Notifications parameters are configured but a user does not have an associated Cisco Unified IP Phone, or if the phone of a user is busy, the system calls the user as specified in the dial preferences and plays the designated message.
- If IP Phone Notifications parameters are not configured, the system calls the user as specified in the dial preferences and plays the designated message.

For information about configuring IP Phone Notifications parameters, see the "Managing Cisco Unified Communications Manager for IP Phone Notifications" section on page 8-25.

When you create a Dial notification action, you can specify a pre-recorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

If you use this action to contact Cisco Unified IP Phones, make sure that at least one multicast address is available in the multicast pool. For more detailed information, see the "Managing the Multicast Pool" section on page 2-31.

Talk Group Notification Action

A Talk Group notification action plays the selected prompt to all participants in the selected VTG.

When you create a Talk Group notification action, you can specify a pre-recorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

Note

- When a Talk Group notification executes, the designated message is added to the multicast stream of the VTG. To inform users that a system message is being played, consider starting the message with a statement such as, "This is the Cisco IPICS administrator with an important recorded message."
- A VTG participant who is dialed in through the TUI and who has the floor does not hear the talk group notification message.

Dial Engine Script Notification

A Dial Engine Script notification action executes the designated dial engine script once for each designated recipient.

Alert Notification Action

An alert notification action sends an alert message to the IDC of each user who is associated with the policy and show has executed the policy from the IDC. The alert message appears in a pop-up window on the IDC.

Adding or Updating an Action for a Multi-Purpose Type Policy

A Multi-Purpose type policy can activate a VTG, send notification messages to recipients, add participants to a VTG, or call users and invite them to a VTG.

To add or update actions for a Multi-Purpose type policy, perform the following procedure. If you update an action for a policy that is executing, that change takes affect after the policy execution completes.

Note After you save a notification action, you cannot change the type of that action. Instead, you must delete the action and then add a new one.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy for which you want to add an action.

Step 3 Click the **Action** tab.

The Policies > *Policy Name* window displays a list of actions that have been created for this policy. The Action Type column displays the type of action and the Action Name column displays the name that was assigned to the corresponding action when it was created.

Step 4 Take either of these actions:

- To add a new action, choose one of these options from the **Add Action** drop-down list:
  - Activate VTG—Activates the designated VTGs
  - Notification—Sends the designated message to the designated recipients
  - VTG Add Participants—Adds designated participants to the designated VTG
  - Dial Out—Calls designated users to invite them to the designated VTG
- To view or update an existing action, click the link for the action in the Action Type column.

The New Action window displays. The areas and fields in this window vary depending on the action type that you choose.

Step 5 In the Action Name field, enter a name for this action.

If a policy includes more than one action, each action name must be unique.

Step 6 Follow the steps in Table 6-5 to enter additional information for the action type that you chose.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy

