CHAPTER 3

Performing Cisco IPICS Operator Tasks

The Cisco IPICS operator is responsible for setting up and managing Cisco IPICS users and user groups, granting users access to Cisco IPICS and to the PMC, and assigning user channels, roles, and operational views (ops views).

A user can participate in an active VTG and communicate with other VTG participants. A user group is a logical grouping of users. A user group can be added to a VTG, which provides a Cisco IPICS dispatcher with an efficient method of adding several users to a VTG one at a time.

You perform Cisco IPICS operator activities from the User 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 1-12, then choose the **User Management** drawer in the Server tab. You must be assigned the operator role to access the User Management drawer.

Note

- Some of the explanations and procedures in this chapter refer to information that displays or to tasks that you can perform only if ops views is enabled. For more information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views.".
- Several procedures in this chapter describe how to view or update information for a user from the User Management drawer. Users can also perform many of these procedures for their personal information from the Home drawer. For more information, see Chapter 5, "Performing Cisco IPICS User Tasks."

The following sections describe the operator activities that you can perform from the Cisco IPICS Administration Console:

Managing Users

A Cisco IPICS user can perform the following activities:

- Access the My Profile window in the Cisco IPICS Administration Console and perform the tasks that are available in that window
- Access channels with which they are associated
- Participate in VTGs to which they are assigned
- Use direct two-way channels to communicate through the PMC over a SIP channel with other associated users with which they are associated
- Communicate through the PMC with associated dial-in users
- Download the PMC installer

This section describes the following user management activities:

Understanding the Users Window

The Users window lists information about users that you have added in Cisco IPICS and provides the ability to perform several user management functions. The bottom area of this window displays a list of Cisco IPICS users and general information for each user. By default, this area displays all users, but you can choose to display only those users that match search criteria that you specify in the top area of the window.

To display the Users window, access the User Management drawer and click **Users**.

Table 3-1 describes the items in the Users window.

Table 3-1 Items in the Users Window

Item	Description	Reference
Filters		
User Name field First Name field Last Name field	Provides the ability to display only those users whose user name, first name, or last name begins with the character string that you enter (characters are not case-sensitive)	See the "Using Search Windows" section on page 1-14
Location drop-down list Role drop-down list Ops View drop-down list	Provides the ability to display only those users whose location, role, or associated ops view match the information that you choose	
Go button (in Users area)	Displays users according to the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of users	
User Information		
User Name field	User name assigned to the user	See the "Adding a User" section on page 3-6

Table 3-1 Items in the Users Window (continued)

Item	Description	Reference
Last Name field	Last name of the user	See the "Managing General Information for a User" section on page 3-9
First Name field	First name of the user	
Ops View field	Ops view to which the user belongs	See the "Managing Ops Views for a User" section on page 3-38
End Device Status field	Can display these icons:  —Audio of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk or listen in a channel or VTG  —Microphone of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk in a channel or VTG	See the "Changing User Status" section on page 3-41 and the "Managing an End Device from the User Management Window" section on page 3-15
Status field	Indicates whether a user is enabled or disabled	See the "Changing User Status" section on page 3-41
Prompt	Indicates whether a spoken name prompt is recorded for the user	See the "Managing Prompts for a User" section on page 3-40
Password Expiration field	Indicates when the password of the user expires	See the "Managing Cisco IPICS Options" section on page 2-127
Account Status field	Shows if a user account is locked or available	See the "Locking or Unlocking a User Account" section on page 3-42
Add button	Provides the ability to add a new Cisco IPICS user	See the "Adding a User" section on page 3-6
Copy button	Provides the ability to copy information from an existing user when you add a new user	
Delete button	Provides the ability to you delete a user	See the "Deleting a User" section on page 3-44

Table 3-1 Items in the Users Window (continued)

Item	Description	Reference
Change Status drop-down list	Provides the ability to enable or disable a user and lock or unlock a user account	See the "Changing User Status" section on page 3-41 and the "Locking or Unlocking a User Account" section on page 3-42
End Device drop-down list	Provides the ability to perform several activities for the PMC, Cisco Unified IP Phone, and dial-in phone of a user	See the "Managing an End Device from the User Management Window" section on page 3-15
Associations button	Displays the Associations window for a user	See these sections: • Associating PTT Channels with a User, page 3-28 • Associating Users with a User to Configure the Direct Two-Way Channel Feature, page 3-30 • Associating Phones with a User to Configure the Direct Dial Feature, page 3-31 • Associating Policies with a User, page 3-32 • Viewing Information about VTGs in which a User is a Participant, page 3-40
Display Controls		
Rows per page drop-down list	Specifies the number of rows of users that are included in a users list page	See the "Navigating Item Lists" section on page 1-16
Page field	Displays users on a specific page	
|< (First page) button	Displays the first page of the users list	
< (Previous page) button	Displays the previous page of the users list	
> (Next page) button	Displays the next page of the users list	
>| (Last page) button	Displays the last page of the users list	

Adding a User

When you add a user to Cisco IPICS, you assign a user ID to that user and configure several other options for the user.

If you add a user who has the same channel assignments, roles, and other information as that of an existing user, you might find it convenient to start by copying the information of the existing user. When you copy such information, Cisco IPICS opens a New Users window and enters all information that is stored for the existing user, except the user ID, password, digit ID, and digit password (PIN).

Before you add a user, you must configure locations as described in the "Adding Radio and Tone Descriptors" section on page 2-70.

To add a new user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 From the Users area in the Managing Users window, take either of these actions:

- To add a user starting with a blank New User window, click **Add**.
- To add a user starting with a New User window that includes information based on an existing user, check the check box next to the existing user, and then click **Copy**.

Note The **Copy** button appears dimmed if you do not check an existing user or if you check more than one existing user.

The New User window displays. If you clicked **Copy**, this window includes information from the existing user, except for the user ID and password.

Step 3 In the New User window, take these actions:

a. In the User Name field, enter a unique identification name for this user.

The User ID can include alphanumeric characters, numbers, underscores (_), and periods (.).

