CHAPTER 2

Performing Cisco IPICS System Administrator Tasks

The Cisco IPICS system administrator is responsible for installing the Cisco IPICS software and for setting up Cisco IPICS resources, including servers, routers, multicast addresses, locations, and PTT and radio channels. The system administrator also manages the Cisco IPICS licenses and IDC versions, monitors the status of the system, reviews log files, as needed, and creates operational views.

In addition, the system administrator is responsible for managing radios and radio descriptors, managing optional high availability, and performing backup and restore operations. For more information, see Chapter 9, "Managing Radios and Radio Descriptors," Chapter 10, "Configuring and Managing Cisco IPICS High Availability," and Chapter 11, "Performing Cisco IPICS Database Backup and Restore Operations."

Most of the system administrator activities that you perform are accessible from the Administration Console Configuration and Administration drawers. To access these drawers, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-10, then choose the **Configuration** or the **Administration** drawer.

Note You must be assigned the system administrator role to access the Configuration and Administration drawers.

The following sections describe many of the system administrator activities that you can perform from the Cisco IPICS Administration Console:

- Managing Activity Log Options Per Ops View, page 2-88
- Managing Cisco IPICS Options, page 2-89
- Managing IDC Versions, page 2-101
- Managing IDC Alert Tones, page 2-104
- Managing the IDC Installer, page 2-108
- Managing IDC Regions, page 2-110
- Configuring LDAP, page 2-112

For information about managing operational views in the Ops Views window, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

For information about managing database backup and restore operations in the Database Management window, see Chapter 11, "Performing Cisco IPICS Database Backup and Restore Operations."

Managing PTT Channels and Channel Groups

A PTT channel, also referred to as a channel, is a communications path that allows users to communicate with each other. A Cisco IPICS channel defines and describes the specific content stream of the channel regardless of the source of that content. Channel connections distinguish one content stream from another, and are determined by location.

A channel carries traffic to and from a VTG, a land mobile radio (LMR) gateway, an IDC, and an IP phone. Remote IDC users can connect to a channel by using a unicast SIP connection to an RMS component.

A channel can also refer to a radio control interface (radio or radio channel), which also has an audio stream. For information about managing radios in Cisco IPICS, see Chapter 9, "Managing Radios and Radio Descriptors."

A channel group is a logical grouping of PTT channels. Channel groups allow Cisco IPICS dispatchers to work with multiple PTT channels efficiently. For example, instead of dragging individual PTT channels one at a time to set up a VTG, a Cisco IPICS dispatcher can drag a channel group to move all associated channels in the group. A PTT channel can be in as many channel groups as you require.

As a Cisco IPICS system administrator, you can perform the following PTT channel and channel group management tasks:

Channel Management Tasks

- Adding a PTT Channel, page 2-5
- Viewing and Editing Channel Details, page 2-5
- Changing the Status of a PTT Channel, page 2-12
- Understanding Association Attribute Behaviors, page 2-13
- Associating PTT Channels to Ops Views, page 2-14
- Associating Users to PTT Channels, page 2-15
- Associating Radio Control Signals to PTT Channels, page 2-16
- Viewing Channel Associations, page 2-17
- Deleting a PTT Channel, page 2-18

Channel Group Management Tasks

- Adding a Channel Group, page 2-20
- Viewing and Editing Channel Group Details, page 2-21
- Viewing Channel Group Associations, page 2-23
- Removing a PTT Channel from a Channel Group, page 2-23
- Associating Ops Views to Channel Groups, page 2-24
- Deleting a Channel Group, page 2-25

You perform the PTT channel management tasks in the Channels and Channel Groups windows, located in the Configuration drawer of the Administration Console. For more information about these windows, including how to access them, see the "Understanding the Channels Window" section on page 2-3 and the "Understanding the Channel Groups Window" section on page 2-19.

Understanding the Channels Window

The Channels window lists information about each of the channels that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS channels and general information for each channel. By default, this area displays all channels, but you can choose to display only channels that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of channels that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to perform several channel management functions. To display the Channels window, access the Configuration drawer; then click **Channels**.

Table 2-1 describes the items in the Channels window.

Table 2-1 Items in the Channels Window

Item	Description	Reference
Filter		
Channel Name field	This field allows you to display only channel names that include the character string that you enter (characters are not case-sensitive).	To limit the display of channels or to display a certain channel, enter the desired search criteria in the filter field; then, click **Go**.
Ops View drop-down list	This field allows you to display only channels for which the associated ops view matches the information that you choose.	
Go button	Click this button to display channels by the filters that you choose.	
Clear Filter button	Click this button to remove filter selections and display an empty list of channels. Click the **Channels** link again to display the full list of entries.	
Channel Information		

Table 2-1 Items in the Channels Window (continued)

Item	Description	Reference
Channel Name field	This field indicates the unique identifier that is assigned to the channel.	See the "Viewing and Editing Channel Details" section on page 2-5 and the "Adding a PTT Channel" section on page 2-5
Ops View field	This field indicates the ops view to which the channel belongs.	See the "Associating PTT Channels to Ops Views" section on page 2-14
Secure field	This field indicates whether the channel is secure.	See the "Viewing and Editing Channel Details" section on page 2-5
VTG field	This field indicates whether the channel is allowed in a Virtual Talk Group (VTG).	See the "Viewing and Editing Channel Details" section on page 2-5 and the "Adding a PTT Channel" section on page 2-5
Users field	This field indicates whether the channel is allowed to be associated to users to affect all endpoints such as the IDC and IP phone.	
Channel Status field	This field indicates whether the channel is enabled, disabled, or active.	See the "Changing the Status of a PTT Channel" section on page 2-12
Prompt field	This field indicates whether a spoken name prompt is recorded for the channel. This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface. You can record the spoken name prompt for a user by clicking the **Not Recorded** or the **Recorded** link in the Prompt column. When you click a link in the Prompt column, the Spoken Names window displays.	See Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"
Add button	Click this button to add a new channel in Cisco IPICS.	See the "Adding a PTT Channel" section on page 2-5
Delete button	Click this button to delete the specified channel(s).	See the "Deleting a PTT Channel" section on page 2-18
Change Status drop-down list	Choose from the enable or disable option to change the status of a channel.	See the "Changing the Status of a PTT Channel" section on page 2-12
Associations button	Click this button to view associations for the specified channel.	See the "Associating Users to PTT Channels" section on page 2-15, the "Viewing Channel Associations" section on page 2-17, and the "Associating Radio Control Signals to PTT Channels" section on page 2-16
Display Controls		
Rows per page drop-down list	Specifies the number of rows of channels that are included in a channels list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays channels on a specific page.	
|< (First page) button	Displays the first page of the channels list.	
< (Previous page) button	Displays the previous page of the channels list.	
> (Next page) button	Displays the next page of the channels list.	
>| (Last page) button	Displays the last page of the channels list.	

Adding a PTT Channel

Adding a PTT channel makes it available for use by Cisco IPICS.

Before you add a PTT channel, configure locations as described in the "Adding a Location" section on page 2-30.

To add a new channel, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Configuration > Channels** window.

Step 2 In the Channels window, click **Add**.

The General tab for a new channel displays.

Step 3 Follow the steps in the "Viewing and Editing Channel Details" section on page 2-5.

Step 4 Enter appropriate information in the Ops Views fields as described in Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

This field is optional.

Step 5 Click **Save** to add the channel without exiting the current window.

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

Viewing and Editing Channel Details

You can view and edit information for any channel.

To view or edit channel details, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 In the Channel Name column, click the link for the channel for which you want to view or change information.

The General tab for the selected channel displays. This window contains general information for that channel. Table 2-2 provides descriptions of the fields in the General tab.

Note If an endpoint, such as the IDC or dial engine, does not support the attributes that are described in Table 2-2, the attributes do not display in the General tab of the Channels window.

Table 2-2 General Tab Fields in Channels Window

Field	Description
Channel Information	
Name	This field represents the name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: ". , – ' # ( ) / :_". Choose a unique and recognizable name that accurately describes the PTT channel. It is often helpful to name the PTT channel according to the department or organization that use it, or for a particular geographic region (for example *Fire Department* or *North Area*). **Note** The IDC truncates the channel name if the name includes more characters than the IDC can display.
Short Name	This field represents the condensed name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: ". , _ ' # ( ) / :_".
Description	(Optional) This field allows you to enter a description for this channel.
Secure Channel	This drop-down list allows you to specify whether this channel is a secure channel. This field is for reference only and should be set to reflect the configuration of the channel in your network. Changing this setting does not affect the security configuration of the channel. **Note** This field displays as read-only if the channel is a participant in an active VTG, an active IDC user is associated with this channel, or if a user has activated this channel via an IP phone or PSTN phone. To make the field editable, either disable the channel, or deactivate the VTG in which the channel is a participant.
Allow association to users	This check box allows you to indicate whether this channel is available to all Cisco IPICS users. Use this option to prevent certain channels from being associated to users. If the channel is configured to disallow association to a user (attribute check box is not checked), the channel does not display as available to users in the User window and it is not available on the IDC. In addition, the User tab, in the channel Association window, does not display. **Note** If you change the channel status such that a channel that was previously associated with a user is no longer associated with a user, Cisco IPICS automatically removes the channel associations from the users. This check box is checked by default upon creation of the channel.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Allow use in VTGs	This check box allows you to indicate whether this channel is an available resource for participation in a VTG. Use this setting to prevent certain channels from being included in a VTG. For example, an IDC user who interacts with a another user may wish to hear all the call progress tones that the other user's handset generates, to give feedback when a radio channel is available. These types of progress tones can be assigned to this channel. Because the tones can be disruptive, however, you might not want to add this type of channel to a VTG with a large group of users; therefore, when you create this channel, you would disallow its use in VTGs. If the channel is configured to disallow this channel in a VTG (attribute check box is not checked), the channel does not display in the Resources area of the VTGs in the VTG Management window and is not available for participation in VTGs. The channel can, however, display as available for association to users and user groups, in the User and User Groups windows. If you change the channel such that it is no longer allowed in a VTG, the channel remains active in any current VTG to which it is a participant. However, the channel is not allowed to join any other VTG. **Note** This attribute is checked by default upon creation of the channel.
Status *Display only*	This field displays one the following channel states: • Active—Channel in use by an active VTG. • Enabled—Channel is available (channel can be connected to a VTG) and IDC clients can use the channel. • Disabled—Channel is not in use and IDC clients cannot use the channel (it is dimmed), and the channel cannot be connected to a VTG. You can still modify connection attributes on the channel.
Media Connection Assignments	
Type	This field specifies the type of connection that Cisco IPICS and devices use to connect to this channel when connecting from the corresponding location. Choose one of the following options from the drop-down list: • **Multicast**—If you choose a multicast connection type, you must also configure the location, IP address, port. and codec fields for the multicast connection. For more information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34. • **Pooled Radio**—If you choose a pooled radio device type, you must also choose a descriptor from the Descriptor drop down list and a channel selector from the Channel Selector drop-down list. The Pooled Radio options appear only if you have enabled one or more serial control radios to serve as a pooled resource and have enabled one or more channel selectors for a pooled radio. For more information, see the "Managing Radios" section on page 9-1. • **ISSIG**—If you choose an ISSIG (ISSI Gateway) device type, you must also configure the Multicast address for the channel media (media address) and the port for channel media. You must also choose the ISSI Gateway and selector (P25 group on which to talk) to use for the channel. The ISSIG options appear only if you have configured one or more ISSI Gateways.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Location	This field displays when you choose a multicast connection type from the Type drop-down list. Channels or users who are associated with the same location are reachable within a multicast network boundary. Therefore, users who are in the same multicast domain are also in the same Cisco IPICS location. Remote, SIP-based users are not in the same location as multicast users. Remote users connect by establishing connectivity with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user. **Note** Channels achieve media connectivity by being mapped to a multicast address and port in a location. A channel can be assigned to multiple locations. In this case, a channel can have more than one media connection. The media connection count in the **Serviceability > Dashboard** window reflects the total number of media connections. See the "Viewing the Information in the Dashboard Window" section on page 12-1 for more information about the Dashboard window. If the network is configured so that the channel can be accessed by users in every location, set this value to **All**. See the "Managing Locations" section on page 2-25 for more detailed information about how to configure locations.
Address	This field displays when you choose a multicast connection type from the Type drop-down list. This field specifies the multicast address, in the corresponding location, that is used to connect to this channel. **Note** Cisco strongly recommends that you configure only multicast IP addresses that are in the 239.192.0.0 to 239.251.255.255 range. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34. Two channels in the same location cannot have the same multicast address. See the "Managing Locations" section on page 2-25 for more detailed information about locations.
Port	This field displays when you choose a multicast connection type from the Type drop-down list. This field specifies the multicast address port number, in the corresponding location, that is used to connect to this channel. **Note** This value must be an even number in the range of 21000 through 65534. Cisco IPICS does not allow the configuration of ports below 21000 or any odd ports.
Codec	This drop-down list allows you to choose the codec (G.711 or G.729) that is used by this connection. Use G.711 if this connection should be available to Cisco Unified IP Phone users or if it is part of a VTG. Use G.711 or G.729 if this connection is available to IDC users. G.729 requires digital signal processor (DSP) resources for transcoding. **Note** You cannot edit the codec and media connection attributes if users who are associated to the channel are logged in to an IP phone or an IDC. For more information about codecs, see the *Solution Reference Network Design (SRND) for Cisco IPICS* document.
Radio	This drop-down list displays when you choose a tone radio device type from the Type drop-down list. It allows you to choose a configured tone control radio.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Descriptor	This drop-down list displays when you choose a pooled radio device type from the Type drop-down list. It allows you to choose a serial control radio that has been enabled to serve as a pooled device.
Channel Selector	This drop-down list displays when you choose a pooled radio or tone radio device type from the Type drop-down list. It allows you to choose a channel selector. **Note** You cannot configure multiple channels on the same radio with the same channel selector. However, a channel can have more than one radio connection for a given radio. That is, a radio has more than one control sequence to tune to the same content. For more information about radios, see Chapter 9, "Managing Radios and Radio Descriptors." Each channel can have a specific set of signaling (over-the-air) tones that need to be broadcast over the radio. When a user is associated with the channel, any signaling tones that are defined for that channel are available for use by the IDC. **Tip** When you define channel selectors, consider the different actions that users may want to perform on the channel, such as tuning the radio or beginning a transmission over-the-air. These actions determine the commands that are sent to the radio when the user invokes the action by pressing the button on the channel. For more information about the IDC, see *Cisco IPICS Dispatch Console User Guide*.
Ops Views	
Belongs To	This drop-down list allows you to choose the ops view to which you want to associate this channel. See the "Associating PTT Channels to Ops Views" section on page 2-14 for detailed information. **Note** To associate a channel to an ops view, you must belong to the SYSTEM ops view. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Accessible To	This drop-down list allows you to choose the ops views to which you want this channel to be accessible. See the "Associating PTT Channels to Ops Views" section on page 2-14 for information about how to associate ops views to channels. **Note** This option appears only after you save a channel. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	Click this button to make this channel accessible to other ops views. **Note** This button does not display if there are no additional ops views configured in Cisco IPICS. See the "Associating PTT Channels to Ops Views" section on page 2-14 for more information. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

Step 3 To view the IDC details for this channel, click the **IDC** tab.

The Client tab for the selected channel displays. This window contains IDC information for the selected channel. Table 2-3 provides descriptions of the fields in the IDC tab.