Step	Notes
Action Type: Activate VTG	
1. In the Duration fields, enter the number of days, hours, or minutes that a VTG remains active after it is activated by the policy.	If you do not enter a value in this field, the VTG will remain active until it is deactivated manually.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
2. Specify the VTGs that this action activates when the policy executes: • Choose **VTG** from the View drop-down list. • Click **Search** and, in the Search window, locate and choose the VTGs that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-12. If you want to remove any VTG from the list, click the check box next to the VTG in the Select VTGs area, click **Delete**, and then click **OK** in the confirmation dialog box that appears.
3. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.
Action Type: Notification	
1. From the Type drop-down list, choose the type of notification message.	Notification types are Email, IP Phone Text, Dial, Talk Group, Dial Engine Script, and Alert. For detailed information about these notification types, see the "Understanding Notification Actions" section on page 6-6.
2. Take one of these actions: • If you chose **Email** from the Type drop-down list, take these actions: – In the Subject field, enter a descriptive subject for the message. – In the Message area, enter the message to be sent to the e-mail, SMS, and pager addresses that are configured as notification preferences for the user. • If you chose **IP Phone Text** from the Type drop-down list, in the Message area, enter the text to display on the phone. • If you chose **Dial** from the Type drop-down list, from the Prompt drop-down list, choose the prompt to play. You can also choose to record a prompt by clicking **Record New Message Notification**. • If you chose **Talk Group** from the type Type drop-down list, from the Prompt drop-down list, choose the prompt to play. You can also choose to record a prompt by clicking **Record New Message Notification**. • If you chose **Dial Engine Script** from the Type drop-down list, from the Dial Engine Script drop-down list, choose the desired script. • If you chose **Alert** from the Type drop-down list, enter text for the alert message in the Message field.	When you click **Record New Message Notification** for a Dial or Talk Group action, you can record a prompt that you can then choose from the Prompt drop-down list. After clicking **Record a New Prompt**, follow these steps: **1.** 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. **2.** In the Phone Number field, enter a telephone number where the system should call you. Enter only numbers in this field. The SIP provider must be able to route the call to the number that you enter. **3.** In the Name field, enter a name for the .wav file of this prompt, including the extension .wav. **4.** (Optional) In the Destination Folder field, enter the name of the logical folder in which the prompt will be stored. **5.** Click **Call**. The dial engine calls the telephone number that you specified. **6.** Answer the telephone and follow the verbal prompts to log in to the TUI and record the prompt. **7.** In the Call Completed dialog box, click **OK**.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
3. From the View drop-down list, choose the type of recipient to receive the notification.	View types include the following: • User—Users with any role that are configured in Cisco IPICS. • User Group—User groups that are configured in Cisco IPICS. • VTG—VTGs that are configured in Cisco IPICS. When you designate a VTG, the notification is sent to all participants in that VTG.
4. Click **Search** and, in the Search window, locate and choose the recipients that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-12. If you want to remove any recipient from the list, click the check box next to the recipient in the Recipients area, click **Delete;** then, click **OK** in the confirmation dialog box that appears. If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.
5. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.
Action Type: VTG Add Participants	
1. From the VTG drop-down list, select the VTG to which participants will be added when this policy executes.	VTGs that you see depend on the ops views configuration. For more information, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views.")
2. From the View drop-down list, choose the type of participant to be added to the VTG.	View types include the following: • User—Users with any role that are configured in Cisco IPICS. • User Group—User groups that are configured in Cisco IPICS. • VTG—VTGs that are configured in Cisco IPICS.
4. Click **Search** and, in the Search window, locate and choose the participants that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-12. If you want to remove any participant from the list, check the check box next to the participant in the Participants area, click **Delete**; then, click **OK** in the confirmation dialog box that appears. If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
5. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.
Action Type: Dial Out	
1. From the VTG drop-down list, choose the VTG to which the user who is called will be added.	This list shows only those VTGs that you are associated with.
2. From the View drop-down list, choose the type of recipient to be called and invited to join the VTG.	View types include the following: • User—Users with any role that are configured in Cisco IPICS. • User Group—User groups that are configured in Cisco IPICS.
3. Click **Search** and, in the Search window, locate and choose the recipient that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-12. If you want to remove any recipient from the list, check the check box next to the recipient in the Recipients area, click **Delete**; then, click **OK** in the confirmation dialog box that appears. If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.
4. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.

Adding or Updating an Action for an Invitation Type Policy

An invitation type policy calls designated users and invites them to join a VTG.

To add or update actions for an invitation type policy, perform the following procedure. If you update an action for a policy that is executing, that change takes affect after the policy execution completes.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy for which you want to add an action.

Step 3 Click the **Action** tab.

The Policies > *Policy Name* window displays a list of actions that have been created for this policy. The Action Type column displays the type of action and the Action Name column displays the name that was assigned to the corresponding action when it was created.

Step 4 Take either of these actions:

- To add a new action for the policy, choose **Invite To VTG** from the action type from the **Add Action** drop-down list.
- To view or update an existing action, click the link for the action in the Action Type column.

Step 5 In the Action Name field, enter a name for this action.

If a policy includes more than one action, each action name must be unique.

Step 6 Click **Search** and, in the Search window, locate and choose the users to be invited to the VTG.

For information about using the Search window, see the "Using Search Windows" section on page 1-12.

If you want to remove any recipient from the list, check the check box next to the recipient in the Recipients area, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.

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

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

Deleting an Action

You can delete a single action from a policy or you can delete several actions at one time. If you delete an action while its associated policy is executing, the action is removed after the execution completes.

To delete an action or actions, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy that includes the action that you want to delete.

Step 3 Click the **Action** tab.

Step 4 Check the check box next to each action that you want to delete.

Step 5 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 6 To confirm the deletion, click **OK**.

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

Managing Triggers for a Policy

A trigger is a mechanism that activates a Multi-Purpose type policy according to a schedule that you specify. Triggers do not apply to invitation policy types, which can be activated only through the TUI. A Multi-Purpose type policy can have an unlimited number of triggers.

A trigger can be configured to activate a policy one time at a designated start date and time, or it can be configured to execute the policy repeatedly according to a designated schedule.

Managing triggers involves these activities:

- Adding, Viewing, or Updating a Trigger, page 6-13
- Deleting a Trigger, page 6-15

Adding, Viewing, or Updating a Trigger

You can add, view, or update triggers for any Multi-Purpose type policy.