A User ID is not case-sensitive. If a User ID contains alphabetic characters, a user can enter the characters in upper case or lower case when logging in to Cisco IPICS.

b. In the First Name field, enter the First name of the user.

Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (').

c. In the Last Name field, enter Last name of the user.

Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (').

d. In the Password and the Confirm Password fields, enter the password that the user enters when logging in to Cisco IPICS or the PMC. (The actual characters in the password are represented by asterisks (*)).

You specify requirements for passwords, including length and character requirements, in the **Administration > Options** window.

Valid characters include: alphanumeric characters and these special characters: @ [\ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?.

Passwords are case-sensitive. A user must enter a password exactly as it is configured.

e. (Optional) In the Description field, enter a description of, or notes that relate to, the user for your reference.

f. From the Belongs To drop-down list in the Ops Views area, choose the ops view to which the user group belongs.

Step 4 Perform the tasks that are described in Table 3-2, as needed.

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

Table 3-2 Tasks for Adding a Cisco IPICS User

Task	Reference
In the Address tab, enter the physical address and the e-mail address for the user.	See the "Managing Address Information for a User" section on page 3-11.
In the General tab, assign one or more Cisco IPICS roles to the user.	See the "Managing Roles for a User" section on page 3-12.
In the General tab, choose the ops view to which this user belongs, and specify the ops views that can access this user.	See the "Managing Ops Views for a User" section on page 3-38.
In the Dial Login tab, enter login information, if the user will access Cisco IPICS from a Cisco Unified IP Phone.	See the "Managing Dial Login Information for a User" section on page 3-13.
In the PMC tab, designate how a user communicates through the PMC, choose whether PMC log files are on or off, and specify debug levels for PMC log files.	See the "Managing an End Device from the PMC Tab" section on page 3-19.
In the Communications tab, specify how a user is contacted when a Cisco IPICS policy engine (hereafter referred to as policy engine) notification action executes or when a Cisco IPICS dispatcher initiates a policy engine dial-out to the user.	See the "Managing Communications Preferences for a User" section on page 3-23.
Associate ops views with the user.	See the "Managing Ops Views for a User" section on page 3-38.

Step 5 Click **Save** to add the user.

If you do not want to add the user, click **Cancel**.

Managing User Information

Cisco IPICS provides the ability for the operator to manage a variety of user information, as described in the following sections:

Managing General Information for a User

General information for a user includes the name, Cisco IPICS login credentials, and default location of the user.

You can add, view, or update general information for any user. To do so, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 In the User Name column, click the link for the user whose information you want to view or update.

Step 3 Click the **General Information** tab and view or enter the information that is described in Table 3-3.

Table 3-3 General Information

Field	Description
User Name	*Display only.* User name assigned when the user was created.
First Name	First name of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Last Name	Last name of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Password	Password that the user enters when logging in to Cisco IPICS or the PMC. (The actual characters in the password are represented by asterisks (*)). You specify requirements for passwords, including length and character requirements, in the **Administration > Options** window. Valid characters include: alphanumeric characters and these special characters: @ [\ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?.
Confirm Password	Confirmation of the entry in the password field.
Description	Description of, or notes that relate to, the user for your reference.
Password Expiration Date	*Display only.* Indicates when the password of the user expires.

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

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

Managing Address Information for a User

Address information for a user includes the physical address and e-mail address of the user.

You can add, view, or update address information for any user. To do so, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 In the User Name column, click the link for the user whose information you want to view or update.

Step 3 Click the **Address Information** tab and view or enter the information that is described in Table 3-4.

Table 3-4 Address Information

Field	Description
Address	Street address of the user. Valid characters include: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :
Address (cont)	Additional street address information. Valid characters include: alphanumeric characters, spaces, and these special characters include: . , – ‘ # ( ) / :
City	City of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
State/Province	State or province of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Country	Country of the user. Valid characters include: alphanumeric characters, space, and period (.).

Table 3-4 Address Information (continued)

Field	Description
Zip/Postal Code	Zip code or postal code of the user. Valid characters include: alphanumeric characters, space, and period (.).
E-mail	E-mail address of the user. Valid characters include: alphanumeric characters, underscore (_), period (.), and at sign (@).

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

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

Managing Roles for a User

Roles determine the Cisco IPICS features that a user can access and the functions that a user can perform. All users are assigned the user role by default. In addition, you can assign one or more of the following roles to a user:

- Dispatcher—Responsible for setting up system policies and setting up inactive VTGs, activating VTGs to begin conferences, and adding or removing participants in inactive VTGs and active VTGs. Also monitors active VTGs, and creates and manages policies.
- Operator—Responsible for setting up and managing users, granting access to Cisco IPICS and the PMC, and assigning user channels, roles and ops views.
- Ops view administrator—Manages and monitors the activity logs that are filtered by ops views.
- System administrator—Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. Also creates ops views, manages Cisco IPICS licenses and PMC versions, creates and manages policies, and monitors the status of the system and its users via the activity log files and dashboard.
- All—Equivalent to assigning each of the above roles individually.

To add, view, or change roles for a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **General Information** tab.

Step 4 Choose the desired role from the drop-down list in the Roles area.

When you do so, a new Role field displays, which allows you to assign another role. Repeat this step to assign additional roles.

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

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

Managing Dial Login Information for a User

Dial login information consists of the login credentials that a user enters in the following situations:

- When logging in to the Cisco IPICS service from a Cisco Unified IP Phone. This service allows a Cisco Unified IP Phone user to communicate on PTT channels and participate in channels and VTGs.

  For related information, see Appendix B, “Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device.”

- When logging in to the policy engine telephony user interface (TUI) from a touch-tone telephone. The TUI allows a phone user to interact with the policy engine.

  For related information, see the “Using the Policy Engine Telephony User Interface” section on page 7-30.

To add, view, or change dial login information for a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Dial Login** tab view or update the information that is described in Table 3-5.