Table 2-3 IDC Tab Fields in Channels Window

Field	Description
IDC	
RX Mute During PTT	The following values affect how the receive mute functionality is configured on the IDC for this channel. • None—When PTT is engaged on this channel, this channel is not muted when it receives traffic. • All—When PTT is engaged on this channel, incoming audio traffic is muted on all resources. • Channel—When PTT is engaged on this channel, incoming audio is muted for this channel only. This value is the default.
Enable Voice Activity Detection (VAD)	When you enable VAD on Cisco IPICS, the IDC only sends voice traffic when it detects a voice packet on this channel. When this attribute is set to true (attribute check box is checked) on a channel, VAD is used by the IDC when communicating with the channel. By default, this attribute is set to false (attribute check box is not checked).
Allow Latch	When set to true (attribute check box is checked) on a channel, the user can use latch to lock in the channel. By default, this attribute is set to false (attribute check box is unchecked).
Listen Only	When set to true (attribute check box is checked), the user can hear, but cannot talk, on the channel.
Channel Color	This attribute specifies a color tag that you can choose from a drop-down list. This setting identifies specific channels by using predefined colors for the background text that appears on the channel. You configure the color by choosing from the options in the drop-down list. **Note** If you do not want the channel to be tagged with a color, you can choose **Not colored** from the drop-down list.
Channel Region	From the drop-down list, choose the region in which this channel should appear on the IDC. For information about configuring IDC regions, see the "Managing IDC Regions" section on page 2-110.

Step 4 To view channel associations, choose a channel in the Channels window, then click the **Associations** button that displays at the bottom of the window.

Step 5 To view channel associations, from the Associations window take one of the following actions:

- Click the **Users** tab—This tab displays the Cisco IPICS users who are associated to this channel.

  The users who are currently associated to this channel display. The Users window lists information about each of the users who are associated to the channel.

Table 2-4 describes the items in the Users window.

Table 2-4 Items in the Users Window

Item	Description
User Name field	This field specifies the unique identification name assigned to the user.
Last Name field	This field specifies the last name of the user.
First Name field	This field specifies the first name of the user.
Status field	This field indicates whether the user is enabled or disabled.
Association Attributes	
Latchable field	This field indicates whether the user can latch (lock in) channels on end devices.
Disable Audio field	This field indicates whether audio is disabled on end devices.
Listen Only field	This field indicates that the user is restricted to listening only on the channel; no transmission is allowed.

Note User association values are appended with a superscript (1) if they are configured as a customized value. See the "Understanding Association Attribute Behaviors" section on page 2-13 for more information about association attribute behaviors.

You can associate additional users to the channel, by performing the steps in the"Associating Users to PTT Channels" section on page 2-15.

- Click the **Virtual Talk Groups** tab—This tab displays the VTGs in which this channel participates.
- Click the **Signals** tab—This tab lets you associate signals to channels.

  For more detailed information, see the "Associating Radio Control Signals to PTT Channels" section on page 2-16.

Step 6 From the Users tab, you can change the IDC status for a user by checking the check box next to selected users.

The Change End Device Status drop-down list becomes active.

Note The Change End Device Status drop-down list becomes available only after you have checked the check box next to one or more user names. If you do not check the check box, the Change End Device Status drop-down list appears dimmed.

Step 7 From the Change End Device Status drop-down list, choose one of the available options:

- **Allow Latch**—User can latch, or lock in, channels
- **Disallow Latch**—User cannot latch channels
- **Set Listen Only**—User can only listen on the channel; transmission is not allowed
- **Unset Listen Only**—User can listen and transmit on the channel
- **Enable Audio**—Audio is enabled
- **Disable Audio**—Audio is disabled

Note Be aware that when you choose the Disable Audio feature from any location in the Cisco IPICS server, the audio on all end user devices (IDC, IP phones), except for radios, is disabled.

Changing the Status of a PTT Channel

Cisco IPICS allows you to change the status (enable/disable) of a channel from either the main Channels window, or in the individual channel configuration windows.

The status of a channel affects whether the channel is available to the IDC, IP phones, and dialed-in users, or whether the channel can connect to a VTG. If the channel is disabled, it cannot be connected to a VTG.

In addition, a channel can be in the *active* state. Cisco IPICS puts a channel into this state automatically when it is in use by an active VTG in the system. When a channel is in the active state, you must deactivate the referencing VTG or disable the channel before you can change any of its media connection assignments.

For more information about the IDC, see *Cisco IPICS Dispatch Console User Guide* for this release.

A channel can be configured as enabled or disabled.

You can change the status of a single channel, or you can change the status of several channels at one time.

To determine the current status, access the Configuration drawer, click **Channels**, and look at the information in the Status column for the channel.

To change the status of a channel from the main Channels window, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Take either of these actions:

- Click the link for the channel in the Channel Name column to display the configuration window for the channel, click **Enable** or **Disable**; then, click **Save**.

  The **Enable** or **Disable** button appears at the bottom of the channel configuration window. The name of the button depends on the current status of the channel.

- In the Channels window, check the check box next to each channel for which you want to change the status, then choose the desired action (**Enable** or **Disable**) from the Change Status drop-down list.

Understanding Association Attribute Behaviors

Users, channels, and VTGs have attributes that control their behavior. In some cases, these resources may have the same attribute behaviors, so that when you associate channels to users, or users to VTGs, the system determines the resulting IDC behavior by how the attributes are configured for each associated resource. For an example of association attribute behaviors, see the "User-Channel Association Example" section on page 2-13.

Cisco IPICS allows you to override the resulting behaviors for specific associations. When you modify channel or user attributes that are part of an association, the resulting behavior depends on the attribute settings for users within the association. Typically, when resources are part of an association, any attribute changes to the resources also apply to the resource and associations within that resource. Resource attributes may have different settings when they are not part of an association.

The following section provides an example of some of the expected system behaviors when you configure user, channel, and VTG associations.

Changes to channel, user, or VTG attributes that are also present in associations, behave differently, depending on the override status. If the association is not overridden you are prompted to remove the overrides. An example of some association attribute behaviors is described below.

Note The example in the "User-Channel Association Example" section on page 2-13 is also applicable to user-VTG associations.

To associate an ops view to a channel, see the "Associating Users to PTT Channels" section on page 2-15.

User-Channel Association Example

The following example describes different user-channel association scenarios that can be performed by a Cisco IPICS operator and a system administrator:

- User A is allowed to latch (the Allow Latch attribute check box is checked).
- Channel A is not allowed to latch (the Allow Latch check box is not checked).
- The Cisco IPICS operator associates User A to Channel A.

  The resulting behavior for this association is that User A is not allowed to latch on Channel A on the IDC. On the server side, the Allow Latch attribute displays as **No** for both the user and the channel for this association, in the Latchable column in the Associations tab.

Note This behavior results because the Allow Latch setting, for both the user and the channel, must have the same value for latching to be allowed in this association. In this example, the value for Allow Latch must be **Yes**.

- You decide to allow all users to latch on Channel A, so you change the Allow Latch attribute on the channel by checking the Allow Latch check box in the **Channels > IDC** window. Because the association settings have not been customized, Cisco IPICS automatically updates the User A-Channel A association. The IDC updates to allow latching on this channel for this association.
- The operator disallows latch on Channel A by navigating to the Association tab (for Channel A), selecting all of the users, clicking **Change End Device Status**, and selecting the Allow Latch menu item.

Cisco IPICS marks this attribute as a customized value.

Note A superscript (1) displays next to the value in the Latchable column in the Associations tab, for both the user and the channel. The superscript indicates a customized value, meaning that the previous value of the attribute in the association has been overridden.

After the IDC updates, users in this association can no longer latch on Channel A.

- You decide to allow all users to latch on Channel A and you check the Allow Latch check box in the IDC tab for the channel. Because the association had previously been marked as a customized value the system prompts you with a message stating that this action overrides the custom IDC settings for Latch.

  If you click OK to the message, the overrides are removed and latching on Channel A, for this association, is allowed on the IDC.

See the "Viewing and Editing Channel Details" section on page 2-5 for more information about the specific channel attributes.

For information about associating a channel to a user or ops view, see the "Associating Users to PTT Channels" section on page 2-15.

For more information about the IDC, see *IPICS Dispatch Console User Guide* for this release.

Associating PTT Channels to Ops Views

You can associate a channel to an ops view in the General tab of an individual window for a channel. When you associate a channel to an ops view, the channel can be seen by the users who belong to that particular ops view.

For more information about the Accessible To and Belongs To attributes for ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

To associate a channel to an ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 In the Channel Name column, click the link for the channel that you want to make accessible to an ops view.

Step 3 In the General tab, click the **Edit** button that appears in the Ops View pane.

The Ops View to Channel Association window displays the following information:

- Available Ops Views—Ops views that can be made accessible to this channel
- Associated Ops Views—Ops views to which this channel is currently accessible

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it; 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 **Ctrl+click** to select the ops views; then, click **>** or **<**.
- To move all ops views 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**.

The ops views that you chose display in the Accessible To: field in the individual window for the channel.

Step 6 To change the ops view to which this channel belongs, choose an ops view from the Belongs To: drop-down list.

Step 7 Click **Save**.

Associating Users to PTT Channels

You can associate specific users to a channel in the Associations window. When you associate channels with a user, the channels that you choose appear as options on an IDC or a Cisco Unified IP Phone that has been configured for use with Cisco IPICS.

To determine the ops views to which the channels are currently associated, access the Configuration drawer, click **Channels**, and look at the information in the Ops View column for the channels.

Note You can perform this procedure only if users have already been added in Cisco IPICS.

System administrators and operators who belong to an ops view that is associated to a channel can associate other users to the channel, and add the channel to VTGs, as long as the Allow in association to users and Allow use in VTGs check boxes are checked. See the "Adding a PTT Channel" section on page 2-5 for more information.

To associate users to channels, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Take either of these actions to display the Associations window for the channel with which you want to associate users:

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

Note The Associations button is dimmed if you do not check a channel or if you check more than one channel.

In the Associations window, make sure that the **Users** tab is selected.

This tab shows a list of the users who are associated with the channel, the status of each user, and information about attributes for devices that the user is using.

Step 3 Click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the channel by choosing criteria based on the following filters:

- User Name field—Specifies the user name of a user
- First Name field—Specifies the first name of a user
- Last Name field—Specifies the last name of a user
- Location drop-down list—Choose from a list of locations

  See the "Managing Locations" section on page 2-25 for detailed information about how to configure locations.
- Role drop-down list—Choose from a list of Cisco IPICS roles
- Ops View drop-down list—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the users in Cisco IPICS, click the **Go** button without entering any search criteria.

The results of your search criteria display in a list.

Step 5 To choose a user to associate to the channel, check the check box to the left of the user name and click **OK**.

The user that you choose displays in the user list in the Users tab.

Step 6 To change the status of an end device for a user, see Step 7 in the "Viewing and Editing Channel Details" section on page 2-5.

Step 7 To delete a user from this channel association, check the check box to the left of the user and click **Delete**.

Step 8 To view the VTGs in which the channel participates, click the **Virtual Talk Groups** tab.

If the channel participates in a VTG, the VTG name and status displays.

Associating Radio Control Signals to PTT Channels

You can associate specific radio control functions to channels in the channel Associations window. When you associate signals to channels, the specific functions that the signals perform appear as options on the IDC for that channel.

Each channel can be associated with one or more signals. Users who are associated with channels can send signals from the IDC.

You can associate signals with a channel that is not associated with a radio, such as another type of tone-controlled device. For example, you could have a Cisco IPICS PTT channel that includes an LMR gateway that is connecting to a tone-controlled device that is not a radio, such as a device that opens a gate. This type of device can interpret tones and perform specific actions.

When the IDC plays the RFC 2833 and RFC 2198 signals, the LMR gateway detects these signals (in this example, the open gate signal) and converts them into audio. This audio gets sent to the devices that open the gate that triggers them to activate. No radio is present in this scenario. The devices are directly connected to the E&M interface on the LMR gateway.

Unlike alerting tones that cannot be restricted to a specific channel, you can associate signals directly with specific channels. This flexibility gives you the ability to control the appearance of and the ability to play out signals to the appropriate channel(s).

To associate signals to channels, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Take either of these actions to display the Associations window for the channel with which you want to associate users:

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

Note The Associations button appears dimmed if you do not check a channel or if you check more than one channel.

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

This tab shows a list of the signals that are associated with the channel, and includes the short name, description, and where it originated.

Step 4 Click **Add**.

The Search Signals window displays. This window allows you to search for additional signals to associate to the channel.

Step 5 To add a signal, check the check box to the left of the signal name; then, click **OK**.

Step 6 To delete a signal from this channel association, check the check box to the left of the signal name and click **Delete**.

Step 7 To view the VTGs in which the channel participates, click the **Virtual Talk Groups** tab.

If the channel participates in a VTG, the VTG name and status displays.

Step 8 To view the users who are associated with the channel, click the **Users** tab.

To associate users to the channel, see the "Associating Users to PTT Channels" section on page 2-15.

Viewing Channel Associations

You can view channel associations by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 To view channel associations, take either of these actions:

- Click the link for the channel in the Channel Name column; then, click the **Associations** button, which appears at the bottom of each tab.

- Check the check box to the left of the Channel Name; then, click the **Associations** button at the bottom of the Channels window.

Note The Associations button appears dimmed if you do not check a channel or if you check more than one channel.

Step 3 From the Associations window, you can view the associations for the channel by clicking either of the following tabs:

- **Users**—View users who are associated with this channel and associate other users to the channel.

Note To associate other users to the channel, see the "Associating Users to PTT Channels" section on page 2-15.

- **Virtual Talk Groups**—View the VTGs in which this channel participates.
- **Signals**—View the radio signals that are associated with this channel and associate other signals to the channel.

Note To associate other signals to the channel, see the "Associating Radio Control Signals to PTT Channels" section on page 2-16.

Deleting a PTT Channel

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

To delete a channel, perform the following procedure.

Note This procedure deletes a channel even if it is in use by a VTG. If you delete an in-use channel, it becomes unavailable immediately.

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Check the check box next to each channel 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 channel(s), click **Cancel**.

Understanding the Channel Groups Window

The Channel Groups window lists information about each of the channel groups that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS channel groups and general information for each channel group. By default, this area displays all channel groups, but you can choose to display only channel groups that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of channel groups that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also provides you with the ability to perform several channel group management functions.

To display the Channel Groups window, access the Configuration drawer and click **Channel Groups**.

Table 2-5 describes the fields in the Channel Groups window.

Table 2-5 Fields in the Channel Groups Window

Field	Description	Reference
Filter		
Name field	Allows you to display only channel group names that include the character string that you enter (characters are not case-sensitive)	To limit the display of channel groups or to display a certain channel group, enter the desired search criteria in the filter field; then, click **Go**.
Ops View drop-down list	Allows you to display only channel groups for which the associated ops view matches the information that you choose	
Go button	Displays channel groups by the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of channel groups	
Channel Group Information		
Channel Group Name field	Name that is assigned to the channel group	See the "Viewing and Editing Channel Group Details" section on page 2-21 and the "Removing a PTT Channel from a Channel Group" section on page 2-23
Ops View field	Ops view to which the channel group belongs	See the "Associating Ops Views to Channel Groups" section on page 2-24

Table 2-5 Fields in the Channel Groups Window (continued)

Field	Description	Reference
Add button	Allows you to add a new channel group in Cisco IPICS	See the "Removing a PTT Channel from a Channel Group" section on page 2-23
Copy button	Allows you to copy information from an existing channel group when you add a new channel group	
Delete button	Allows you to delete a channel group	See the "Deleting a Channel Group" section on page 2-25
Associations button	Displays the Associations window for a channel group	See the "Associating Ops Views to Channel Groups" section on page 2-24 and the "Viewing Channel Group Associations" section on page 2-23
Display Controls		
Rows per page drop-down list	Specifies the number of rows of channel groups that are included in a channel groups list page	See the "Navigating Item Lists" section on page 1-13
Page field	Displays channel groups on a specific page	
|< (First page) button	Displays the first page of the channel groups list	
< (Previous page) button	Displays the previous page of the channel groups list	
> (Next page) button	Displays the next page of the channel groups list	
>| (Last page) button	Displays the last page of the channel groups list	

Adding a Channel Group

A channel group enables you to organize channels. You may find it useful to create and name channel groups according to location (for example, South Area Fire Department PTT Channel) or function (for example, Maintenance PTT Channel).