Before you can configure a trigger, you must configure an action for the policy as described in the "Adding or Updating an Action for a Multi-Purpose Type Policy" section on page 6-8.

To add, view, or update a trigger for a Multi-Purpose type policy, perform the following procedure. If you update a trigger for a policy that is executing, that change takes affect with the policy execution completes.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the Multi-Purpose type policy for which you want to add an action.

Step 3 Click the **Trigger** tab.

The Policies > *Policy Name* window displays a list of triggers that have been created for this policy. The Trigger Type column displays the type of trigger and the Trigger Name column displays the name that was assigned to the corresponding trigger.

Step 4 Take either of these actions:

- To add a new trigger, click **Add** at the bottom of the list of triggers.
- To view or update an existing trigger, click the link for the trigger in the Trigger Type column.

The New Trigger window displays.

Step 5 From the Trigger Type drop-down list, choose **Time**.

Step 6 In the Trigger Name field, enter a descriptive name for the trigger.

If a policy includes more than one trigger, each trigger name must be unique.

Step 7 Designate the date and time at which the policy first executes by taking these actions:

a. In the Start Date field, enter the date on which the policy first executes.

b. From the Start Time drop-down list, choose the hour, minute, and time designation (AM or PM) at which the policy executes on the start date.

For a non-recurring policy, these fields designate the date and time that the policy executes for a single occurrence. For a recurring policy, these fields designate the date and time that the policy first executes and the time that each subsequent execution starts.

Step 8 Take either of these actions:

- If you want the policy to execute only once, choose **None** from the Recurrence drop-down list, and then go to Step 11.
- If you want the policy to execute more than once, choose one of the following options from the Recurrence drop-down list:
  - **Daily**—Policy executes every day or every certain number of days
  - **Weekly**—Policy executes every certain number of weeks on designated days
  - **Monthly**—Policy executes every certain number of months on designated days
  - **Yearly**—Policy executes once a year on the designated day

Step 9 If you chose a recurrence option, in the Recurrence End Date field, enter the date on which the policy will last execute.

Step 10 If you chose a recurrence option, follow the steps in Table 6-6 to designate how often the policy executes.

Table 6-6 Designating a Recurrence Pattern for a Trigger

Steps	Examples
Recurrence: Daily	
Enter a number between 1 and 999 to designate the cycle, in days, for the execution of the policy.	• Every 1 day(s)—Policy executes every day. • Every 2 day(s)—Policy executes every other day.
Recurrence: Weekly	
1. Enter a number between 1 and 999 to designate the cycle, in weeks, for the execution of the policy. 2. Check one or more check boxes to indicate the days on which a policy executes during a week that it executes.	• Every 1 week(s) on Monday, Tuesday—Policy executes on Monday and Tuesday of every week. • Every 3 week(s) on Monday, Wednesday, Friday—Policy executes on Monday, Wednesday and Friday every 3 weeks.
Recurrence: Monthly	
Take either of these actions: • Click the **Day** radio button, choose how often during a month the policy executes, and choose the cycle, in months, for the execution of the policy • Click the lower radio button and choose the day that a policy executes, and choose how often, in months, the policy executes.	• Day 04 every 1 month(s)—Policy executes the 4th day of every month. • Day 06 every 3 month(s)—Policy executes every 6th day of the month every 3 months. • The First Monday every 1 month(s)—Policy executes on the 1st Monday of every month. • The Last Friday every 6 month(s)—Policy executes on the last Friday every 6 months.
Recurrence: Yearly	
Choose the month and date on which the policy executes each year.	• January 3—Policy executes on January 3 each year.

Step 11 Click **Save** to save your changes.

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

Deleting a Trigger

You can delete a trigger at any time. You can delete a single trigger or you can delete several triggers at one time. If you delete a trigger while its associated policy is executing, the action is removed after the execution completes.

To delete a trigger or triggers, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy that includes the trigger that you want to delete.

Step 3 Click the **Trigger** tab.

Step 4 Check the check box next to each trigger that you want to delete.

Step 5 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 6 To confirm the deletion, click **OK**.

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

Associating Users with a Policy

A user who is associated with a policy can activate and deactivate the policy. A policy can have an unlimited number of associated users, and a user can be a associated with an unlimited number of policies.

To associate a user with a policy, perform the following procedure. If you update associations for a policy that is executing, that change takes effect after the policy execution completes.