Table 3-5 Dial Login Information

Field	Description
Digit ID	Numeric ID that the user enters when accessing the Cisco IPICS service from a Cisco Unified IP Phone or when accessing the TUI. Valid characters include: numeric characters.
Digit Password (PIN)	Password that the user enters when accessing the Cisco IPICS service from a Cisco Unified IP Phone or PIN that the user enters when accessing the TUI. (The actual characters in the password are represented by asterisks (*)) You specify requirements for passwords, including length and character requirements, in the **Administration** > **Options** window. Valid characters include: numeric characters.
Confirm Digit Password	Confirmation of the entry in the Digit Password (PIN) field.
Default Location	Location from which a phone connects to Cisco IPICS. For additional information about locations, see the "Adding Radio and Tone Descriptors" section on page 2-70.

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

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

Managing an End Device for a User

An end-device can be the PMC, Cisco Unified IP Phone, or dial-in phone. As a Cisco IPICS operator, managing an end device of a user involves the following activities:

- Managing an End Device from the User Management Window, page 3-15—Provides the ability to mute or unmute an end device, disable or enable an end device, and obtain PMC log files
- Managing an End Device from the PMC Tab, page 3-19—Provides the ability to obtain log files, turn log files on or off, set log levels, and designate whether a user can listen or speak in a VTG
- Managing the PMC from the Associations Tab, page 3-21—Provides the ability to control a variety of options for each channel that is associated with a user

Managing an End Device from the User Management Window

From the User Management window, you can perform the following activities for the PMC, Cisco Unified IP Phone, or dial-in phone of a user:

- Mute or unmute the PMC, Cisco Unified IP Phone, or dial-in phone
- Disable or enable the PMC, Cisco Unified IP Phone, or dial-in phone
- Obtain a variety of log files for use in troubleshooting

You can perform these activities for a single user, or for several users at one time.

To manage the end device of a user or users from the User Management window, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Check the check box next to each user whose end device you want to manage.

Step 3 From the End Device drop-down list at the bottom of the window, choose the desired option.

Table 3-6 describes these options.

Table 3-6 PMC Drop-Down List Options

Option	Explanation	Notes
Set Listen Only	Disables the transmission of audio from the PMC, Cisco Unified IP Phone, and dial-in phone, which restricts a user to listening only	Affects any PMC or Cisco Unified IP Phone that a user logs in to, and affects any phone from which the user dials in to the TUI. You can also control whether a user can listen or talk from an end device as described in the "Managing an End Device from the PMC Tab" section on page 3-19 and the "Managing the PMC from the Associations Tab" section on page 3-21.
Unset Listen Only	Enables the transmission of audio from the PMC, Cisco Unified IP Phone, and dial-in phone	

Table 3-6 PMC Drop-Down List Options (continued)

Option	Explanation	Notes
Disable Audio	Disables the microphone and speaker on the PMC or a Cisco Unified IP Phone that is logged in to the Cisco IPICS service, which prevents a user from listening and talking	Affects any PMC or Cisco Unified IP Phone that a user logs in to. Does not affect a phone from which a user dials in to the TUI.
Enable Audio	Enables the microphone and speaker on the PMC or a Cisco Unified IP Phone that is logged in to the Cisco IPICS service, which allows a user to listen and talk	

Table 3-6 PMC Drop-Down List Options (continued)

Option	Explanation	Notes
Get Authentication Logs	Obtains the PMC authentication log file	If the user is logged in to the PMC, copies the specified log file from that PMC to the following location on the Cisco IPICS server: /root/tomcat/current/webapps/ipics_server/pmclogs/<*user_name*>/<*PMC_ID*>/<*folder*> where: • *user_name* is the unique user name that is assigned to the user • *PMC_ID* is the ID that the system generates for the PMC installation • *folder* is the name of the log file type: Authentication, Channel Statistics, User Interface, or Debug Log file naming uses this convention: <*year*>.<*month*>.<*day*>.<*hour(24)*>.<*minute*>.<*second*>.<*millisecond*>.log where *year*, *month*, *day*, *hour(24)*, *minute*, *second*, and *millisecond* identify the date and time that the file was created. If the user is not logged in to the PMC, the request for a log file is ignored. When you request a log file, the PMC client closes the file, renames it, and starts a new file. After the renamed file uploads to the Cisco IPICS server, it is deleted from the PMC client. **Note** A log may be empty if logging is not turned on. For descriptions of these log files, refer to the "Using the PMC Application Logs" chapter in *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*. For related information about log files, see the "Managing Cisco IPICS Options" section on page 2-127.
Get Channel Statistics Logs	Obtains the PMC channel statistics log file	
Get User Interface Logs	Obtains the PMC user interface log file	
Get Debug Logs	Obtains the PMC debug log file	

Managing an End Device from the PMC Tab

From the User Management: Users > *Username* > PMC tab, you can perform the following activities for the end device of a user:

- Designate how a user communicates in VTGs
- Obtain PMC log files
- Turn PMC log files on or off and set log levels

To manage the end device of a user from the User Management: Users > *Username* > PMC tab, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **PMC** tab.

Step 4 To designate how a user communicates in VTGs, check the appropriate check boxes in the PMC Info area:

- Disable Audio—Disables the microphone and speaker on the PMC or Cisco Unified IP Phone that is logged in to the Cisco IPICS service. Does not affect a phone from which a user dials in to the TUI.
- Listen Only—Disables the transmission of audio from the PMC, Cisco Unified IP Phone, and dial-in phone, which restricts a user to listening only.
- Allow Latch—User can use the latch feature on the PMC or Cisco Unified IP Phone.
- Advanced PMC Permissions (Multi-select, Tones, DTMF, All Talk)—User can use the Multi-select, Alert Tones, Dual-Tone Multi-Frequency (DTMF), and All Talk features on the PMC.

Step 5 To turn on or set log levels for the PMC log files, take the desired actions:

- Choose whether the following PMC log files are on or off by making a selection from the corresponding drop-down list:
  - Authentication
  - User Interface
  - Channel Statistics
- Choose the debug level for the following PMC log files by making a selection from the corresponding drop-down list:
  - Debug Signaling
  - Debug User Interface
  - Debug Media

Note Do not turn on the PMC log file unless you need it. If you turn on a log file, set it to the lowest debug level that provides the information that you need. Log files can consume significant disk space, and the higher the debug level, the more disk space that is used.