To create a channel group, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Groups window, take either of these actions:

- To add a channel group starting with a blank New Channel Group window, click **Add**.
- To copy an existing channel group, check the check box next to the existing channel group; then click **Copy**.

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

The New Channel Group window displays. If you clicked Copy, this window includes information from the existing channel group, except for the channel group name.

Step 3 In the General tab, enter information for the channel group as described in the "Viewing and Editing Channel Group Details" section on page 2-21, starting with Step 3.

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

Step 4 Click **Save** to add the channel group without exiting the current window.

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

For information about how to associate channel groups to a VTG, see the "Managing VTGs" section on page 5-2.

Viewing and Editing Channel Group Details

You can view information about and edit any channel group in your Cisco IPICS network, including adding new channel members to the channel group.

To add a new channel group, see the "Adding a Channel Group" section on page 2-20.

To view and edit channel group details, and add channel members, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group Name column, click the link for the channel group that you want to view or edit.

The General tab for channel groups displays. This window contains general information for that channel group.

Step 3 To view or update general information for a channel group, click the **General** tab. Table 2-6 provides a description of the fields in the General tab.

Table 2-6 General Tab Fields in Channel Groups Window

Field	Description
Channel Group Information	
Channel Group Name	Unique name of the channel group. The name can include alphanumeric characters, spaces, and any of these characters: ". , – ' # ( ) / :_".
Description	*Optional*. Description of the channel group
Ops View	

Table 2-6 General Tab Fields in Channel Groups Window (continued)

Field	Description
Belongs To	Name of the ops view to which you want to associate this channel group. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Accessible To	Name of the ops view to which you want this channel group to be accessible. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	Click this button to associate ops views to the channel group. See the "Associating Ops Views to Channel Groups" section on page 2-24 for detailed information. **Note** To associate a channel group to an ops view, you must belong to the SYSTEM ops view.

Step 4 To view or update members who are associated with this channel group, click the **Members** tab. Table 2-7 provides a description of the fields in the Members tab.

Table 2-7 Member Tab Fields in the Channel Groups Window

Field	Description
Channel Name	Specifies name of the channel member
Ops View	Specifies ops view to which the channel member belongs
Secure	Indicates whether the channel member is configured as a secure channel
VTG	Indicates whether the channel is configured to be used in a VTG
Users	Indicates whether the channel is configured to be associated with users
Channel Status	Indicates whether the channel is enabled or disabled

Step 5 To add additional channel members to the channel group, click the **Add** button.

The Search Channels window displays. This window allows you to search for channels to add as members by choosing criteria based on the following filters:

- Name field—Allows you to enter a channel name
- Ops View drop-down list—Allows you to choose from a list of ops views

Step 6 To search for a channel, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the channels in Cisco IPICS, click the **Go** button without entering any search criteria.

You search results display in a list.

Step 7 To choose a channel to add as a member to the channel group, check the check box to the left of the channel name and click **OK**.

The channel that you choose displays in the channel members list in the Members tab.

To view current channel group associations, see the "Viewing Channel Group Associations" section on page 2-23.

Viewing Channel Group Associations

To view channel group associations, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group Name column, click the link for the channel group for which you want to view associations.

The General tab for channel groups displays.

Step 3 To view current channel group associations, take either of the following actions:

- Check the check box of the channel group name; then click the **Associations** button.
- Click the link of the channel group; then click the **Associations** button.

Table 2-8 provides descriptions of the fields in the Associations window.

Table 2-8 Virtual Talk Groups Tab in the Associations Window

Field	Description
VTG Name	VTG to which this channel group is associated
Status	Status of the associated VTG, which includes the following designations: • Active—Channel group is a participant in an active VTG • Idle—Channel group is a member of an inactive VTG

Removing a PTT Channel from a Channel Group

When you remove a PTT channel from a channel group, the channel is no longer a part of that group. Removing a PTT channel from a channel group does not remove the channel itself from Cisco IPICS, nor does it remove the channel from any other channel group to which it belongs.

To remove a PTT channel from a channel group, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group Name column, click the link for the channel group from which you want to remove a channel.

The General tab of the channel group displays.

Note To view the associations for the channel group, click the Associations button.

Step 3 Click the **Members** tab.

Step 4 Check the check box to the left of each channel that you want to remove from the channel group.

Step 5 Click **Delete**.

Tip To delete all the channels from this channel group, check the check box at the top of the channel list and click **Delete**.

To add channel members to a channel group, see the "Viewing and Editing Channel Group Details" section on page 2-21.

Associating Ops Views to Channel Groups

You can associate specific ops views to channel groups from the Channel Groups window. When you associate an ops view to a channel group, the channel group can be seen by the users who belong to that particular ops view.

For more information about the Accessible To and Belongs To attributes for ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

To determine the ops views to which the channel group is currently associated, access the Configuration drawer, click **Channel Groups**, and look at the information in the Ops View column for the channel group.

To associate ops views to channel groups, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group name column, click the channel group that you want to associate to an ops view.

Step 3 From the General tab in the Ops View pane, click the **Edit** button.

The Ops View to Channel Group Association window displays the following information:

- Available Ops Views—Ops views that can be made accessible to this channel group
- Associated Ops Views—Ops views to which this channel group is currently accessible

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it; 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 **Ctrl+click** to select the ops views; then, click **>** or **<**.
- To move all ops views 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 associate the ops view to the channel group, click **Cancel**.

The ops views that you choose display in the Accessible To: field in the individual window for the channel group.

Step 6 To change the ops view to which this channel group belongs, from the Belongs To: drop-down list, choose an ops view.

Step 7 Click **Save**.

Deleting a Channel Group

When you delete a channel group, it is no longer available for use in Cisco IPICS. Deleting a channel group does not affect the channels that are contained in the channel group.

To delete a channel group, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 Check the check box next to each channel 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 this channel group, click **Cancel**.

Managing Locations

In Cisco IPICS, locations are used to define multicast domains within a Cisco IPICS deployment. A multicast domain comprises a set of multicast addresses that are reachable within a multicast network boundary. This implementation enables the Cisco IPICS server to assign the appropriate multicast address based on a specific user location.

If two or more users are connected to the same multicast network (or domain), they are in the same location but not necessarily in the same physical place. If two or more users are in the same location and are using the same multicast channel, they can talk to each other without the need for additional resource configuration.

This section includes the following topics:

Predefined Cisco IPICS Locations

In addition to specifically assigning names to locations, Cisco IPICS includes the following two predefined locations: ALL and REMOTE.

The ALL location signifies no network boundaries; that is, a channel that is designated with the ALL location means that there are no network boundaries within the Cisco IPICS deployment for that associated multicast address. The designation of ALL is the sum total of all defined locations.

Note The ALL defines the scope or reachability of a multicast address. For this reason, the ALL location applies to channels and VTGs, which are associated with multicast addresses, but not applicable to IP phones or RMS components, which are not associated with multicast addresses. The Cisco IPICS server assumes that the multicast address associated with a channel or VTG that is designated with the ALL location can reach all multicast locations. However, this assumption is not always accurate.

- Channels that are designated with the ALL location can be mixed on any RMS, including RMS components that are not configured with the ALL location, because any RMS can send packets to a multicast address that is associated with the ALL location.
- VTGs are always associated with the ALL location because every VTG multicast address is dynamically-assigned and associated with the ALL location.

The REMOTE location is available only to IDC users. When an IDC user chooses the REMOTE location from the Location drop-down list, connectivity is established with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user.

- For each channel that is associated with the user, the IDC establishes a SIP-based unicast connection with the RMS that is defined in the same location as the channel.
- For each VTG that is associated with the user, the IDC can establish a SIP-based unicast connection with any RMS because VTGs always use a multicast address in the ALL location.

In all cases, the Cisco IPICS server allocates RMS resources upon successful IDC authentication. When additional channels or VTGs are assigned to a logged-in user, the server immediately allocates the necessary RMS resources for each channel or VTG. When the IDC user activates the channel or VTG, the IDC places the SIP call to the appropriate RMS.

Note An RMS includes digital signal 0 (DS0) resources that are used to connect channels in to VTGs (or VTGs in to VTGs) and to provide SIP-based unicast access to IDC users.

Location Associations

The following Cisco IPICS resources always maintain location associations:

- RMS—Each RMS that you configure for use with Cisco IPICS must be associated with a location. An RMS can host only those channel resources that are assigned to the same location as the RMS or to the ALL location. If the RMS is associated with the ALL location, it can host only those channels that are also assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location to an RMS.
- Channels—You can associate a channel with one or more locations. If you associate a user to a channel, the user is assigned the channel configuration that is associated to the current user location. Whenever possible, user access via multicast communication is preferable over SIP to minimize the user of RMS resources.

The following examples describe the access that is available based on the specified configurations:

Configuration:

- Channel 1 is defined with the Alpha location and the Bravo location
- Channel 2 is defined with the Delta location
- Channel 3 is defined with the ALL location
- User 1 is a member of VTG X
- User 1 is assigned to Channel 1, 2, and 3 and VTG X

Example 1: IDC User 1 logs in to Cisco IPICS by using the Alpha location

- User 1 is given access to Channel 1 via the multicast address that is assigned to Channel 1 in the Alpha location.
- Channel 2 is not included in the current location of User 1 (Alpha), so the server allocates an RMS resource in the Delta location to provide SIP-based connectivity.
- Channel 3 is defined with the ALL location, so the server enables User 1 for multicast access to Channel 3.
- VTG X is, by definition of a VTG, in the ALL location, so the server enables User 1 for multicast access to VTG X.

Example 2: IDC User 1 logs in to Cisco IPICS by using the Delta location

- Channel 1 is not included in the Delta location, so the server allocates an RMS resource in either the Alpha location or the Bravo location to provide SIP-based access to Channel 1.
- Channel 2 is included in the Delta location, so the server enables multicast access.
- Channel 3 is defined with the ALL location, so the server enables User 1 for multicast access.
- VTG X is defined in the ALL location, so the server enables User 1 for multicast access.

Example 3: IDC User 1 logs in to Cisco IPICS by using the REMOTE location

- Channel 1, 2, and 3 and VTG X all require that the server allocate RMS resources for this connection.
- Channel 1 requires that the server allocates an RMS resource from either the Alpha location or the Bravo location.
- Channel 2 requires that the server allocates an RMS resource from the Delta location.
- Channel 3 and VTG X are both defined with the ALL location.

- VTGs—VTGs are always assigned to the ALL location. Each channel that you assign to a VTG uses one RMS resource.
- IDC—During the login process, the IDC user chooses the current location or the REMOTE location.

  When a user chooses the REMOTE location, the server configures all of the user-assigned channels and VTGs for SIP-based access. In this case, the server must allocate one RMS resource for each channel and VTG. If the server has insufficient resources to use in the location that is specified by the channel configuration, the IDC user receives a message to indicate that the channel is not available.

  When the user chooses a location other than REMOTE, the server assigns direct multicast access to each channel that you configure with the same location as the chosen location, and any channel that you configure with the ALL location.

Note The server considers any assigned channels that cannot be accessed directly by using a multicast connection to be in the REMOTE location, which causes Cisco IPICS to allocate RMS resources for each one of those assigned channels.

- IP Phones—Cisco Unified IP Phones support only multicast connections. To use IP phones with Cisco IPICS, you must assign a location that is the same as the dial login default location. The server assigns the configured default location to an IP phone user when the user logs in to Cisco IPICS. (In this case, there is no user selection for location.) IP phone users can access only the associated channels that are assigned to their default location, along with any assigned VTGs. If the configured default location is the ALL location, IP phone users can access only the channels that are assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location as the default location for the IP phone user.
- Dial-in/Dial-out Users—When a user accesses the telephony user interface (TUI), the user connects to the Cisco IPICS dial engine by using unicast communications. The dial engine allows the TUI user to join any VTG or channel to which the user is associated.
  - When the user selects a channel, the server creates a VTG that contains the selected channel and assigns the VTG an address from the multicast pool. For this VTG, the server uses the RMS that is configured with the same location as the channel that the TUI user has selected.
  - When the user selects a VTG, the server creates a VTG that contains the selected VTG and assigns the VTG an address from the multicast pool. For this VTG, the server can use any RMS.

  In both cases, the server establishes a unicast call flow between the TUI user and the dial engine. The dial engine converts the unicast call flow to multicast by using the address that was assigned from the multicast pool. This multicast traffic flows to the RMS where the VTG was activated. When the VTG traffic reaches the RMS it is bridged to the channel or VTG that the user has selected. Therefore, the dial engine must be in the ALL location, or multicast domain.
- Allocation of RMS resources—When multiple eligible RMS components exist, Cisco IPICS allocates resources by using the “least recently used” algorithm to achieve load balancing. The following examples show how this algorithm works:

  Example 1:

  - Channel A is defined in the ALL location
  - RMS 1 is defined in Location 1
  - RMS 2 is defined in Location 2

  When the server needs to allocate an RMS resource for Channel A, it determines which RMS is the “least recently used” RMS and allocates the resource in the appropriate RMS.

  Example 2:

  - Channel B is defined in Location 2
  - RMS 1 is defined in Location 1
  - RMS 2 is defined in Location 2

  In the above example, the server allocates resources from RMS 2 because RMS 1 is defined in a different location.

Summary of Access Types and Connections

Table 2-9 shows a summary of the Cisco IPICS access types and connections, as they pertain to locations.

Table 2-9 Cisco IPICS Access Types and Connections

Access	Type of Connection	Description
IP Phone	Multicast (in all cases)	Can connect to any VTG that the IP phone user is associated with. Can connect to any channel that the IP phone user is associated with if the channel is in the same location as the location that is defined in the user dial login default location.
Dial-in	Unicast to the dial engine (in all cases)	Can connect to any channel or VTG that the dial-in user is associated with.
IDC (remote login)	Unicast	All channels and VTGs are unicast calls to the appropriate RMS.
IDC (non-remote login)	Multicast	Can connect to any channel via multicast if the user is associated with the channel and the channel is configured with the same location as the location that was chosen by the user at login. Can connect to any VTG that the user is associated with.
IDC (non-remote login)	Unicast	Can connect to any channel that is configured with a location that is different from the location that was chosen at login.

The following section provide additional information about location-related management tasks that you can perform:

- Understanding the Locations Window, page 2-29
- Adding a Location, page 2-30
- Viewing or Editing a Location, page 2-30
- Deleting a Location, page 2-31

Understanding the Locations Window

The Locations window lists information about each of the locations that you have added in Cisco IPICS. It also allows you to perform several locations management functions.

To display the Locations window, navigate to the **Configuration > Locations** link in the Administration Console.

Note By default, location names appear in ascending alphanumeric order.

Table 2-10 describes the items in the Locations window.