Note A Cisco IPICS operator can associate users with a policy as described in the "Associating Policies with a User" section on page 3-20.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 Take either of these actions:

- Click the link for the policy in the Policies column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the Policy name, then click the **Associations** button at the bottom of the Policies window

Step 3 The Associated Users window appears, which displays the following information for each user that is associated with the policy:

- User Name—Unique identification name assigned to the user when the user was added to Cisco IPICS

- First Name—First name of the user
- Last Name—Last name of the user
- Status—Whether the user is enabled or disabled

Step 4 Click **Add** and, in the Search window, locate and choose the users to be associated with the policy.

For information about using the Search window, see the "Using Search Windows" section on page 1-12.

The users that you choose appear in the list of associated users. If you want to remove any user from the list, check the check box next to the user, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

Activating a Policy Manually

You can manually activate a Multi-Purpose type policy at any time. When you activate a policy, it immediately begins to execute the actions that are configured for it.

You can manually activate a single policy, or you can manually activate several policies at one time.

Note A Multi-Purpose type policy can also be activated by a trigger, by re-activating it on the Execution Status window, or through the TUI.

An invitation type policy can be activated only through the TUI.

To manually activate a Multi-Purpose policy, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 Check the check box next to each Multi-Purpose type policy that you want to activate.

Step 3 Click **Activate**.

Deleting a Policy

You can delete a policy when you no longer need it. You can delete a single policy or you can delete several policies at one time. If you delete a a policy that is executing, the execution completes.

To delete a policy, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 Check the check box next to each policy 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 user group, click **Cancel**.

Viewing Information about Executing or Executed Policies

You can view summary or detailed information about policies that are executing or that have executed. This information includes the policy name, associated actions, status, start time, execution messages. You can also access additional information for actions, including a list of recipients that a policy calls, whether the call was successful, and if not, why not.

In addition, you can export to an .xml file information about policies to which you are associated or that are created by users who belong to or are accessible to your ops view.

To view information about policies that have not executed, see the "Viewing Information about Scheduled Policies" section on page 6-19.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Execution Status**.

Step 2 Click the **Executing/Executed Policy** tab.

This tab displays the following information:

- Name—Name of the policy, or name of an action in an expanded policy view.
- Action Type—Type of action. Information displays if you expand the view of a policy.
- Status—Status of the policy, such as Successful, Executing, or Failed.

  If any action in a policy with more than one action fails, the status of the policy will show as Failed. The policy attempts to execute all actions even if one or more actions fail.
- Start Time—Date and time that an upcoming policy or action is scheduled to start, or date and time that an executing policy or action started.
- Message—Summary information regarding the execution of the policy.

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

Step 3 To navigate this tab or to change the display, see Table 6-7.

Table 6-7 Executing/Executed Policy Tab Activities

Activity	Procedure
Designate how many rows of information appear on a page.	Choose a value from the Rows per page drop-down list and then click **Go**.

Table 6-7 Executing/Executed Policy Tab Activities (continued)

Activity	Procedure
Go to another page of the display.	Use these buttons at the bottom of the window: • |< (go to first page) • < (go to previous page) • > (go to next page) • >| (go to last page)
Display the list of policies in alphabetical or reverse alphabetical order by name or status, or in numerical order or reverse numerical order by start time.	Click the appropriate column heading, then click the Up Arrow or the Down Arrow next to that column heading.
See an expanded view with information about the actions that are associated with a policy.	Click + next to the policy name.
Close an expanded view with information about the actions that are associated with a policy.	Click - next to the policy name.
See additional information about the participants in a dial out or notification action that is associated with the policy.	Click the action name link after expanding the view of the policy.
Export to an .xml file information about policies that are executing or that have executed to which you are associated or that are created by users who belong to or are accessible to your ops view.	Click **Download Execution Status**, which appears at the bottom of the window, and enter the file name and storage location in the pop-up window.
Export to an .xml file information about all policies that are executing or that have executed.	Click **Download All Execution Status**, which appears at the bottom of the window, and enter the file name and storage location in the pop-up window.
Delete the information for a policy.	Click **Delete**, which appears at the bottom of the window. This action deletes execution information only. It does not delete the policy. You cannot select and delete information about individual actions in a policy.
Reactivate a policy, an action, or an action for a specific participant in a policy.	See the "Re-Activating a Policy or an Action" section on page 6-19.

Viewing Information about Scheduled Policies

You can view summary or detailed information about policies that are scheduled to execute. This information includes the policy name, associated actions, status, start time, and execution messages.

To view summary information about policies that are executing or that have completed executing, see the Viewing Information about Executing or Executed Policies, page 6-17.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Execution Status**.

Step 2 Click the **Scheduled Policy** tab.