Step 6 To obtain a log file from the PMC, choose one of the following options from the Get Logs from PMC drop-down list, and then click **Get Logs from PMC**:

- **Authentication**—Obtains the PMC authentication log file
- **Channels Statistics**—Obtains the PMC channel statistics log file
- **User Interface**—Obtains the PMC user interface log file
- **Debug**—Obtains the PMC debug log file

If the user is logged in to the PMC, clicking **Get Logs from PMC** copies the specified log file from that PMC to the following location on the Cisco IPICS server:

/root/tomcat/current/webapps/ipics_server/pmclogs/<*user_name*>/<*PMC_ID*>/<*folder*>

where:

- *user_name* is the unique user name that is assigned to the user
- *PMC_ID* is the ID that the system generates for the PMC installation

- *folder* is the name of the log file type: Authentication, Channel Statistics, User Interface, or Debug

Log file naming uses this convention:

<year>.<month>.<day>.<hour(24)>.<minute>.<second>.<millisecond>.log

where *year*, *month*, *day*, *hour(24)*, *minute*, *second*, and *millisecond* identify the date and time that the file was created.

If the user is not logged in to the PMC, the request for a log file is ignored.

When you request a log file, the PMC client closes the file, renames it, and starts a new file. After the renamed file uploads to the Cisco IPICS server, it is deleted from the PMC client.

Note A log file may be empty if logging is not turned on.

For descriptions of the PMC log files, refer to the "Using the PMC Application Logs" chapter in *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*. For related information about log files, see the "Managing Cisco IPICS Options" section on page 2-127.

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

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

Managing the PMC from the Associations Tab

From the User Management: Users > *Username* > Associations tab, you can perform the following activities for the PMC, Cisco Unified IP Phone, or dial-in phone of a user:

- Enable or disable the latch feature on the PMC or Cisco Unified IP Phone
- Enable or disable Listen Only on the PMC, Cisco Unified IP Phone, or dial-in phone
- Enable or disable Voice Activation Detection (VAD) on the PMC

You can perform these activities for any or all channels with which the user is associated.

To manage the PMC of a user from the User Management: Users > *Username* > Associations tab, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Associations** button at the bottom of the window.

Step 4 Make sure that the **Channels** tab is selected.

This table displays the channels that are associated with this user. The status field shows whether the channel is enabled or disabled. The Associations Attributes fields display settings for various end device parameters.

Step 5 Check the check box next to each channel for which you want to change the end device status.

Step 6 From the Change PMC Status drop-down list, choose the desired option.

Table 3-7 describes these options.

Table 3-7 PMC Drop-Down List Options

Option	Explanation
Allow Latch	Allows the user to use the latch feature on the PMC or Cisco Unified IP Phone.
Disallow Latch	Prevents the user from using the latch feature on the PMC or Cisco Unified IP Phone.
Set Listen Only	Disables the transmission of audio from the PMC, Cisco Unified IP Phone, or dial-in phone, which restricts a user to listening only.
Unset Listen Only	Enables the transmission of audio from the PMC, Cisco Unified IP Phone, or dial-in phone.

Table 3-7 PMC Drop-Down List Options (continued)

Option	Explanation
Enable Audio	Enables the microphone and speaker on the PMC or a Cisco Unified IP Phone that is logged in to the Cisco IPICS service, which allows a user to listen and talk. Does not affect a phone from which a user dials in to the TUI.
Disable Audio	Disables the microphone and speaker on the PMC or Cisco Unified IP Phone that is logged in to the Cisco IPICS service, which prevents a user from listening and talking. Does not affect a phone from which a user dials in to the TUI.

Note The options that you choose are applied immediately. You do not need to click **Save** to save changes, and clicking **Cancel** does not cancel changes.

Managing Communications Preferences for a User

Communications preferences specify how the policy engine contacts a user when a policy with which the user is associated executes or when a Cisco IPICS dispatcher initiates a policy engine dial-out call to the user. For more information about the policy engine and messages that users receive when they are contacted, see Chapter 7, "Using the Cisco IPICS Policy Engine" and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

When you specify communication preferences, you can provide the following information:

- Notification Preferences—Any combination of one or more e-mail, Short Message Service (SMS), or pager addresses
- Dial Preferences—One or more telephone numbers

This section includes these topics:

Viewing, Adding, Editing, or Deleting Communications Preferences

When a policy with which a user is associated executes, the policy engine handles communications preferences for the user as follows:

- Notification Preferences—Policy engine contacts each e-mail, Short Message Service (SMS), or pager address that is specified
- Dial Preferences—If the policy engine is configured to dial, it calls each number in sequence until it reaches a user who enters a valid ID and PIN to confirm receipt of the call

To view, add, edit, or delete notification preferences and dial preferences for a user perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Communications** tab.

This tab displays the following information:

- Type (under Notification Preferences)—Method by which the user is notified:
  - Email—Notification is sent to an e-mail address
  - Pager—Notification is sent to a pager through an e-mail gateway
  - SMS—Notification is sent to an SMS through an e-mail gateway
- Number/Address (under Notification Preferences)—E-mail address for the corresponding notification type
- Type (under Dial Preferences)—Description of the location to be dialed, such as Business, Car, or Home

- Dial Number (under Dial Preferences)—Telephone number of the corresponding location type

Step 4 To add, edit, or delete notification preferences, take the appropriate actions under the Notification Preferences list:

- To add a notification preference:
  a. Click **Add**.
  b. From the drop-down list, choose a method by which the user receives notifications (e-mail, pager, or SMS).
  c. In the field next to the drop-down list, enter the e-mail address for the corresponding notification method.

     For the SMS and Pager methods, the e-mail address is for a gateway through which the message will be sent to the device.
  d. Click **Done**.
  e. Repeat these steps as needed to add more notification preferences.
- To edit a notification preference:
  a. Check the check box next to the notification preference that you want to edit.
  b. Click **Edit**.
  c. From the drop-down list, choose a method by which the user receives notifications.
  d. In the field next to the drop-down list, enter the enter the e-mail address for the corresponding notification method.
  e. Click **Update**.
- To delete a notification preference:
  a. Check the check box next to the notification preference or preferences that you want to delete.
  b. Click **Delete**.