Table 2-10 Items in the Locations Window

Item	Description	Reference
Location Name field	Specifies the name that is assigned to the location	See the "Viewing or Editing a Location" section on page 2-30
Add button	Allows you to add a new location in Cisco IPICS	See the "Adding a Location" section on page 2-30
Delete button	Allows you to delete a location	See the "Deleting a Location" section on page 2-31

Adding a Location

You can add locations to Cisco IPICS as needed To do so, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Locations** window.

Step 2 To add a location, click **Add**.

Step 3 In the Location Name field, enter a name for the location.

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

Note The IDC may truncate the location name if the name includes more characters than the IDC can display.

Tip Remember to assign location names that make sense to you.

Step 4 Click **Save**.

If you choose not to add this location, click **Cancel**.

Viewing or Editing a Location

You can view or edit a location that is configured in Cisco IPICS.

To view or edit a location, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Locations** window.

Step 2 In the Location Name column, click the link of the location that you want to view or edit.

The window for the location that you choose displays.

Step 3 View or edit the location as desired; then click **Save**.

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

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

To add a location, see the “Adding a Location” section on page 2-30. To delete a location, see the “Deleting a Location” section on page 2-31.

Deleting a Location

You can delete a location when it is no longer needed.

You cannot delete a location if it is associated with a channel or if it is set as the default location for a user. In these cases, you must disassociate the location from the channel or set another default location for the user before you can delete the location.

You also cannot delete the **ALL** or **REMOTE** locations.

To delete a location from Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Locations** window.

Step 2 Check the check box next to each location 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 choose not to delete this location, click **Cancel**.

Managing the Multicast Pool

Cisco IPICS stores multicast addresses in the multicast pool. When you activate a VTG, Cisco IPICS automatically assigns an available multicast address from the multicast pool to that VTG.

Note Multicast addresses are dynamically assigned from the multicast pool to VTGs only; channels are explicitly configured with static addresses.

When a VTG deactivates, its multicast address is released for use by another VTG.

Note You cannot activate more VTGs than there are multicast addresses in the multicast pool.

As a Cisco IPICS system administrator, you can perform these multicast pool management tasks:

- Adding Multicast Addresses, page 2-34
- Viewing and Editing Multicast Address Information, page 2-35
- Deleting a Multicast Address, page 2-36

When using multicast communications with Cisco IPICS, Cisco recommends that you follow the guidelines in the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34.

You perform the multicast pool management tasks in the Multicast Pool window. For more information about this window, including how to access it, see the "Understanding the Multicast Pool Window" section on page 2-32.

Understanding the Multicast Pool Window

The Multicast Pool window lists information about each of the multicast addresses that you have added in Cisco IPICS. It also allows you to perform several multicast pool functions.

Note Cisco strongly recommends that you follow the guidelines in the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34 when you use multicast communications with Cisco IPICS.

To display the Multicast Pool window, access the Configuration drawer and click **Multicast Pool**.

Each multicast address in the multicast pool window appears on its own row with related information in various columns. By default, rows of information appear in ascending order by multicast address.

Table 2-11 describes the items in the Multicast Pool window.

Table 2-11 Fields in the Multicast Pool Window

Field	Description	Reference
Address	This field specifies the multicast address and port.	See the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34
Location	This field specifies the location that is assigned to this multicast address. The location name can include alphanumeric characters, spaces, and any of these characters: . , – ' # ( ) / :_ .	See the "Viewing and Editing Multicast Address Information" section on page 2-35 and the "Deleting a Multicast Address" section on page 2-36 See the "Managing Locations" section on page 2-25 for more detailed information about locations.
Status	Either of the following designations can display in this field: • Active—Address is assigned to an active channel/VTG/radio. • Idle—Address is not assigned to an active channel/VTG/radio.	
Connection Type	Either of the following designations can display in this field: • Used by Channel—Multicast address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG. • Used by Radio—Multicast address is assigned to a radio.	
Used By	This field specifies the name of the active channel, VTG, or radio that is using the multicast address, if applicable.	
Add button	Click this button to add a multicast address.	See the "Adding Multicast Addresses" section on page 2-34
Delete button	Click this button to delete a multicast address.	See the "Deleting a Multicast Address" section on page 2-36

Guidelines for Using IP Multicast Addresses with Cisco IPICS

Be aware of the following guidelines when you use multicast communications with Cisco IPICS:

Cisco IPICS strongly recommends IP multicast addresses that are in the 239.192.0.0 to 239.251.255.255 range.

- This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in a local domain. As such, this address range is less likely to cause an addressing conflict in an existing multicast domain.
- For more information, see RFC 3171 - Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment and RFC 2365 - Administratively Scoped IP Multicast.

For additional information about the use of IP multicast addressing, go to the following URL:

http://www.cisco.com/en/US/tech/tk828/tsd_technology_support_protocol_home.html

Adding Multicast Addresses

When you add a multicast address to the multicast pool, it becomes available for use by active VTGs.

If you later assign the address to a channel, it is no longer available for use by active VTGs.

Before you add a multicast address, configure locations, as described in the "Managing Locations" section on page 2-25.

To add one or more multicast addresses to the multicast pool, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Multicast Pool** window.

Step 2 Click **Add**.

The New Multicast Pool window displays.

Step 3 In the Address field, enter the multicast address that you want to add.

Be sure to enter a valid multicast address that begins with 239.

Note Cisco strongly recommends that you configure only addresses that are in the 239.192.0.0 to 239.251.255.255 range. For more information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34.

Step 4 In the Number of Addresses field, enter the number of IP addresses that you want Cisco IPICS to generate.

You can enter a number between 1 and 255.

Cisco IPICS can generate a list of multicast addresses and add them to the multicast pool. This feature can be useful when you need to add several multicast addresses.

When you choose to have Cisco IPICS generate a sequence of multicast addresses, you specify the first address and the number of addresses that you want. Cisco IPICS returns the number of addresses that you specify, starting with the first address that you specified and incrementing the fourth octet of each additional address by one. You can generate a sequence of up to 255 multicast addresses at a time.

For example, if you request five addresses and specify the first address to be 239.195.5.1, Cisco IPICS generates this sequence of addresses:

```
239.195.5.1
239.195.5.2
239.195.5.3
239.195.5.4
239.195.5.5
```

Note When you generate multicast addresses in this way, Cisco IPICS assigns the port number that you designate to each address. After Cisco IPICS generates the list of addresses, you can change the number or port for any address, and you can delete any addresses that you do not want in the multicast pool. For more information, see the "Deleting a Multicast Address" section on page 2-36.

Step 5 In the Port field, enter the port number for this address.

This value must be an even number in the range of 21000 through 65534.

Step 6 Click **Save**.

If you choose not to add this address, click **Cancel**.

Step 7 If you want to add other individual addresses, repeat Step 3 through Step 6.

Viewing and Editing Multicast Address Information

You can view information for any multicast address, and you can change a multicast address and port number. You do so in the Multicast Pool window.

To view or edit multicast address information, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Multicast Pool** window.

Step 2 To view or edit a multicast address, click the link for the multicast address that you want to view or change.

The Multicast Address Pool Information window for the selected multicast address displays.

Step 3 View or update the information that is described in Table 2-12.

Table 2-12 Multicast Address Details Area Fields

Field	Description
Address	This field represents the multicast address. You add an address, enter a valid multicast address, and make sure to enter all 4 octets of the address. Each octet must be in the range of 0 through 255. **Note** Cisco IPICS strongly recommends addresses that are configured in the 239.192.0.0 to 239.251.255.255 range. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34.

Table 2-12 Multicast Address Details Area Fields (continued)

Field	Description
Port	This field represents the port number assigned to the multicast address. This value must be an even number in the range of 21000 through 65534. **Note** Cisco IPICS does not allow the configuration of any port below 21000 or any odd ports.
Connection Type *Display only*	This field can include either of the following designations: • Used by Channel—Address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG. • Used by Radio—Address is assigned to a radio.
Status *Display only*	This field can include either of the following states: • Active—Address is assigned to an active channel/VTG/radio. • Idle—Address is not assigned to an active channel/VTG/radio.
Location *Display only*	Location that is assigned to this multicast address. An address for a PTT channel has a specific location, either location ALL or another location name. Regardless of the location in this field, a VTG can contain only channels that are in the same multicast domain as the RMS that is used to mix the channels. See the "Managing Locations" section on page 2-25 for more detailed information about locations.
Used By *Display only*	Name of the active channel, VTG, or radio that is using the multicast address, if applicable.
Last Released *Display only*	This field displays when the multicast address was last released.

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

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

Deleting a Multicast Address

You can delete a multicast address when it is no longer needed.

Note You cannot delete a multicast address that is assigned to an active VTG. You must deactivate the VTG before you can delete the address. You also cannot delete a multicast address that is assigned to a channel. To delete the address in this case, delete the channel, which automatically removes the multicast address from the multicast pool.

To delete a multicast address from the multicast pool, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Multicast Pool** window.

Step 2 Check the check box next to each multicast address 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 choose not to delete this address, click **Cancel**.

Managing the RMS

An RMS is a component that enables the Cisco IPICS IDC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.

Note Before you perform the RMS management procedures that are described in the following sections, you must configure the RMS. For more information see Appendix A, "Configuring the Cisco IPICS RMS Component."

As a Cisco IPICS system administrator, you can perform these RMS management tasks:

- Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS, page 2-39
- Adding an RMS, page 2-43
- Viewing and Configuring Loopbacks, page 2-44
- Deleting an RMS, page 2-46
- Managing the RMS Configuration, page 2-47

You perform the RMS management tasks in the RMS window, which is located in the Configuration drawer. For more information about this window, including how to access it, see the "Understanding the RMS Window" section on page 2-37.

Note Cisco IPICS is not intended to provide complete management capabilities for an RMS. Cisco IPICS manages only the voice-specific parameters that are necessary to set up audio services for Cisco IPICS.

Understanding the RMS Window

The RMS window lists the RMS components that are available in your Cisco IPICS network. This window also allows you to perform the RMS management functions.

To display the RMS window, navigate to the **Configuration > RMS** window in the Administration Console.

The Routers pane in the RMS window displays the name of each RMS that is configured in your Cisco IPICS network.

For detailed RMS configuration information, see Appendix A, "Configuring the Cisco IPICS RMS Component."

Table 2-13 describes the items in the RMS window.

Table 2-13 Items in the RMS Window

Item	Description	Reference
RMS Name field	This field specifies a unique name that is assigned to the RMS.	See the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-39 and the "Adding an RMS" section on page 2-43 See the "Managing Locations" section on page 2-25 for detailed information about configuring locations
Location field	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this RMS.	
IP Address field	This field specifies the IP address of the Loopback interface.	
Router Type field	This field specifies the model number of the RMS.	
Status field	This field indicates whether an RMS is operational, configured, stopped, deactivated, or unreachable.	
Available field	Number of DS0s that are available for use in Cisco IPICS.	See the "Viewing and Configuring Loopbacks" section on page 2-44
In Use field	Number of DS0s that are currently being used in Cisco IPICS.	
Reserved field	Number of DS0s that are reserved for non-Cisco IPICS use.	
In Error field	Number of DS0s that are misconfigured.	
Add button	Choose this button to add an RMS component.	See the "Adding an RMS" section on page 2-43
Delete button	Choose this button to delete an RMS component.	See the "Deleting an RMS" section on page 2-46
Configuration drop-down list	Provides the ability to merge, update, or show configuration information for an RMS component.	See the "Managing the RMS Configuration" section on page 2-47

Table 2-13 Items in the RMS Window

Item	Description	Reference
Display Controls		
Rows per page drop-down list	Specifies the number of rows of RMS components that are included in a RMS components list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays RMS components on a specific page.	
|< (First page) button	Displays the first page of the RMS components list.	
< (Previous page) button	Displays the previous page of the RMS components list.	
> (Next page) button	Displays the next page of the RMS components list.	
>| (Last page) button	Displays the last page of the RMS components list.	

Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS

You can view and edit information for any RMS in your Cisco IPICS network. You can also deactivate an RMS, which makes it unavailable for use by Cisco IPICS, or reactivate an RMS. You perform these tasks in the Edit Router Details area.

By default, Cisco IPICS polls the RMS every 10 minutes, using the RMS comparator mechanism. The RMS comparator checks the responsiveness of the RMS if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. (You can change the polling period by entering a new value in the **RMS Polling Frequency field** in the Options window in the Administration drawer. For more information, see the "Managing Cisco IPICS Options" section on page 2-89.)

Tip Because the RMS comparator mechanism can interject delays, you can disable it by navigating to the **Administration > Options** window and checking the **Disable RMS Comparator** check box. You should check this check box if you are connected via a high latency (high delay), low bandwidth connection, such as a satellite link. Be aware that when you disable the RMS Comparator, you must merge the RMS configuration to make sure that the router is synchronized with the server. For information about how to merge RMS configuration, see the "Managing the RMS Configuration" section on page 2-47. For more complete configuration and deployment details, see *Solution Reference Network Design (SRND)* (latest version).

Note Disabling the RMS Comparator affects every router in the network.

Editing or Viewing RMS Details

You can edit or view a variety of information for an RMS. To do so, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 In the RMS Name column, click the link of the RMS that you want to view or change.

The General tab for the selected RMS displays.

Step 3 To change any RMS information, except updating the name, configuring loopbacks, or reserving or unreserving DS0s, click **Deactivate**.

This action makes the RMS temporarily unavailable to Cisco IPICS.

Tip Before you make changes, wait until all RMS resources are not in use, or manually disable the channel or deactivate any VTG that uses the resources of this RMS. For more information about how to disable a channel, see the "Changing the Status of a PTT Channel" section on page 2-12. For information about how to deactivate a VTG, "Changing the Status of a VTG" section on page 5-12.

Step 4 To view or update the information in the General tab, see Table 2-14.

Table 2-14 Fields in the General Tab of the RMS Window

Field	Description
Identification	
Name	This field specifies the name of the RMS. The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :.
Location	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this RMS. An RMS must be configured with the same location that is configured for the channels that it serves. See the "Managing Locations" section on page 2-25 for detailed information about locations.
Description	This field specifies a description for the RMS.

Table 2-14 Fields in the General Tab of the RMS Window (continued)

Field	Description
Status *Display only*	This field can include any of the following statuses: • Operational—RMS has at least one loopback configured and that is operating. • Unconfigured—RMS has no loopbacks. • Stopping—RMS has been deactivated but has at least one DS0 in use by Cisco IPICS. The RMS deactivates when Cisco IPICS no longer uses any of its voice ports. **Note** If one or more VTGs are active and you try to deactivate an RMS, the RMS status displays as Stopping. You must deactivate the VTG(s) before the RMS displays a deactivated status. To deactivate a VTG, see the "Changing the Status of a VTG" section on page 5-12. • Deactivated— RMS has been deactivated and has no DS0s in use. **Note** You can change the user name, password, multicast address, or location of the RMS only when it is in the Deactivated state. • Unreachable—RMS cannot be reached by the Cisco IPICS server.
Hardware Settings	
IP Address	This field specifies the IP address of the Loopback interface.
Host Name *Display only*	This field specifies the host name of the RMS.
User Name	This field specifies the user name that Cisco IPICS uses to access the RMS. This name must have administrator privileges on the RMS.
Password	This field specifies the password that Cisco IPICS uses to access the RMS.
Router Type *Display only*	This field specifies the model number of the RMS.
Controllers *Display only*	This field displays the T1/E1 connections on the RMS. The number in parentheses is the number of ports on the corresponding controller.
Loopbacks (Click the **Loopbacks** Tab to access the Loopback information)	This field specifies the mappings between two controllers that are physically connected. To change a loopback, choose a pair of controllers from the two Loopback drop-down lists and click **Add**. A controller appears in gray if it is in use. Each configured loopback appears in a list near the bottom of this area. To see detailed information about a loopback, click the right arrow next to its name. To see detailed information about all loopbacks, click **Expand All**. To collapse an expanded view of a loopback, click the down arrow next to its name. To collapse detailed information about all loopbacks, click **Collapse All**. For an explanation of the detailed loopback information, see the "Viewing and Configuring Loopbacks" section on page 2-44.