This tab displays the following information:

- Name—Name of the policy, or name of an action in an expanded policy view.
- Action Type—Actions that are created for this policy. Information displays if you expand the policy as described in Step 3.
- Status—Status of the policy, such as Successful, Executing, or Failed.
- Start Time—Date and time that an upcoming policy is scheduled to start, or date and time and an executing policy started.
- Message—Summary information regarding the execution of the policy.

Step 3 To see an expanded view with information about the actions that are associated with a policy, click **+** next to the policy name.

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

Re-Activating a Policy or an Action

You can use the reactivate feature to perform any of these activities:

- Reactivate a policy—Activates a Multi-Purpose type policy again. This activity has the same effect as manually activating the policy as described in the "Activating a Policy Manually" section on page 6-16. You can reactivate a single policy, or you can re-execute several policies at one time. You cannot reactivate an invitation type policy.
- Reactivate an action—Activates one or more specific actions in a designated policy.
- Reactivate an action for a specific participant—Activates a dial out or a notification action for one or more specific participants in that action.

To reactivate a policy or an action, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Execution Status**.

Step 2 Click the **Executing/Executed Policy** tab.

Step 3 Perform the desired activity as described in Table 6-8.

Table 6-8 Re-activation Activities

Activity	Procedure
Reactivate a policy	1. Check the check box next to each policy or policies that you want to reactivate. 2. Click **Reactivate** at the bottom of the list of policies.
Reactivate an action in a policy.	1. Click **+** next to the name of the policy that includes the action. 2. Check the check box next to each action or actions that you want to reactivate. 3. Click **Reactivate** at the bottom of the list of policies.
Reactivate a dial out or a notification action for a specific participant in the action.	1. Click **+** next to the name of the policy that includes the action. 2. Click the link in the Name column for the action that includes the participant. 3. Check the check box next to each participant or or participants that you want to reactivate. 4. Click **Reactivate** at the bottom of the list of participants.

Using the Policy Engine Telephony User Interface

The policy engine TUI lets you use a touch-tone telephone to receive information from and provide instructions to the policy engine. When you use the TUI, the policy engine communicates with you through verbal prompts that you hear on your telephone. You respond to these prompts by pressing keys on your telephone.

The TUI provides the capability for you to perform these activities:

- Join and participate in a group with which you are associated by using your phone as a push-to-talk (PTT) device

Note You can also use a Cisco Unified IP Phone as a Cisco IPICS PTT device as described Appendix C, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

- Activate a policy of any type
- Perform activities designated by a policy
- Invite other users to join a group
- Record spoken name prompts
- Change your digit password (PIN)
- Obtain status information about policies that have executed or are executing

Accessing the TUI

You can access the TUI from a touch-tone telephone. You can access the TUI in these ways:

- By calling the policy engine—Call the number that is configured in the Dial Number field for your ops view. (For related information, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views.")
- By receiving a call from the policy engine—You receive a call when another user invites you to join a group, when a Cisco IPICS dispatcher initiates a dial out from the VTG Management window, when a policy that includes one or more actions to call you executes, or when you record a prompt.

When you access the TUI, perform these actions:

1. Follow the verbal prompts to enter your user ID and PIN.

   A user ID and PIN are configured by a Cisco IPICS operator or by a user. Your login credentials work only for the dial number that is configured for the ops view that you belong to.

2. Follow the verbal prompts to perform the desired action or actions.

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 6-21
- Menu Guidelines, page 6-22

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 group, 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 group. (As the call is being dialed out, the system does not play any sounds.)
- To terminate your input, press #.
- To return to the previous menu, except when you are using the main menu, press *.
- To select resources, such as groups or policies, from a menu, press the number that corresponds to your selection when the number of entries is 9 or less. When 10 or more entries exist, you must press the number that corresponds to your selection followed by #.
- The option to select a resource by spelling its name depends on your locale:
  - The TUI supports the following locales: Afrikaans (af), Albanian (sq), Basque (eu), Catalan (ca), Danish (da), Dutch (nl), English (en), Faroese (fo), Finnish (fi), French (fr), German (de), Icelandic (is), Irish (ga), Italian (it), 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 group, press 1. Then, you can press 1 to select an assigned group to join by spelling out the group name, or press 2 to listen to the list of assigned groups and then selecting from that list. (If you know the name of the group that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available groups.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke a general purpose policy, press 2. Then, you can press 1 to select a policy by spelling its name, or press 2 to listen to the list of available policies. (If you know the name of the policy that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available policies.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke the system menu, press 0. From this menu, you can take the following actions:

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

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

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

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

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

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

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

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

    - To perform an ad-hoc invitation, press 1. To confirm your selection, press 1 (no 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 *.