Step 5 To add, edit, or delete dial preferences, take the appropriate actions under the Dial Preferences list:

- To add a dial preference:
  a. Click **Add**.
  b. From the drop-down list, choose a description for the dial preference.
  c. In the field next to the drop-down list, enter the telephone number for the corresponding dial preference.

     The first character must be a digit or a plus sign (+).

     This character can be followed by zero or more of these characters: digits, upper case or lower case letters, space, : . , - ( ) # *.

     One or more digits must be included next.

     The number may end with a digit or with one or more pound signs (#) or asterisks (*).
  d. Click **Done**.
  e. Repeat these steps as needed to add more dial preferences.
- To edit a dial preference:
  a. Check the check box next to the notification preference that you want to edit.

     You can use the Up Arrow and Down Arrow buttons to move a check to an adjacent check box.
  b. Click **Edit**.
  c. From the drop-down list, choose a description for the dial preference.
  d. In the field next to the drop-down list, enter the enter the telephone number for the corresponding dial preference.

     This field can contain numerals, dashes (-), and spaces. If the telephone number includes an extension, precede the extension with an uppercase or lowercase X.
  e. Click **Update**.

- To delete a dial preference:
  a. Check the check box next to the dial preference or preferences that you want to delete.

     You can use the Up Arrow and Down Arrow buttons to move a check to an adjacent check box.

  b. Click **Delete**.

Step 6 Check the **Dial after sending notifications** check box if you want the policy engine to attempt to call a user on the numbers in the Dial Preference list when a policy with which the user is associated executes.

If you check this check box, the policy engine attempts to call the user even if you do not specify a notification preference.

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

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

Changing the Order of Dial Preferences

If you check the **Dial after sending notifications** when you configure communications preferences, the policy engine attempts to call a user on the numbers in the Dial Preference list when a policy with which the user is associated executes. The policy engine calls each number on the list in sequence until it reaches a user who enters a valid ID and PIN to confirm receipt of the call.

To change the order of numbers to call in the dial preferences list, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Communications** tab.

Step 4 Check the check box next to the dial preference type that you want to move to a different position in the list.

Step 5 Click the **Up Arrow** button to move the dial preference up in the list or click the **Down Arrow** button to move it down in the list.

Step 6 Repeat Step 4 and Step 5 as needed to move other dial preferences.

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

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

Associating Resources with a User

When you associate a Cisco IPICS resource with a user, you provide the user with access to various features and functions that relate to the resource. You can perform the following association activities:

- Associating PTT Channels with a User, page 3-28
- Associating Users with a User to Configure the Direct Two-Way Channel Feature, page 3-30
- Associating Phones with a User to Configure the Direct Dial Feature, page 3-31
- Associating Policies with a User, page 3-32
- Associating Radios with a User, page 3-34

Associating PTT Channels with a User

Associating PTT channels with a user has the following effects:

- Causes the channels to appear as channels on the PMC of the user
- Causes the channels to appear on a Cisco Unified IP Phone when the user accesses the Cisco IPICS phone service
- Causes the channels to be available to the user through the policy engine telephony user interface

You can also associate PTT channels with a user in the Channels window. See the "Associating Users to PTT Channels" section on page 2-26 for more information.

To associate PTT channels with a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions to display the Associations window for the user with whom you want to associate channels:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list appears dimmed if you do not check a user or if you check more than one user.

Step 3 In the Associations window, make sure that the **Channels** tab is selected.

This tab shows a list of the channels that are associated with the user, the status of each channel, and information about attributes for devices that use the channel.

Step 4 Click **Add**.

The Search Results window appears.

Step 5 In the Search Results window, locate one or more channels with which to associate with this user by optionally specifying search criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-14.

Step 6 In the Search Results window, check the check box next to each channel that you want to associate with this user and then click **OK**.

The channels that you choose appear in the list of associated channels.

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

Associating Users with a User to Configure the Direct Two-Way Channel Feature

Two users who are associated with each other can communicate with each other by using direct two-way channels on their PMC clients. In this way, two online PMC users can communicate with each other even if they are not associated with a channel or are not participants in a VTG.

Associating one user (User A) with another user (User B) has the following effects:

- User B is automatically associated with User A
- The user name of User A appears as a channel on the PMC of user B
- The user name of User B appears as a channel on the PMC of user A

To associate a user with other users, perform the following procedure:

Procedure

Step 1 Take either of these actions to display the Associations window for the user with whom you want to associate users:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list appears dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Users** tab.

This tab shows the user name, last name, first name, and status (enabled or disabled) of each user that is associated with the user that you selected.

Step 3 Click **Add**.

The Search Results window appears.

Step 4 In the Search Results window, locate one or more users with which to associate with this user by optionally specifying search criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-14.

Step 5 Check the check box next to each user that you want to associate with this user and then click **OK**.

The users that you choose appear in the list of associated users.

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

Associating Phones with a User to Configure the Direct Dial Feature

When you associate phones with a user, the user can communicate directly with those phones by using the policy engine direct dial feature.

For information about configuring direct dial, see the "Managing the Direct Dial Feature" section on page 8-39.

To associate phones with a user, perform the following procedure:

Procedure

Step 1 Take either of these actions to display the Associations window for the user with whom you want to associate phones:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list is dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Phones** tab.

This tab shows the dial destination and label of each phone that is associated with this user.

Step 3 Click **Edit**.

The Phone Associations window displays. This window shows the following information:

- Available Phones—Direct dial numbers that can be associated with this user
- Associated Phones—Phones that are associated with the user or that will be associated with the user after you click **Save**

Step 4 Take any of these actions:

- To move a phone from one list to the other, click the phone to highlight it and then click > or <. Or, double-click the phone.
- To move several phones from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the phones and then click > or <.
- To move all phones from one list to the other at one time, click >> or <<.

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

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

Associating Policies with a User

When you associate policies with a user, the user can perform the following activities:

- Activate the policy from the Policies window, as described in the "Activating a Policy Manually" section on page 7-24.
- Activate the policy by calling the policy engine. For related information, see the "Using the Policy Engine Telephony User Interface" section on page 7-30.
- Use the 1 through 9 keys on a telephone as *hot keys* to quickly activate a policy that is associated with the corresponding key.