Step 5 If you changed information in the IP Address, User Name, or Password fields, make the corresponding change in the router by using the configuration application of the router.

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

To exit without saving changes, click **Cancel**.

Step 7 If you deactivated the router, click **Activate** to reactivate it.

After you change information for an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the changes. If you want to cause Cisco IPICS to recognize the changes immediately, see the "Managing the RMS Configuration" section on page 2-47.

Note You can change the default time that Cisco IPICS takes to recognize an RMS by entering a new value in the RMS Polling Frequency field in the **Administration > Options** window. For more information, see the "Managing Cisco IPICS Options" section on page 2-89.

Deactivating or Activating an RMS

When you deactivate an RMS, it goes into the Deactivated state and becomes unavailable for use by Cisco IPICS until you activate it. You should deactivate an RMS when you make certain changes to it, as described in the "Editing or Viewing RMS Details" section on page 2-40.

Note If you deactivate an RMS that has one or more voice ports in use by Cisco IPICS, or if one or more VTGs are active, the RMS goes into the Stopping state. You cannot deactivate an RMS if any VTGs are active. A router that is in the stopping state cannot provide additional support for IDC SIP connections or additional channels that are participants in active VTGs. Existing connections and channels that are supported by the RMS are not affected. The RMS becomes deactivated when Cisco IPICS no longer uses any of its voice ports. To deactivate a VTG, see the "Changing the Status of a VTG" section on page 5-12.

When you activate an RMS component, it becomes available for use by Cisco IPICS.

To deactivate or activate an RMS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 In the RMS Name column, click the link of the RMS that you want to deactivate.

Step 3 Click **Deactivate** to deactivate an active RMS, or click **Activate** to activate a deactivated RMS.

Note Activation or deactivation of a VTG requires that the Cisco IPICS server communicate with the RMS. If a VTG is deactivated when the RMS is unavailable, the deactivation occurs in the Cisco IPICS database, but is not reflected in the RMS until the Cisco IPICS server is back in communication with, and synchronizes with the RMS.

Adding an RMS

When you add an RMS, you make it available to Cisco IPICS. Before you add an RMS, make sure that these conditions are met:

- The router must exist on the Cisco IPICS network and it must be configured as described in Appendix A, "Configuring the Cisco IPICS RMS Component"
- At least one location must be defined, as described in the "Managing Locations" section on page 2-25

To add a new RMS in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Click **Add**.

The Add New Router Media Service window displays.

Step 3 In the Add New Router Media Service area, enter the following information:

Note For detailed descriptions of the RMS fields, see Table 2-14.

a. In the IP Address field, enter the IP address of the loopback interface. The IP address of the loopback interface must be configured to support SIP calls.

b. In the User Name field, enter the user name that is required to log in to the RMS.

c. In the Password field, enter the password that is required to log in to the RMS.

d. From the Location drop-down list, choose a location that is defined by the IP address that you entered for the router.

See the "Managing Locations" section on page 2-25 for more detailed information about locations.

e. Click **Save**.

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

When you click **Save**, Cisco IPICS determines whether it can access the RMS. This process can take up to one minute. If the RMS is accessible, Cisco IPICS displays the Router Details area for the RMS. If the router is not accessible, a message informs you of the possible reason.

The Router Details area displays the following information for the router that you added:

- Location—This field specifies the location that is defined for this RMS
- Status—This field displays unconfigured because you have not yet saved the changes that you made.
- IP Address—This field specifies the IP address that you entered for this router.
- Host Name—This field specifies the host name that you configured on the router.
- User Name—This field specifies the user name that you entered for this router.
- Password—This field specifies the password that you entered for this router.
- Type—This field specifies the model number of this router
- Controllers—This field specifies the T1 connections that the router has available for loopback.

Step 4 In the Name field, enter a name for the RMS if you want to change the name that displays in the list or routers in the Manager Routers window.

By default, the name that displays is the router host name. You might find it useful to give the RMS a descriptive name. A name that you enter is for Cisco IPICS use only, it does not change the router host name.

Step 5 In the adjacent Loopbacks drop-down lists, create a loopback by choosing two controllers that are physically connected on the router; then click **Add**.

Repeat this step as needed to create additional loopbacks.

Step 6 Configure digital signal 0 (DS0s) for each loopback as described in the "Viewing and Configuring Loopbacks" section on page 2-44.

Step 7 Click **Save** to save the configuration for this RMS.

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

After you add an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the addition. If you want to cause Cisco IPICS to recognize the addition immediately, see the "Managing the RMS Configuration" section on page 2-47.

Viewing and Configuring Loopbacks

Each loopback that you create in Cisco IPICS appears in a list near the bottom of the Edit Router Details area. You can perform the following tasks related to loopbacks:

Viewing Detailed Information about a Loopback

You view loopback information in the **Loopbacks** tab of the RMS window. You can access this tab by navigating to the **Configuration > RMS** window and clicking the **Loopbacks** tab.

For more information about the RMS window, see the "Understanding the RMS Window" section on page 2-37.

To see detailed information about a loopback, click the left arrow next to its name. To collapse an expanded view of a loopback, click the down arrow next to its name.

To see detailed information about all loopbacks, click **Expand All**. To collapse detailed information about all loopbacks, click **Collapse All**.

An expanded view of a loopback provides this information for each time slot in the loopback:

- Number—DS0 in the loopback
- State—One of the following:
  - Enabled—DS0 can be used by Cisco IPICS
  - Disabled—DS0 cannot be used by Cisco IPICS

- DS0 Status—One of the following:
  - In Use—DS0 is being used to add a channel to a VTG, add a VTG to a VTG, or add a SIP connection for a channel/radio for a user
  - Available—DS0 can be used by Cisco IPICS
  - Reserved—DS0 is reserved for non-Cisco IPICS use
  - Errors—DS0 is misconfigured
- DS0 Source and DS0 Destination—Connections that the loopback is making. Port Source can be a channel or a VTG. Port Destination can be a channel, a VTG, or a user.

Enabling DS0s in a Loopback

After you create a loopback, you must enable the DS0s that can be used by Cisco IPICS. You can enable DS0s in one loopback at a time, or in several loopbacks at a time.

To enable DS0s in a loopback, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Click the **Loopbacks** tab.

Step 3 Expand each loopback in which you want to enable DS0s by clicking the right arrow next to its name or by clicking **Expand All**.

Step 4 Check the check box next to each DS0 that you want to enable.

If you want to enable all DS0s in a loopback, check the check box next to Number at the top of the list of DS0s for that loopback.

If you want to uncheck check boxes, take one of these actions:

- Uncheck specific check boxes, or uncheck the check box next to Number at the top of the list of DS0s to clears all check boxes for that loopback.
- Click **Clear** to clear all check boxes for all loopbacks.

Step 5 Click **Enable DS0s**.

The state for the DS0 displays **Enabled** in green text.

Step 6 Click **Save**.

If you do not want to enable the DS0 or DS0s, click **Cancel**.

Disabling DS0s in a Loopback

If you disable a DS0 in a loopback, it cannot be used by Cisco IPICS. You can disable DS0s in one loopback at a time, or in several loopbacks at a time.

To disable DS0s in a loopback, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Click the **Loopbacks** tab.

Step 3 Expand each loopback in which you want to disable DS0s by clicking the left arrow next to its name or by clicking **Expand All**.

Step 4 Check the check box next to each DS0 that you want to disable.

If you want to disable all DS0s in a loopback, check the check box next to Number at the top of the list of DS0s for that loopback.

If you want to uncheck check boxes, take one of these actions:

- Uncheck specific check boxes, or uncheck the check box next to Number at the top of the list of DS0s to clears all check boxes for that loopback.
- Click **Clear** to clear all check boxes for all loopbacks.

Step 5 Click **Disable DS0s**.

The state for the DS0 displays **Disabled** in red text.

Step 6 Click **Save**.

If you do not want to disable the DS0 or DS0s, click **Cancel**.

Removing a Loopback

To remove a loopback, click **Remove** next to its name; then, click **Save**.

If you decide not to remove the loopback, click **Add** next to its name or click **Cancel** instead of clicking **Save**.

Deleting an RMS

Deleting an RMS removes all of its resources from Cisco IPICS and makes the RMS unavailable to Cisco IPICS.

You cannot delete an RMS if any of its DS0s are in use by Cisco IPICS.

To delete an RMS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Check the check box next to the RMS 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 RMS, click **Cancel**.

Managing the RMS Configuration

You can manage the RMS configuration by navigating to the **Configuration > RMS** window.

Merging RMS configuration updates Cisco IPICS with the following router information:

- Host name
- Router type
- Controllers

Merge the RMS configuration if you add or remove controllers on the router or if you change its host name, and you want Cisco IPICS to recognize the change.

Updating the configuration of an RMS applies the RMS configuration that is specified in Cisco IPICS to the RMS. This procedure can be useful in the following situations:

- You have changed information for an RMS as described in the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-39 and you do not want to wait for Cisco IPICS to recognize the changes, which can take up to 10 minutes (by default).
- You have added an RMS as described in the "Adding an RMS" section on page 2-43 and you do not want to wait for Cisco IPICS to recognize the addition, which can take up to 10 minutes (by default).
- You restarted an RMS and are experiencing voice connectivity or voice quality issues. Updating the configuration of the RMS can help to eliminate the router configuration as the source of the problem.
- The RMS has restarted but Cisco IPICS has not yet updated the router configuration with the configuration that is specified in Cisco IPICS.

  An RMS that shuts down returns to its default configuration when it restarts. Within 10 minutes—by default—after it restarts, Cisco IPICS compares the current RMS configuration with the RMS configuration in the Cisco IPICS database. If there is a discrepancy, Cisco IPICS refreshes the RMS configuration to match the configuration in the database.

Note Manually updating the configuration for an RMS disconnects all users who are connected to the RMS through a SIP connection and may interrupt any active VTG participant that is hosted on that RMS.

To manage the RMS configuration, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 To manage the RMS configuration, check the check box to the left of the RMS Name of the RMS.

Step 3 From the Configuration drop-down list, take any of the following actions:

- To merge the RMS configuration, choose **Merge**.
- To update the RMS configuration, choose **Update**.

  After you click the **Update** button, wait approximately 90 seconds while the system goes through its checks and resets the RMS, then refresh your browser window to see current information.
- To view the RMS configuration, choose **Show**.

  The configuration output displays in a separate window showing the configuration of the voice-ports and dial-peers for this RMS.

Cisco IPICS displays changes in the Edit Router Details area.

Tip You can manage the RMS configuration for all of the RMS components that are configured in Cisco IPICS by checking the check box at the top of the RMS list, and choosing **Merge, Update,** or **Show** from the Configuration drop-down list.

Managing the UMS

The unified media service (UMS) is a component that performs audio mixing functions similar to those performed by the RMS. For more information, see the "UMS" section on page 1-5.

The following sections describe the sections that a Cisco IPICS system administrator can perform for the UMS:

You perform the UMS management tasks in the UMS window, which is located in the Configuration drawer. For more information about this window, including how to access it, see the "Understanding the UMS Window" section on page 2-48.

Understanding the UMS Window

The UMS window lists the UMS components that are available in your Cisco IPICS network. This window also allows you to perform the UMS management functions.

To display the UMS window, navigate to the **Configuration > UMS** window in the Administration Console.

The UMS List pane in the UMS window displays the name of each UMS that is configured in your Cisco IPICS network.

Table 2-15 describes the items in the UMS window.

Table 2-15 Items in the UMS Window

Item	Description	Reference
Name field	This field specifies a unique name that is assigned to the UMS.	See the "Viewing and Editing UMS Details" section on page 2-50 and the "Adding a UMS" section on page 2-54.
Location field	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this UMS.	See the "Managing Locations" section on page 2-25 for detailed information about configuring locations.

Table 2-15 Items in the UMS Window (continued)

Item	Description	Reference
IP Address field	This field specifies the IP address of the UMS.	See the "Viewing and Editing UMS Details" section on page 2-50 and the "Adding a UMS" section on page 2-54.
Configuration Port field	This field specifies the port on the UMS that the Cisco IPICS server uses to configure and control the UMS.	
High Availability Port field	This field specifies the port on the UMS that is used for HA heartbeats.	
SIP Connection Port	This field specifies the port on the UMS that remote clients use to communicate with the UMS.	
Mode	This field shows the current HA mode of the UMS ("Primary" or "Secondary"). Displays "Primary" for a standalone UMS.	
HA Status field	This field shows the HA status of the UMS ("Active," "Standby," "Initializing," "Out of Service," or "Unknown").	
Status field	This field shows the operational status of the UMS ("Enabled" or "Disabled"). The Cisco IPICS server excludes disabled UMS components when attempting to fulfill an audio mixing request.	
Number of Voice Ports in User field	The first value in this field shows how many VTGs and remote channels are being mixed on this UMS. The second value shows the maximum number of VTGs and remote channels that can be mixed at one time on this UMS.	
Add button	Choose this button to add a UMS component.	See the "Adding a UMS" section on page 2-54.
Delete button	Choose this button to delete a UMS component.	See the "Deleting a UMS" section on page 2-55.
Change Status drop-down list	Choose **Enable** to enable the UMS, or choose **Disable** to disable the UMS. Some operations, such as tearing down HA for the Cisco IPICS server, require that the UMS be disabled.	See the "Enabling or Disabling a UMS" section on page 2-53.

Table 2-15 Items in the UMS Window (continued)

Item	Description	Reference
Configure drop-down list	Choose **Update** to repair various UMS communication issues and update the UMS with the latest configuration from the Cisco IPICS server. Choose **Show** to see the current mixing sessions on the UMS.	See the "Repairing the UMS or Viewing a Mixing Session" section on page 2-53.
Display Controls		
Rows per page drop-down list	Specifies the number of rows of UMS components that are included in a UMS components list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays UMS components on a specific page.	
|< (First page) button	Displays the first page of the UMS components list.	
< (Previous page) button	Displays the previous page of the UMS components list.	
> (Next page) button	Displays the next page of the UMS components list.	
>| (Last page) button	Displays the last page of the UMS components list.	

Viewing and Editing UMS Details

You can view and edit information for any UMS in your Cisco IPICS network.

To view or edit UMS details, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > UMS** window.

Step 2 In the Name column, click the link of the UMS that you want to view or change.

The Configuration window for the selected UMS displays.

Step 3 View or update the information in the Configuration window, as described in Table 2-16.

Table 2-16 Fields in the Configuration Page of the UMS Window

Field	Description
Basic Configuration Tab	
UMS Name	This field specifies the name of the UMS. The name can include alphanumeric characters only.
UMS IP Address	This field specifies the IP address of the UMS. The Cisco server requires this address to send mixing requests to the UMS. Remote Clients also connect to this address in their SIP connections.