To associate policies with a user, perform the following procedure.

Note You can also associate policies with a user as described in the "Associating Users with a Policy" section on page 7-23.

Procedure

Step 1 Take either of these actions to display the Associations window for the user with whom you want to associate policies:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list appears dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Policies** tab.

This tab shows the name and type of each policy that is associated with the user.

Step 3 Click **Edit**.

The Policy Associations window displays. This window shows the following information:

- Available Policies list—Policies that can be associated with this user
- Associated Policies list—Policies that are associated with the user or that will be associated with the user after you click **Save**

Step 4 Take any of these actions:

- To move a policy from the one list to the other, click the policy to highlight it and then click > or <. Or, double-click the policy.
- To move several policies from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the policies and then click > or <.
- To move all policies from one list to the other at one time, click >> or <<.

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

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

A user can access any of the first nine policies in the list by pressing the corresponding key on a touch tone telephone. The first policy corresponds to the 1 key on a telephone, and the ninth policy corresponds to the 9 key on a telephone.

To change the position of a policy, check the check box next to it, then click the up arrow button or the down arrow button to move it up or down in the list.

Associating Radios with a User

Associating radios with a user causes the radios that you choose to appear as options on the PMC for the user. In addition, you can choose whether channel selectors and controls are accessible for each radio that is assigned to the user.

You must have Cisco IPICS administrator privileges to associate radios with users and to configure channel selector and control privileges.

For information about configuring radios that you can associate with users, see the "Managing Radios" section on page 2-41.

Note You can also associate radios with a user from the Radios window. For information, see the "Associating Users to a Radio From the Radios Window" section on page 2-57.

Designating Radios to Associate with a User

To associate radios channels with a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions to display the Associations window for the user with whom you want to associate channels:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list appears dimmed if you do not check a user or if you check more than one user.

Step 3 In the Associations window, click the **Radios** tab.

This tab shows a list of the radios that are associated with the user and provides information about each radio.

Step 4 Click **Add**.

The Search Results window appears.

Step 5 In the Search Results window, locate one or more radios with which to associate with this user by optionally specifying search criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-14.

Step 6 In the Search Results window, check the check box next to each radio that you want to associate with this user and then click **OK**.

The radios that you choose appear in the list of associated radios.

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

Designating Radio Permissions

A Cisco IPICS administrator can designate the following permissions for each radio that is associated with a user. The permissions apply only to the radio that you are configuring.

- Channel Selector Permissions—Enables the user to communicate on the channels that you specify on the radio that you are configuring.

- Control Function Permissions—Enables the user to user the controls that you specify on the radio that you are configuring.

If you do not designate any channel selectors or controls, the user can listen to channels on the radio, but cannot change (retune) channels or control any radio functions.

To designate permissions for a radio that is associated with a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions to display the Associations window for the user with whom you want to associate channels:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list appears dimmed if you do not check a user or if you check more than one user.

Step 3 In the Associations window, click the **Radios** tab.

Step 4 Check the check box next to the radio for which you want to designate permissions.

Step 5 To designate the channels that a user can select from the radio, take these actions:

a. From the Radio Permissions drop-down list, choose **Channel Selector Permissions**.

The User Radio Permissions window displays. This window shows the following information:

– Available Channel Selectors list—Channels that are configured for the radio

- Permitted Channel Selectors list—Channels on which the user can communicate, or on which the user will be able to communicate after you click **Save**

b. Take any of these actions:

- To move a channel from the one list to the other, click the channel to highlight it and then click > or <. Or, double-click the channel.
- To move several channels from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the channels and then click > or <.
- To move all channels from one list to the other at one time, click >> or <<.

c. Click **Save** to save your changes.

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

Step 6 To designate the controls that a user can access on the radio, take these actions:

a. From the Radio Permissions drop-down list, choose **Control Function Permissions**.

The User Radio Permissions window displays. This window shows the following information:

- Available Control Functions list—Controls that are available on the radio
- Permitted Control Functions list—Controls that the user can use, or that the user will be able to use after you click **Save**

b. Take any of these actions:

- To move a control function from the one list to the other, click the channel to highlight it and then click > or <. Or, double-click the control function.
- To move several control functions from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the control functions and then click > or <.
- To move all control functions from one list to the other at one time, click >> or <<.

c. Click **Save** to save your changes.

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

Managing Ops Views for a User

Managing ops views for a user involves these activities:

- Choosing an Ops View to Which a User Belongs, page 3-38
- Associating Ops Views with a User, page 3-39

Choosing an Ops View to Which a User Belongs

A user can belong to only one ops view. To specify this ops view, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 In the User Name column, click the link for the user with which you want to associate an ops view.

Step 3 Choose the **General** tab.

Step 4 Choose the ops view to which the user group belongs from the Belongs To drop-down list in the Ops Views area.

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

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

Associating Ops Views with a User

You can specify one or more ops views that can access a particular user.

To see the ops views that can access a user, from the User Management drawer in the Cisco IPICS Administration Console, click **Users**; then, choose the **General** tab, and look at the Accessible To list in the Ops Views area.

To specify the ops views that can access a particular user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions to associate ops views with a user:

- Click the link for the user in the User Name column; then, click the **General** tab, and then click **Edit** in the Ops View area.
- Check the check box to the left of the User Name of the user; then, choose **Ops Views** from the Associate drop-down list at the bottom right of the Users window.

Note The **Associate** button appears dimmed if you do not check a user or if you check more than one user.

The Ops View to User Association window displays. This window shows the following information:

- Available Ops Views—Ops views that have been configured in Cisco IPICS and that can be associated with the user
- Associated Ops Views—Ops views that are associated with the user or that will be associated with the user after you click **Save**

Step 3 Take any of these actions:

- To move an ops view from the one list to the other, click the ops view to highlight it and then click > or <. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the ops views and then click > or <.

- To move all ops views from one list to the other at one time, click >> or <<.