Table 2-16 Fields in the Configuration Page of the UMS Window (continued)

Field	Description
Location	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this UMS. A UMS must be configured with the same location that is configured for the channels that it serves. A UMS cannot be configured with the same location as an existing RMS. See the "Managing Locations" section on page 2-25 for detailed information about locations.
UMS Admin Password	This fields specifies the password for the Linux OS user "ipicsadmin" on the UMS.
Configuration Port	This field specifies the port on the UMS that the Cisco IPICS server uses to configure and control the UMS.
SIP Connection Port	This field specifies the port on the UMS that remote clients use to communicate with the UMS.
Save	Click this button to exit the UMS Configuration Page and save any changes that you made.
Cancel	Click this button to exit the UMS Configuration Page without saving any changes that you made.
Advanced Configuration Tab	
HA Enabled	Check this check box to make the Paired UMS field available so that HA for the UMS can be enabled. If unchecked, HA for the UMS is disabled. **Note** When HA is enabled, the active UMS and standby UMS maintain a heartbeat between them to continuously confirm the status and availability of each other. After a specified number of heartbeats are missed, an HA failure is declared and failover quickly occurs in the background. Within 5 seconds the audio fails over to the backup UMS, with minimal perceptible voice loss.
Mode *Display only*	This field shows the current HA mode of the UMS ("Primary" or "Secondary"). Displays "Primary" for a standalone UMS.
Paired UMS	Choose the UMS to use as the secondary UMS in an HA deployment. Each UMS must be in the same location to be paired. Before you can set up UMS HA, you must add both UMSs individually, and then select the paired UMS.
Heartbeat Port	This field specifies the port on the UMS that is used for HA heartbeats. The default value is 4000.
Heartbeat Interval (secs)	This field specifies the number of seconds between UMS-to-UMS heartbeats. Each heartbeat checks to confirm the status and availability of the partner server. Valid values are 5 through 600. The default value is 5.
Missed Heartbeat Count	This field specifies the number of missed heartbeats before the active UMS fails over to the standby UMS. Valid values are 5 through 30. The default is 5 (25 seconds if the Heartbeat interval is 5 seconds). The transition process takes approximately 10 seconds.

Table 2-16 Fields in the Configuration Page of the UMS Window (continued)

Field	Description
Save	Click this button to exit the UMS Configuration Page and save any changes that you made.
Cancel	Click this button to exit the UMS Configuration Page without saving any changes that you made.
UMS HA Status Tab	
Note This tab appears only after you save UMS configuration.	
UMS High Availability Mode *Display only*	This field indicates whether HA for the UMS is configured: • Enabled—HA for the UMS is configured • Disable—HA for the UMS is not configured
Standby UMS HA Status *Display only*	This field indicates whether the standby UMS is ready to go to active mode. Values are "Ready" or "Not Ready."
UMS Name *Display only*	This field shows the name of the UMS.
Operational State *Display only*	This field shows the operational status of the UMS ("Enabled" or "Disabled"). The Cisco IPICS server excludes disabled UMS components when attempting to fulfill an audio mixing request.
HA Status *Display only*	This field shows the status of the UMS: • Active—The UMS is ready to mix audio. • Standby—The UMS is ready for failover. • Initializing—The UMS is initializing. • Out of Service—The UMS is reachable, but is either unable to initialize or is in the process of restarting. • Unknown—The UMS is not reachable or there is a SSL certificate problem. The normal UMS operating state is Active or Standby.
Failover Now	Click this button to perform a manual failover from the active UMS to the standby UMS.
Go Standby	Click this button to force one of the UMSs into standby state. After network connectivity is restored, use this button to recover from a *split brain* scenario. For related information, see Chapter 10, "Configuring and Managing Cisco IPICS High Availability."
Refresh	Click this button to update the information on this tab with current information.
Voice Resource List Tab	
Port Number *Display only*	This fields shows an arbitrary identifier for an audio mixing session.
Voice Resource Status *Display only*	Reserved for future use.
Operational Status *Display only*	Displays the current operating status of the voice resource.

Table 2-16 Fields in the Configuration Page of the UMS Window (continued)

Field	Description
Source *Display only*	Channel or VTG of the connection that the voice resource is making.
Destination *Display only*	Channel, user, or VTG of the connection that the voice resource is making.
Refresh	Click this button to update the information on this tab with current information.

Enabling or Disabling a UMS

When you disable a UMS, it goes into the Disabled state and is not available to fulfill audio mixing requests until you enable it. You should disable a UMS when you make certain changes to it, as described in the "Viewing and Editing UMS Details" section on page 2-50.

Note You cannot deactivate a UMS if any VTGs are active or if the UMS is configured for HA. When the UMS becomes disabled, Cisco IPICS no longer uses any of its voice ports. To deactivate a VTG, see the "Changing the Status of a VTG" section on page 5-12.

When you enable a UMS component, it becomes available for use by Cisco IPICS.

To enable or disable a UMS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > UMS** window.

Step 2 Check the check box next to the link of the UMS that you want to enable or disable.

Step 3 From the Change Status drop-down list, choose **Enable** to enable the UMS, or choose **Disable** to disable the UMS.

Repairing the UMS or Viewing a Mixing Session

This section explains how to repair a UMS and view a mixing session that a UMS is handling.

Repairing a UMS fixes various UMS communication issues and updates the UMS with the latest configuration from the Cisco IPICS server. Perform this action in these situations:

- A UMS is in a split brain situation and there is no network issue causing this situation
- After a database restore
- After recovering from a hardware failure of a Cisco IPICS server or a UMS
- When a UMS is out of sync with the Cisco IPICS server

To repair a UMS or view a mixing session, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > UMS** window.

Step 2 Check the check box next to the link of the UMS that you want to update or view information about.

Step 3 From the Configure drop-down list, choose either of these options:

- **Update**—Repairs various UMS communication issues and updates the UMS with the latest configuration from the Cisco IPICS server.

  Repair is a lengthy process and takes more time if you have server HA or UMS HA configured. In some cases, it may take up to 5 minutes to repair a UMS. Be aware that services on the UMS restart during this process.

- **Show**—Displays the current mixing sessions on the UMS.

Adding a UMS

When you add a UMS, you make it available to Cisco IPICS. Before you add an UMS, make sure that these conditions are met:

- The UMS application must be installed on a dedicated server. See *Cisco IPICS Installation Guide* for UMS installation instructions.
- The UMS cannot be in the same location (multicast domain) as an RMS component.
- At least one location must be defined, as described in the "Managing Locations" section on page 2-25.
- You cannot add a UMS to a Cisco IPICS server if it is already in use by another Cisco IPICS server.
- The UMS must be running the same Cisco IPICS software release as the Cisco IPICS server.
- The UMS must be reachable when you add it to the Cisco IPICS server.

To add a new UMS in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > UMS** window.

Step 2 Click **Add**.

The UMS Configuration window displays.

Step 3 The UMS Configuration window, take these actions:

Note For detailed descriptions of the UMS fields, see Table 2-16.

f. In the UMS Name field, enter a unique name for the UMS.

a. In the UMS IP Address field, enter the IP address of the server on which the UMS is installed.

b. From the Location drop-down list, choose a location for the UMS.

See the "Managing Locations" section on page 2-25 for more detailed information about locations.

c. In the UMS Admin Password field, enter the password that you entered for the ipicsadmin user when you installed the UMS.

d. In the Configuration Port field, the port on the UMS that the Cisco IPICS server uses to configure and control the UMS.

   Cisco recommends that you use the default port 5555.

e. In the SIP Connection Port field, enter the port on the UMS that remote clients use to communicate with the UMS.

   Cisco recommends that you use the default port 5060.

f. Click **Save**.

   Cisco IPICS determines whether it can access the UMS. This process can take up to one minute and the message "This will take a minute. Please wait..." appears during this time. If the UMS is accessible, Cisco IPICS displays the UMS List page. If the UMS is not accessible, a message informs you of the possible reason.

Step 4 (Optional) If you are configuring a UMS for high availability, take these actions:

a. Click the name of the UMS that you want to configure as the primary UMS.

b. Click the Advanced Configuration tab.

c. Check the HA Enabled check box.

d. From the Paired UMS drop-down list, choose the UMS that is to be the secondary UMS.

e. In the Heartbeat Port field, enter the port number on the UMS that is used for HA heartbeats.

   Cisco recommends that you use the default port 4000.

f. In the Heartbeat Interval (secs) field, enter a number between 5 and 600 that defines the number of seconds between heartbeats. Each heartbeat checks to confirm the status and availability of the partner server.

   Cisco recommends that you use the default value of 5.

g. In the Missed Heartbeat Count field, enter a number from 5 to 30 that defines the number of missed heartbeats before the active role is transitioned to the secondary server.

   Cisco recommends that you use default value of 5.

h. Click **Save**.

Deleting a UMS

Deleting a UMS removes all of its resources from Cisco IPICS and makes the UMS unavailable to Cisco IPICS. This process can take up to 2 minutes and requires that the UMS be reachable.

To delete a UMS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > UMS** window.

Step 2 Check the check box next to the **UMS** 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 **U**MS, click **Cancel**.

Managing P25 Keys

Cisco IPICS provides features to manage the storage and distribution of keys for IDC users in "End to End" ISSIG mode, ISSI gateways, and DFSI gateways. These keys are used to encrypt and decrypt voice traffic on P25 TalkGroups and P25 Fixed Stations.

A key contains key data, and that data provides the information that the system uses for encryption and decryption. You can create multiple keys in Cisco IPICS.

A keys is assigned to a keyset. You can create up to 15 keysets in Cisco IPICS, and each keyset can contain multiple keys. One keyset is configured to be active. The system uses the keys in the active keyset for encryption and decryption.

In addition, keys can be assigned to P25 Fixed Station digital channels and ISSI gateway channels. The encryption and decryption of traffic on these channels is based on the keys that are assigned to them.

Configuring the system to use keys for security includes these general steps:

1. Create keyset. See the "Adding a Keyset" section on page 2-58.
2. Create keys. See the "Adding a Key" section on page 2-61.
3. Make the desired keyset active. See the "Activating a Keyset" section on page 2-59.
4. Associate keys to ISSI gateways. See the "Associating a Key to an ISSI or DFSI Gateway From the Radios Window" section on page 9-18
5. Assign keys to channels in P25 Fixed Stations and ISSI gateways. See the "Channel Selector Configuration" section on page 9-5.

Key management in Cisco IPICS is based on APCO P25 key management specifications.

As a Cisco IPICS system administrator, you can perform the following key management tasks:

You perform the key management tasks in the Keysets and the Keys windows, located in the Key Management drawer of the Administration Console. For more information about these windows, including how to access them, see the "Understanding the Keysets Window" section on page 2-57 and the "Understanding the Keys Window" section on page 2-60.

Understanding the Keysets Window

The Keysets window lists information about each of the keysets that you have added in Cisco IPICS.

The bottom area of this window displays a list of keysets and general information for each one. By default, this area displays all keysets, but you can choose to display only keysets that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of keysets that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to perform several keyset management functions. To display the Keysets window, access the Configuration drawer; then click **Keysets**.

Table 2-17 describes the items in the Keysets window.

Table 2-17 Items in the Keysets Window

Item	Description	Reference
Filter		
Name field	This field allows you to display only keyset names that begin with or match the character string that you enter (characters are not case-sensitive).	To limit the display of keysets or to display a certain keyset, enter the desired search criteria in the filter field; then, click **Go**.
Go button	Click this button to display keysets that begin with or match the character string that you choose.	
Clear Filter button	Click this button to remove filter selection display the full list of keysets.	
Keyset Information		
Name field	This field indicates the unique name that is assigned to the keyset. The name can include alphanumeric characters and spaces.	See the "Viewing and Editing Keyset Details" section on page 2-58
Ops View field	This field indicates the ops view to which the keyset belongs. All keysets belong to the System ops view.	—
Id field	This field indicates the unique identifier that is assigned to the keyset. Valid values are digits 1 through 15.	See the "Viewing and Editing Keyset Details" section on page 2-58

Table 2-17 Items in the Keysets Window (continued)

Item	Description	Reference
Status field	This field indicates the status of the keyset: • Active—Key data that belongs to this keyset is used for encryption and decryption • Inactive—Key data that belongs to this keyset is not active Only one keyset can be active at a time.	See the "Viewing and Editing Keyset Details" section on page 2-58
Display Controls		
Rows per page drop-down list	Specifies the number of rows of keysets that are included in a keysets list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays keysets on a specific page.	
|< (First page) button	Displays the first page of the keysets list.	
< (Previous page) button	Displays the previous page of the keysets list.	
> (Next page) button	Displays the next page of the keysets list.	
>| (Last page) button	Displays the last page of the keysets list.	

Adding a Keyset

Adding a keyset makes it available for use by Cisco IPICS. When you add the first keyset, it is configured automatically to be the active keyset.

To add a new keyset, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Key Management > Keysets** window.

Step 2 In the Keysets window, click **Add**.

The General tab for a new keyset displays.

Step 3 Follow the steps in the "Viewing and Editing Keyset Details" section on page 2-58.

Step 4 Click **Save** to add the keyset without exiting the current window.

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

Viewing and Editing Keyset Details

You can view and edit information for any keyset.

To view or edit keyset details, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keysets** window.

Step 2 In the Name column, click the link for the keyset for which you want to view or change information.

The General tab for the selected keyset displays. This window contains general information for that keyset . Table 2-18 provides descriptions of the fields in the General tab.

Table 2-18 General Tab Fields in Keysets Window

Field	Description
Name	Unique name of the keyset. The name can include alphanumeric characters and spaces.
Id *Display only*	Unique 8-bit system-assigned identifier that is assigned to the keyset.
Status *Display only*	Status of the keyset: • Active—Key data that belongs to this keyset is used for encryption and decryption • Inactive—Key data that belongs to this keyset is not active Only one keyset can be active at a time.
Description	Description of the key store

Step 3 Click **Save** to update the keyset without exiting the current window, or click **Cancel** to exit the window without saving changes.

Activating a Keyset

A keyset can be active or inactive. The system uses the keys that the active keyset contains to encrypt and decrypt data.

Before you can set the status of a keyset to active, key data must be defined for each key in that keyset.

When you change the status of a keyset to active, the currently active keyset changes to the inactive status automatically.

To determine the current status, access the Key Management drawer, click **Keysets**, and look at the information in the Status column for the keyset.

To activate a keyset, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keysets** window.

Step 2 In the Keysets window, check the check box next to the keyset that you want to activate, then choose **Activate** from the Change Status drop-down list.

Deleting a Keyset

If a keyset is no longer needed, you can delete it from Cisco IPICS. You can delete a single keyset or you can delete several keysets at one time. A keyset must be in the inactive state before it can be deleted.

To delete a keyset, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keysets** window.

Step 2 Check the check box next to each keyset 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 keysets, click **Cancel**.

Understanding the Keys Window

The Keys window lists information about each of the keys that you have added in Cisco IPICS.

The bottom area of this window displays a list of keys and general information for each key. By default, this area displays all keys, but you can choose to display only keys that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of keys that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to perform several keys management functions. To display the Keys window, access the Key Management drawer; then click **Keys**.

Table 2-19 describes the items in the Keys window.

Table 2-19 Items in the Keys Window

Item	Description	Reference
Filter		
Name field	This field allows you to display only key names that begin with or match the character string that you enter (characters are not case-sensitive).	To limit the display of keys or to display a certain key, enter the desired search criteria in the filter field; then, click **Go**.
Go button	Click this button to display keys that begin with or match the character string that you choose.	
Clear Filter button	Click this button to remove filter selection display the full list of keys.	
Key Information		

Table 2-19 Items in the Keys Window (continued)

Item	Description	Reference
Name field	This field indicates the unique name of the key.	See the "Viewing and Editing Key Details" section on page 2-62
Ops View field	This field indicates the ops view to which the key belongs. All keys belong to the System ops view.	—
Key Id (Hex) field	This field represents the ID of the key in decimal format and in hexadecimal format. The hexadecimal format is shown in parentheses.	See the "Viewing and Editing Key Details" section on page 2-62
SLN (Hex) field	This field represents the storage location number of the key in decimal format and in hexadecimal format. The hexadecimal format SLN is shown in parentheses.	
Algorithm field	This field indicates the algorithm that the key uses for encryption and decryption (DES or AES).	
Display Controls		
Rows per page drop-down list	Specifies the number of rows of keys that are included in a keys list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays keys on a specific page.	
|< (First page) button	Displays the first page of the keys list.	
< (Previous page) button	Displays the previous page of the keys list.	
> (Next page) button	Displays the next page of the keys list.	
>| (Last page) button	Displays the last page of the keys list.	