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

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

Managing Prompts for a User

If you are using the policy engine, a user can have an associated spoken name prompt. This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface.

The prompt field in the Users window indicates whether a spoken name prompt is recorded. You can record and manage the spoken name prompt for a user by clicking the **Not Recorded** or the **Recorded** link for the user in the prompt column.

When you click a link in the Prompt column, the Spoken Names window displays. If you clicked **Not Recorded**, the system provides the ability to record the prompt for the first time. If you clicked **Recorded**, the system provides the ability to rerecord the prompt. For instructions about how to record or rerecord a prompt, see the "Recording a Spoken Name Prompt" section on page 8-26.

Viewing Information about VTGs in which a User is a Participant

You can view a list of VTGs in which a user is a participant, and you can view the status of those VTGs. A user becomes a participant of a VTG in the following ways:

- A Cisco IPICS dispatcher adds the user to a VTG
- A Cisco IPICS dispatcher adds a user group that includes the user to the VTG

For related information, see Chapter 4, "Performing Cisco IPICS Dispatcher Tasks."

To view a list of VTGs in which a user is a participant, perform the following procedure:

Procedure

Step 1 Take either of these actions to display the Associations window for the user for whom you want to view associated VTGs:

- Click the link for the user in the User Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name; then, click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list appears dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Virtual Talk Groups** tab.

This tab shows the VTGs that are associated with the user and the status of each VTG.

Managing User Status

Managing the status of a user can involve specifying whether a user can access Cisco IPICS or removing a user from the system. For detailed information about managing user status, see the following sections:

- Changing User Status, page 3-41
- Locking or Unlocking a User Account, page 3-42
- Recovering a Deleted System Administrator User, page 3-43
- Deleting a User, page 3-44

Changing User Status

A user can have either of these statuses:

- Enabled—User can log in to Cisco IPICS from an end device (PMC, Cisco Unified IP Phone, and dial-in phone).

- Disabled—User cannot log in to Cisco IPICS from any end device (PMC, Cisco Unified IP Phone, and dial-in phone).

  If you disable a user who is currently logged in to Cisco IPICS, that login session is terminated automatically.

You can change the status of a single user or you can change the status of several users at one time.

To determine the current status of a user, access the User Management drawer, click **Users**, and look at the information in the Status column for the user.

To change the status of a user or users, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions:

- Click the link for the user in the User Name column to display the User Management window for the user, and click **Enable** or **Disable**.

  The **Enable** or **Disable** button appears at the bottom left of the user management window. The name of the button depends on the current status of the user.

- Check the check box next to each user whose status you want to change; then, choose the desired action (**Enable Users** or **Disable Users**) from the Change Status drop-down list.

Locking or Unlocking a User Account

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

A user account can be locked in the following ways:

- By the user exceeding the designated number of invalid login attempts when the Cisco IPICS administrator has configured user lockout. For more information, see Chapter 2, “Performing Cisco IPICS System Administrator Tasks.”.

- When a Cisco IPICS operator locks the user account as described in this section.

A Cisco IPICS operator must unlock a locked user account before the user can log in to Cisco IPICS.

Note Only the operator or All roles can unlock a user account as described in this section. If there is no user with these roles available to access Cisco IPICS (because, for example, they are locked themselves), you can use the enableuser command to unlock a user account. For more information about the enableuser command, refer to *Cisco IPICS Troubleshooting Guide, Release 2.1(1)*.

To lock or unlock a user account, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions:

- Click the link for the user in the User Name column to display the User Management window for the user, and click **Lock** or **Unlock**.

  The **Lock** or **Unlock** button appears at the bottom of the user management window. The name of the button depends on the current status of the user account.

- Check the check box next to each user whose status you want to change; then, choose the desired action (**Lock Account** or **Unlock Account**) from the Change Status drop-down list.

Recovering a Deleted System Administrator User

You can recover a deleted system administrator user ID by logging in as an operator and creating a new system administrator user ID.

Note You must have operator privileges to recover a deleted system administrator user ID.

To recover the system administrator role, perform the following procedure:

Procedure

Step 1 Log in to the server by using the operator user name and password.

Step 2 From the User Management drawer in the Administration Console, click **Users**.

Step 3 Click **Add**.

Step 4 In the required fields, which are indicated by an asterisk, enter the user information.

Step 5 From the Roles drop-down list box, choose **System Administrator** or **All** for the user role.

The new user appears in the SYSTEM ops view and can perform administrative tasks.

For more detailed information about adding a new user, see the "Adding a User" section on page 3-6.

Deleting a User

If a user is no longer needed, you can delete it from Cisco IPICS. You can delete a single user or you can delete several users at one time.

If you delete a user who is logged in to Cisco IPCS or who has active connections to Cisco IPICS (for example, a user who is associated with an active VTG), Cisco IPICS disables the user and then removes the user.

To delete a user or users, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Check the check box next to each user 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 the user or users, click **Cancel**.

Managing User Groups

A user group is a logical grouping of users. When a Cisco IPICS dispatcher adds a user group to a VTG, all users in that group become participants in the VTG.

This section describes the following user group management activities:

Understanding the User Groups Window

The User Groups window lists information about each of the user groups that you have added in Cisco IPICS. It also provides the ability to perform several user group management functions.

To display the User Groups window, access the User Management drawer and click **User Groups**.

Table 3-8 describes items in the User Groups window.

Table 3-8 Items in the User Groups Window

Items	Description	Reference
Filters		
Name field	Provides the ability to display only those users whose user name, first name, or last name begins with the character string that you enter (characters are not case-sensitive)	See the "Using Search Windows" section on page 1-14
Ops View drop-down list	Provides the ability to display only those users who are associated with ops views that match the information that you choose	
Go button (in Users area)	Displays users according to the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of users	
User Group Information		
User Group Name field	Name assigned to the user group	See the "Adding a User Group" section on page 3-47
Ops View field	Ops view to which the user group belongs	See the "Managing Ops Views for a User Group" section on page 3-50

Table 3-8 Items in the User Groups Window

Items	Description	Reference
Add button	Provides the ability to add a new user group	See the "Adding a User Group" section on page 3-47
Copy button	Provides the ability to copy information from an existing user group when you add a new user group	
Delete button	Provides the ability to delete a user group	See the "Deleting a User Group" section on page 3-54
Associations button	Displays the Associations window for a user group	See the "Viewing Information about VTGs in Which a User Group is a Participant" section on page 3-53
Display Controls		
Rows per page drop-down list	Specifies how many rows of users are included in a users list page	See the "Navigating Item Lists" section on page 1-16
Page field	Displays users on a specific page	
|< (First page) button	Displays the first page of the users list	
< (Previous page) button	Displays the previous page of the users list	
> (Next page) button	Displays the next page of the users list	
>| (Last page) button	Displays the last page of the users list	

Adding a User Group

Adding a user group makes it available to Cisco IPICS.