Adding a Key

Adding a key makes it available for use by Cisco IPICS.

Before you add a key, at least one keyset must be created. For more information, see the "Adding a Keyset" section on page 2-58.

To add a new key, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Key Management > Keys** window.

Step 2 In the Keys window, click **Add**.

The General tab for a new key displays.

Step 3 Follow the steps in the "Viewing and Editing Key Details" section on page 2-62.

Step 4 Click **Save** to add the key without exiting the current window.

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

Viewing and Editing Key Details

You can view and edit information for any key.

To view or edit details for a key, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keys** window.

Step 2 In the Name column, click the link for the key for which you want to view or change information.

The General tab for the selected key displays. This window contains general information for that key. Table 2-20 provides descriptions of the fields in the General tab.

Table 2-20 General Tab Fields in Keys Window

Field	Description
Key Details	
Name	This field represents the name of the key. The name can include alphanumeric characters and spaces.
SLN *Display only*	This field represents the storage location number of the key in decimal format and in hexadecimal format. The hexadecimal format SLN is shown in parentheses. You enter the SLN in decimal format. The system converts it to hexadecimal format for display when you save the key.
Key Type *Display only*	This field indicates that the key type is TEK (traffic encryption key)
Algorithm *Display only*	This field indicates the algorithm that the key uses for encryption and decryption: • AES—Advanced Encryption Standard • DES—Data Encryption Standard
Key Id *Display only*	This field indicates a unique user-assigned identifier of the key. Valid values are numerals 1 through 65535.
Description	This field represents a description of the key. The description can contain up to 100 characters.
Key Data Assignment **Note** One Key Data field appears in this area for each keyset that is defined in the system.	
Keyset_name Key Data *Display only*	This field indicates a numeric representation of the key data and assigns that key data to the corresponding keyset. If the key uses the AES algorithm, enter this value using 64 hexadecimal characters. If the key uses the DES algorithm, enter this value using 16 hexadecimal characters with odd parity. You can enter different key data for each keyset that includes this key.

Step 3 To view key associations, choose a key in the Keys window, click the **Associations** button that displays at the bottom of the window, then take one of the following actions from the Associations window:

- Click the **Users** tab—This tab displays the Cisco IPICS users who are associated to this key.

Table 2-21 describes the items in the Users window.

Table 2-21 Items in the Users Window

Item	Description
User Name field	This field specifies the unique identification name assigned to the user
Last Name field	This field specifies the last name of the user
First Name field	This field specifies the first name of the user
Status field	This field indicates whether the user is enabled or disabled

You can associate additional users to the key by performing the steps in the"Associating Users to Keys" section on page 2-63.

- Click the **Radio** tab—This tab displays the Cisco IPICS radios that are associated to this key.

Table 2-22 describes the items in the Radio window.

Table 2-22 Items in the Radio Window

Item	Description
Radio Name field	This field specifies the name of the radio
Location field	This field specifies the Cisco IPICS location of the radio
Multicast Address field	This field specifies the multicast address of the radio
Type field	This field specifies the type of the radio
Control Type field	This field specifies the control type of the radio
Status field	This field specifies whether the radio is enabled or disabled

You can associate additional users to the key by performing the steps in the"Associating ISSI and DFSI Gateways to Keys" section on page 2-65.

Step 4 Click **Save** to update the key without exiting the current window, or click **Cancel** to exit the window without saving changes.

Associating Users to Keys

You can associate specific users to a key in the Associations window. When you associate users with a key, that key is used to encrypt and decrypt voice traffic on P25 TalkGroups in native mode (if that key is assigned to the channel).

Note You can perform this procedure only if users have already been added in Cisco IPICS.

To associate users to keys, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keys** window.

Step 2 Take either of these actions to display the Associations window for the key with which you want to associate users:

- Click the link for the Key in the Name column, then click the **Associations** button, which appears at the bottom of the General tab.
- Check the check box to the left of the Name of the key, then click the **Associations** button at the bottom of the Keys window.

Note The Associations button is dimmed if you do not check a key or if you check more than one key.

In the Associations window, make sure that the **Users** tab is selected.

This tab shows a list of the users who are associated with the key and the status of each user.

Step 3 Click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the key by choosing criteria based on the following filters:

- User Name field—Specifies the user name of a user
- First Name field—Specifies the first name of a user
- Last Name field—Specifies the last name of a user
- Location drop-down list—Choose from a list of locations

  See the "Managing Locations" section on page 2-25 for detailed information about how to configure locations.
- Role drop-down list—Choose from a list of Cisco IPICS roles
- Ops View drop-down list—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the users in Cisco IPICS, click the **Go** button without entering any search criteria.

The results of your search criteria display in a list.

Step 5 To choose a user to associate to the key, check the check box to the left of the user name and click **OK**.

The user that you choose displays in the user list in the Users tab.

Step 6 To delete a user from this key association, check the check box to the left of the user and click **Delete**.

Associating ISSI and DFSI Gateways to Keys

You can associate specific ISSI and DFSI gateways to keys in the Associations window. When you associate an ISSI or DFSI gateway with one or more keys, the gateway can encrypt and decrypt voice traffic on any channel that also has one of the keys assigned to it.

To associate ISSI and DFSI gateways to keys, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keys** window.

Step 2 Take either of these actions to display the Associations window for the key with which you want to associate radios:

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

Note The Associations button appears dimmed if you do not check a key or if you check more than one key.

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

This tab shows a list of the radios that are associated with the key, location, multicast address, type, control type, and status of the radio.

Step 4 Click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the key by choosing criteria based on the following filters:

- Location drop-down list—Choose from a list of locations

  See the "Managing Locations" section on page 2-25 for detailed information about how to configure locations.

- Name field—Specifies the user name of a radio.

Step 5 To search for a radio, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the radios in Cisco IPICS, click the **Go** button without entering any search criteria.

The results of your search criteria display in a list.

Step 6 To add a radio, check the check box to the left of the radio name; then, click **OK**.

Step 7 To delete a radio from this key association, check the check box to the left of the signal name and click **Delete**.

Viewing Key Associations

You can view key associations by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keys** window.

Step 2 To view key associations, take either of these actions:

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

Note The Associations button appears dimmed if you do not check a key or if you check more than one key.

Step 3 From the Associations window, you can view the associations for the key by clicking either of the following tabs:

- **Users**—View users who are associated with this key and associate other users to the key.

Note To associate other users to the key, see the "Associating Users to Keys" section on page 2-63.

- **Radio**—View the radios that are associated with this key and associate other radios to the key.

Note To associate other signals to the key, see the "Associating ISSI and DFSI Gateways to Keys" section on page 2-65.

Deleting a Key

If a key is no longer needed, you can delete it from Cisco IPICS. You can delete a single key or you can delete several keys at one time. You cannot delete a key if it is assigned to a channel selector in a gateway or P25 Fixed Station.

To delete a key, perform the following procedure.

Note This procedure deletes a key even if it is in use by the system. If you delete an in-use key, it becomes unavailable immediately.

Before You Begin

If a key that you want to delete is assigned to a channel, unassign it from the channel. To do so, from the Administration Console, navigate to the **Configuration > Radios** window, click the link for the radio that contains the channel, click the Selectors tab, and choose the blank line from the Key drop-down list.

Procedure

Step 1 From the Administration Console, navigate to the **Key Management > Keys** window.

Step 2 Check the check box next to each key 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 keys, click **Cancel**.

Managing Cisco VSOM

Cisco IPICS provides features integrate with Cisco Video Surveillance Operations Manager (VSOM). VSOM is a component of Cisco Video Surveillance Manager (VSM) that provides access to live and recorded video from video surveillance cameras that are configured in VSM. When a connection to a VSOM server is configured in Cisco IPICS, video from a camera can be viewed from an incident in the IDC.

As a Cisco IPICS system administrator, you can perform the following VSOM management tasks:

- Adding a VSOM Server, page 2-68
- Viewing VSOM Server Details, page 2-69
- Deleting a VSOM Server Connection, page 2-69

You perform the VSOM management tasks in the VSOM List window, located in the Configuration drawer of the Administration Console. For more information about this windows, including how to access it, see the "Understanding the VSOM List Window" section on page 2-67.

Understanding the VSOM List Window

The VSOM List window lists information about each VSOM server that you have added in Cisco IPICS.

The bottom area of this window displays a list of VSOM servers that are configured for integration with Cisco IPICS. By default, this area displays all VSOM servers, but you can choose to display only VSOM servers that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of VSOM servers that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to add and delete connections to VSOM servers. To display the VSOM List window, access the Configuration drawer; then click **VSOM**.

Table 2-23 describes the items in the VSOM List window.

Table 2-23 Items in the VSOM List Window

Item	Description	Reference
Name field	This field indicates the unique name of the VSOM server	See the "Viewing VSOM Server Details" section on page 2-69
IP Address field	This field indicates the IP address of the VSOM server	See the "Viewing VSOM Server Details" section on page 2-69
Display Controls		
Rows per page drop-down list	Specifies the number of rows of VSOM servers that are included in a VSOM server list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays VSOM servers on a specific page.	
|< (First page) button	Displays the first page of the VSOM servers list.	
< (Previous page) button	Displays the previous page of the VSOM servers list.	
> (Next page) button	Displays the next page of the VSOM servers list.	
>| (Last page) button	Displays the last page of the VSOM servers list.	

Adding a VSOM Server

Adding a VSOM Server makes video from the cameras that are configured in VSM available for use by Cisco IPICS.

Note For supported VSOM server versions, see *Cisco IPICS Compatibility Matrix*.

To add a new VSOM server, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Configuration > VSOM** window.

Step 2 In the VSOM List window, click **Add**.

The Configuration tab for a VSOM server connection displays.

Step 3 Follow the steps in the "Viewing VSOM Server Details" section on page 2-69.

Step 4 Click **Save** to add the connection to the VSOM server without exiting the current window.

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

Viewing VSOM Server Details

You can view and edit information about a VSOM server connection.

To view VSOM Server details, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > VSOM** window.

Step 2 In the Name column, click the link for the VSOM server for which you want to view or change information.

The Configuration tab for the selected VSOM server displays. This window contains general information for that server. Table 2-18 provides descriptions of the fields in the Configuration tab.

Table 2-24 Configuration Tab Fields in VSOM Window

Field	Description
Name	Unique name of the VSOM server
IP Address	IP address of the VSOM server
Description	Description of the VSOM server

Deleting a VSOM Server Connection

If a VSOM server connection is no longer needed, you can delete it from Cisco IPICS. You can delete a single VSOM server or you can delete several VSOM servers at one time.

To delete a VSOM server, perform the following procedure.

Note This procedure deletes a VSOM server even if it is in use by the system. If you delete an in-use VSOM server, it becomes unavailable immediately.

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > VSOM** window.

Step 2 Check the check box next to each VSOM server 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 VSOM servers, click **Cancel**.

Managing Incidents

An incident is an event that you identify in Cisco IPICS and for which various users can coordinate responses by using the IDC. An incident can be any event, such as a fire or other situation, that requires a response.

The following section uses these incident-related terms:

- Active incident—The incident is ongoing and the IDC functionality is available for coordinating it. In addition, mobile client users can access the incident.
- Deactive incident—The incident is closed and the IDC functionality is not available for coordinating the incident. In addition, mobile client users cannot access the incident. (A deactive incident can be reactivated, if needed.)
- Incident VTG—A talk group that consists of the users, channels, and radios that are associated with an incident. When an incident VTG is active, its participants can communicate with each other. When it is inactive, they cannot.

For detailed information about coordinating incidents by using the IDC, see *IPICS Dispatch Console User Guide* for this release.

As a Cisco IPICS system administrator, you can perform the following incident management tasks, which allow you to obtain information and manage system resources:

- Understanding the Incidents Window, page 2-70
- Viewing Incident Details, page 2-72
- Changing the Status of an Incident, page 2-73
- Downloading Archived Incidents, page 2-74
- Deleting an Incident, page 2-74

You perform the incident management tasks in the Incidents window, located in the Configuration drawer of the Administration Console. For more information about this window, including how to access it, see the "Understanding the Incidents Window" section on page 2-70.

Note A user with the Cisco IPICS Dispatcher role or All role creates incidents in the IDC. For more information, see *IPICS Dispatch Console User Guide* for this release.

Understanding the Incidents Window

The Incidents window lists information about each incident that is configured in Cisco IPICS and is not yet archived.

The bottom area of this window displays a list of incidents and general information for incident. By default, this area displays all incidents, but you can choose to display only incidents that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of incidents that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to perform various incident management functions. To display the Incidents window, access the Configuration drawer, then click **Incidents**.

Table 2-25 describes the items in the Incidents window.

Table 2-25 Items in the Incidents Window

Item	Description	Reference
Filter		
Incident ID field	This field allows you to display only the incident with the ID that you enter.	To limit the display of incidents or to display a certain incident, enter the desired search criteria in the filter field; then, click **Go**.
Incident Name field	This field allows you to display only incidents with names that include the character string that you enter (characters are not case-sensitive).	
Started Before fields	These fields allows you to display only incidents that were activated before the date and time that you specify. To specify a date, click the Started Before field, then choose a date. To specify a time, choose the hour (24-hour format) and minute from the "at" drop-down lists.	
State field	This field allows you to display only incidents that are active or only incidents that are inactive.	
Incident VTG field	This field allows you to display only incidents that have an active incident VTG or only incidents that have an inactive incident VTG.	
Ops View field	This field allows you to display only incidents that belong to the designated ops view.	
Go button	Click this button to display incidents by the filters that you choose.	
Clear Filter button	Click this button to remove filter selections and display an empty list of incidents. Click the **Incidents** link again to display the full list of entries.	
Incident Information		
ID field	This field indicates the unique identifier that Cisco IPICS assigned to the incident	—
Name field	This field indicates the name that is assigned to the incident.	See *IPICS Dispatch Console User Guide* for this release.
Ops View field	This field indicates the ops view to which the incident belongs. An incident belongs to the same ops view as that of the user who created it.	—
Activated field	Indicates the date and time that the incident was activated.	See *IPICS Dispatch Console User Guide* for this release.
State field	This field indicates whether the incident is active or inactive.	See the "Changing the Status of an Incident" section on page 2-73.

Table 2-25 Items in the Incidents Window (continued)

Item	Description	Reference
Incident VTG field	This field indicates whether the incident VTG is active or inactive, if the incident includes an incident VTG.	See *IPICS Dispatch Console User Guide* for this release.
Delete button	Click this button to delete the specified incident(s).	See the "Deleting an Incident" section on page 2-74.
Change Status drop-down list	Choose from the Activate or Deactivate option to change the status of an incident.	See the "Changing the Status of an Incident" section on page 2-73.
Download Archived Incident(s) button	Click this button to obtain archived incidents.	See the "Downloading Archived Incidents" section on page 2-74.
Display Controls		
Rows per page drop-down list	Specifies the number of rows of channels that are included in a channels list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays channels on a specific page.	
|< (First page) button	Displays the first page of the channels list.	
< (Previous page) button	Displays the previous page of the channels list.	
> (Next page) button	Displays the next page of the channels list.	
>| (Last page) button	Displays the last page of the channels list.	