If you add a user group that belongs to the same ops view or that has the same members as an existing user group, you may find it convenient to start by copying the information of the existing user group. When you copy such information, Cisco IPICS opens a New User Group area, and enters information that is stored for the existing user group, except the user group name.

You may find it useful to create and name user groups according to location (for example, South Side users) or function (for example, Translators).

To add a new user group, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the Manage Users: User Groups area, take either of these actions:

- To add a user starting with a blank New User window, click **Add**.
- To add a user group starting with a New User window that includes information based on an existing user group, check the check box next to the existing user group and then click **Copy**.

Note The **Copy** button appears dimmed if you do not check an existing user group or if you check more than one existing user groups.

The New User Group area displays. If you clicked **Copy**, this window includes information from the existing user group, except for the user group name.

Step 3 In the User Group Name field, enter a name for this user group.

The name can include alphanumeric characters, spaces, and any of these special characters: . , – ‘ # ( ) / :_.

In the Description field, enter a description for the user group.

Step 4 From the Ops View drop-down list, choose the ops view to which this user group belongs.

Step 5 Perform the tasks that are described in Table 3-9, as needed.

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

Table 3-9 Tasks for Adding a Cisco IPICS User

Task	Reference
In the General tab, specify the ops views that can access this user group	See the "Managing Ops Views for a User Group" section on page 3-50
After you save the user group, in the Members tab, specify users that are members of this user group	See the "Adding Members to a User Group" section on page 3-49.

Step 6 Click **Save** to save your changes.

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

Adding Members to a User Group

A user who you add to a user group becomes a *member* of that user group. A user group can have an unlimited number of members, and a user can be a member of an unlimited number of user groups.

To add members to a user group, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the User Group Name column, click the link for the user group to which you want to add members.

Step 3 Choose the **Members** tab.

This tab displays the following information for each member of this user group:

- User Name—User name assigned to the user
- Last Name—Last name of the user
- First Name—First name of the user
- End Device Status—Can display these icons:

  -  —Audio of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk or listen in a channel or VTG
  -  —Microphone of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk in a channel or VTG
- Status—Indicates whether a user is enabled or disabled
- Account Status—Shows if a user account is locked or available

Moving a user from the Group Members list to the Available Users list removes that user from the user group.

The Search Results window appears.

Step 4 In the Search Results window, locate one or more users to add to this user group by optionally specifying filter criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-14.

Step 5 In the Search Results window, check the check box next to each user that you want to add to this user group and then click **OK**.

The users that you choose appear in the list of members.

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

Managing Ops Views for a User Group

Managing ops views for a user group involves these activities:

- Choosing an Ops View to which a User Group Belongs, page 3-51
- Associating Ops Views with a User Group, page 3-51

Choosing an Ops View to which a User Group Belongs

A user group can belong to one ops view. To specify this ops view, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the User Group Name column, click the link for the user group with which you want to associate an ops view.

Step 3 Choose the **General** tab.

Step 4 Choose the ops view to which the user group belongs from the Belongs To drop-down list in the Ops Views area.

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

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

Associating Ops Views with a User Group

You can specify one or more ops views that can access a particular user group.

To see the ops views that can access a user group, from the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**, click the link for the user group, and look at the Accessible To list in the Ops Views area.

To choose the ops views that can access a particular user group, perform this procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 Take either of these actions to associate ops views with a user group:

- In the User Group Name column, click the link for the user group, click the **General** tab; then, click **Edit** in the Ops View area.

- Check the check box to the left of the User Group Name of the user group; then, click **Associate Ops Views** at the bottom right of the User Groups window.

Note The **Associate Ops Views** button appears dimmed if you do not check a user group or if you check more than one user group.

The Ops View to User Association window displays. This window shows the following information:

- Available Ops Views—Ops views that have been configured in Cisco IPICS and that can be associated with the user group
- Associated Channels list—Ops views that are associated with the user group or that will be associated with the user group after you click **Save**

Step 3 Take any of these actions:

- To move an ops view from the one list to the other, click the ops view to highlight it and then click > or <. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the ops views and then click > or <.
- To move all ops views from one list to the other at one time, click >> or <<.

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

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

Changing the Name of a User Group

You can change the name of a user group at any time. To do so, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the User Group Name column, click the link for the user group whose name you want to change.

Step 3 Choose the **General** tab.

Step 4 In the User Group Name field, enter a new name for this user group.

The name can include alphanumeric characters, spaces, and any of these special characters: . , – ‘ # ( ) / :_.

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

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

Viewing Information about VTGs in Which a User Group is a Participant

You can view a list of VTGs in which a user group is a participant, and you can view the status each VTG. A user group becomes a participant in a VTG when a Cisco IPICS dispatcher adds the user group to a VTG.

For related information, see Chapter 4, “Performing Cisco IPICS Dispatcher Tasks.”

To view a list of VTGs in which a user group is a participant, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 Take either of these actions:

- In the User Group Name column, click the link for the user group; then, click **Associations** at the bottom of the Users window.
- Check the check box to the left of the User Group Name of the user group; then, click **Associations** at the bottom of the User Groups window.

The following information displays for each VTG in which the user is participating:

- VTG Name—Name of the VTG
- Status—Whether the VTG is active or inactive

Deleting a User Group

You can delete a user group when you no longer need it to organize users. You can delete a single user group or you can delete several user groups at one time.

To delete a user group, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

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