Viewing Incident Details

You can view information for any incident. To do so, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Incidents** window.

Step 2 In the ID column, click the link for the incident for which you want to view information.

Information for the selected incident displays in the following tabs:

- General tab— Table 2-26 describes the information in this tab.

Table 2-26 General Tab Information for Incidents

Field	Description
Incident Information Area	
ID	This field shows the unique identifier that Cisco IPICS assigned to the incident.
Name	This field shows the name that was assigned to the incident in the IDC.
Description	This field shows the description that was entered for the incident in the IDC.
State	This field shows whether the incident is active or inactive.
Incident VTG	This field shows whether the incident VTG for the incident is active or inactive.

Table 2-26 General Tab Information for Incidents (continued)

Field	Description
Ops View Area	
Ops View	This field indicates the ops view to which the incident belongs.
History Area	
Created By	This field shows the date and time that the incident was created.
Created	This field shows the date and time that the incident was created.
Activated	This field shows the date and time that the incident was activated.
Deactivated	This field shows the date and time that the incident was deactivated. If the incident is still active, this field displays "(Still Active)."

- User tab—Shows the Cisco IPICs user name, first name, and last name of each user who is a participant in the incident.
- Channel tab—Shows the name, description, and status (Enabled or Disabled) of each channel that is used in the incident.
- Radio tab—Shows the name, description, and status (Enabled or Disabled) of each radio that is used in the incident.
- Photo tab—Shows the name, description, and URL of each photograph that has been uploaded for the incident. To delete a photograph from the incident, check the check box to the left of the photograph and click **Delete**.
- Video tab—Shows the name, description, and URL of each video that has been uploaded for the incident. To delete a video from the incident, check the check box to the left of the video and click **Delete**.
- VTG tab—Shows the name, description, and status (Active or Inactive) of each incident VTG that has been created for the incident.
- Journal tab—Shows the name, description or message, type, and creation date of each journal entry that has been created for the incident. Type indicates that a user created the entry.
- Camera tab—Shows the name, VSOM server, VSOM location, description, and creator of each VSOM camera feed in the incident.

Step 3 To exit the display of incident details, click **Done**.

Changing the Status of an Incident

Cisco IPICS allows you to change the status of an incident. An incident status can be either of the following:

- Active incident—The incident is available on the IDC. You can use the IDC to add or remove resources and perform other activities for an active incident.
- Inactive incident—The incident is closed and the incident is not available on the IDC or to mobile client users cannot access the incident.

To determine the current status of an incident, access the Configuration drawer, click **Incidents**, and look at the information in the State column for the incident.

To change the status of an incident, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Incidents** window.

Step 2 Check the check box next to each incident for which you want to change the state, then choose the desired action (**Activate** or **Deactivate**) from the Change Status drop-down list.

Step 3 In the pop-up window that prompts you to confirm the action, click **OK**.

Downloading Archived Incidents

Cisco IPICS automatically archives an incident 30 days after it is deactivated (by default) or after the retention period that you configured. (For information about configuring archives, see the description of the Incident Archive pane options in Table 2-33 on page 2-90.) The system stores information about each archived incidents in a unique XML file. The XML files contain information about users, channels, radios, VTGs, journal entries, images, and videos that are part of the incident.

You can download the incident archive, which contains the XML files for all archived incidents. This process copies the zipped archived incident file to your local disk.

When an incident is archived, the system deletes it from the Cisco IPICS database, and it no longer appears in the list of incidents in the Incidents window. If the incident includes images or video clips that are stored on the Cisco IPICS server disk, and these items are not referenced by another incident the archiving process deletes these items from the disk.

To download an archived incident, To delete an incident, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Incidents** window.

Step 2 Click the **Download Archived Incident(s)** button.

This button is enabled only after the system creates and archive file.

Step 3 In the File Download dialog box, click Save, and follow the on-screen prompts to save the archive file in a location of your choice.

By default, the archive file name is ipics_incident_archive.zip.

Deleting an Incident

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

When you delete an incident, it goes into the *pending deletion* state. The system archives incidents in this state the next time it runs the archiver, then deletes the incidents from the Cisco IPICS database. When an incident is in this state, it does not appear in the IDC nor in the Incidents page in the Cisco IPICS Administration Console.

To delete an incident, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Incidents** window.

Step 2 If an incident that you want to delete is active, deactivate is as described in the "Changing the Status of an Incident" section on page 2-73.

Step 3 Check the check box next to each incident that you want to delete.

Step 4 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 5 To confirm the deletion, click **OK**.

If you do not want to delete the incident(s), click **Cancel**.

Managing Licenses

The Cisco IPICS license determines the number of concurrent LMR ports, multicast ports, dial users, Cisco Unified IP Phone users, Silver IDC users, Platinum IDC users, mobile endpoint users, and ops views that are available for your system. Licenses also determine whether the policy engine is enabled on your system, and whether high availability is enabled on your system.

If your requirements exceed the limits of your current license, you can obtain additional licenses. For detailed information about licenses and how to obtain them, see *Cisco IPICS Server Installation and Upgrade Guide* for this release.

As a Cisco IPICS system administrator, you can obtain and upload new license files, after you have obtained them, to the Cisco IPICS server so that the new licenses take effect. For instructions, see the "Uploading a License File" section on page 2-81.

You perform the license management tasks in the Administration > License Management window. For more information about this window, including how to access it, see the "Understanding the License Management Window" section on page 2-75.

Understanding the License Management Window

The License Management window provides information about the licenses that you configure for your Cisco IPICS installation. It also allows you to upload new licenses to the Cisco IPICS server after obtaining the licenses. See the "Uploading a License File" section on page 2-81 for information about uploading licenses.

To access the License Management window, navigate to Administration >License Management window in the Cisco IPICS Administration Console.

Note The data that displays in the License Management window shows the usage at the time that the license window was last accessed. To view the most current license information, refresh your browser window. Make sure to refresh your browser window often and before you perform any server administration functions, to ensure that you are working with the most current information. If you attempt to perform

an administration update in a window that does not display the most current data, the update may not succeed and cause Cisco IPICS to display an error. If you receive an error, refresh your browser window and retry the operation.

The License Management window contains the following tabs:

- Summary Tab
- Usage Per Ops View Tab
- Installed License Files Tab

Summary Tab

The **Summary** tab provides a summary of information about the licenses you have obtained for Cisco IPICS. This tab displays license feature names, the total number of ports, current port usage, and available ports. Table 2-27 describes the information in this tab.

If your system includes high availability, the high availability license resides on the secondary server only. The other licenses reside on the primary server only.

Table 2-27 Summary Tab Fields in the License Management Window

Field	Description
Feature Name	
Concurrent LMR Ports	An enabled channel uses an LMR port license. After a channel is disabled, the server releases the LMR license and makes it available for use. **Note** Each radio channel that you add in Cisco IPICS uses one LMR license. However, each unique channel that you configure within a radio channel, does not use a separate LMR license. Cisco IPICS uses only one LMR license per radio. Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location. If a channel has two multicast addresses that are assigned to the channel, the single channel uses two licenses. If one of the multicast addresses is removed, the system releases one of the licenses so that the port only uses one license.
Concurrent Multicast Ports	An activated VTG uses a multicast port license. After a VTG is deactivated, the server releases the multicast license and makes it available for use. **Note** Be aware that an inactive VTG uses a license when a policy triggers (activates) that VTG; therefore, if the number of licenses has been exceeded, the policy is not able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.
Concurrent Cisco Unified IP Phone Users	A Cisco Unified IP Phone user who is logged in to Cisco IPICS consumes one Cisco Unified IP Phone license. Cisco IPICS release the license when the user logs out. If you use all of the Cisco Unified IP Phone licenses, no more Cisco Unified IP Phone users can dial in.

Table 2-27 Summary Tab Fields in the License Management Window (continued)

Field	Description
Concurrent Dial Users	Each time that the policy engine performs a dial-in or dial-out action, one license is used. If you use all of the dial user licenses, the policy engine cannot perform additional dial-in or dial-out actions. **Note** To enable dial-in/dial-out functionality in Cisco IPICS, you must have a policy engine base license. After you have purchased the policy engine base license, you are able to access the policy engine-related windows and to perform dial-in/dial-out functions in Cisco IPICS. If you do not have a policy engine base license, the dial-in/dial-out functionality is disabled and you are not able to access the policy engine windows.
Concurrent Dispatch Console Silver Users	An IDC Silver user who is logged in to Cisco IPICS consumes one IDC Silver license. Cisco IPICS release the license when the user logs out. If you use all of the IDC Silver licenses, no more IDC Silver users can log in.
Concurrent Dispatch Console Platinum Users	An IDC Platinum user who is logged in to Cisco IPICS consumes one IDC Platinum license. Cisco IPICS release the license when the user logs out. If you use all of the IDC Platinum licenses, no more IDC Silver users can log in.
Concurrent Mobile Endpoint Users	A mobile endpoint user who is logged in to Cisco IPICS consumes one mobile endpoint license. Cisco IPICS release the license when the user logs out. If you use all of the mobile endpoint licenses, no more mobile endpoint users can log in.
Concurrent EndtoEnd P25 Vocoders	The number of concurrent connections to end-to-end P25 channels that your Cisco IPICS system is licensed to use on the IDC. An IDC user uses a license each time a P25 channel is powered up in EndtoEnd mode. **Note** The IDC supports a maximum of 4 concurrent P25 channels in EndtoEnd mode per user session. If a user is logged in from 2 IDC consoles at the same time, only one IDC can join P25 channels in EndtoEnd mode.
Concurrent Gateway P25 Vocoders	The number of P25 channels that can be concurrently enabled at any time on the Cisco IPICS server. The Cisco IPICS server uses a license each time a P25 channel is enabled on that server.
Concurrent DFSI Gateway fixed station ports	The number of DFSI P25 Fixed Stations that can be concurrently enabled at any time on the Cisco IPICS server. The Cisco IPICS server uses a license each time a P25 Fixed Station is enabled on that server.
Concurrent UMS Servers	The number of UMSs that can be configured and enabled in the Administration Console. The Cisco IPICS server uses a license each time a UMS is enabled on that server.
Concurrent ISSI Gateway Servers	The number of ISSI Gateway servers that can be configured and enabled in the Administration Console. The Cisco IPICS server uses a license each time an ISSI gateway is enabled on that server.
Concurrent DFSI Gateway servers	The number of DFSI Gateway servers that can be configured and enabled in the Administration Console. The Cisco IPICS server uses a license each time a DFSI gateway is enabled on that server.

Table 2-27 Summary Tab Fields in the License Management Window (continued)

Field	Description
Cisco IPICS Ops View	Cisco IPICS uses one license for each ops view that you configure. The number of ops views that are available for use displays in the License Summary pane. **Note** To create additional ops views, you must purchase and install a Cisco IPICS license that includes additional ops view ports.
Cisco IPICS Base Server License	License usage does not apply to this field. This field displays whether you have a base license for Cisco IPICS.
Cisco UMS High Availability License	License usage does not apply to this field. This field indicates whether you have a base license for UMS high availability.
Policy Engine Base License	License usage does not apply to this field. This field displays whether Cisco IPICS policy engine is enabled. When the policy engine is enabled, the Summary tab displays **Licensed**. When the policy engine is not enabled, the Summary tab displays **Not Licensed**.
High Availability License	License usage does not apply to this field. This field displays whether you have a high availability license for Cisco IPICS.

Note Dial ports can be used for dial-in or dial-out connections. For dial ports that are allocated among the ops view, the dial ports are used by dial-in, according to the pre-assigned dial-in phone number, that is configured in each ops view, that is dialed. For dial-out, the dial ports are used from the ops view, to which the user to be dialed, belongs. See Chapter 7, "Configuring and Managing Cisco IPICS Operational Views" for more information about ops views.

Usage Per Ops View Tab

The **Usage Per Ops View** tab provides license information per ops view. This tab displays types of licenses, the ops view, current license usage, and the allocated ports. Table 2-28 describes the information in this tab.

Table 2-28 Usage Per Ops View Tab in the License Management Window

Field	Description
License Type	
Concurrent LMR Ports	Ops View—Ops view to which this license belongs Current Usage—Number of LMR ports that are in use for this ops view Allocated Ports—Number of LMR ports that have been allocated to this ops view
Concurrent Multicast Ports	Ops view—Ops view to which this license belongs Current Usage—Number of multicast ports that are in use for this ops view Allocated Ports—Number of multicast ports that have been allocated to this ops view

Table 2-28 Usage Per Ops View Tab in the License Management Window (continued)

Field	Description
Concurrent Cisco Unified IP Phone Users	Ops View—Ops view to which this license belongs Current Usage—Number of Cisco Unified IP Phone ports in use for this ops view Allocated Ports—Number of Cisco Unified IP Phone ports that have been allocated to this ops view
Concurrent Dial Users	Ops View—Ops view to which this license belongs Current Usage—Number of dial ports that are in use for this ops view Allocated Ports—Number of dial ports that have been allocated to this ops view
Concurrent Dispatch Console Platinum Users	Ops View—Ops view to which this license belongs Current Usage—Number of IDC ports that are in use for this ops view Allocated Ports—Number of IDC ports that have been allocated to this ops view
Concurrent Mobile Endpoint Users	Ops View—Ops view to which this license belongs Current Usage—Number of mobile endpoint users that are in use for this ops view Allocated Ports—Number of mobile endpoint users that have been allocated to this ops view
Concurrent EndToEnd P25 Vocoders	Ops View—Ops view to which this license belongs Current Usage—Number of end-to-end P25 vocoders that are in use for this ops view Allocated Ports—Number of end-to-end P25 vocoders that have been allocated to this ops view
Concurrent Gateway P25 Vocoders	Ops View—Ops view to which this license belongs Current Usage—Number of gateway P25 vocoders that are in use for this ops view Allocated Ports—Number of gateway P25 vocoders that have been allocated to this ops view
Concurrent ISSI Gateway Servers	Ops View—Ops view to which this license belongs Current Usage—Number of ISSI gateway servers that are in use for this ops view Allocated Ports—Number of ISSI gateway servers that have been allocated to this ops view
Concurrent UMS Servers	Ops View—Ops view to which this license belongs Current Usage—Number of UMS servers that are in use for this ops view Allocated Ports—Number of UMS that have been allocated to this ops view

Table 2-28 Usage Per Ops View Tab in the License Management Window (continued)

Field	Description
Concurrent DFSI Servers	Ops View—Ops view to which this license belongs Current Usage—Number of DFSI gateway servers that are in use for this ops view Allocated Ports—Number of DFIS gateway servers that have been allocated to this ops view
Concurrent DFSI Talk Groups	Ops View—Ops view to which this license belongs Current Usage—Number of DFSI talk groups that are in use for this ops view Allocated Ports—Number of DFSI talk groups that have been allocated to this ops view
Dispatch Console Silver Users	Ops View—Ops view to which this license belongs Current Usage—Number of IDC ports that are in use for this ops view Allocated Ports—Number of IDC ports that have been allocated to this ops view

Installed License Files Tab

The **Installed License Files** tab provides information about the license files installed on the IPICS server. It displays the file name, file size (in bytes), and modify date for each license file. Table 2-29 describes the information in this tab.

Table 2-29 Installed License Files Tab in the License Management Window

Field	Description
File Name	Name of the installed license file.
File Size	Size (in bytes) of the installed license file.
Modify Date	Date and time when the license file was uploaded to the server.

Understanding Time-bound License Behavior

Time-bound, or evaluation, licenses differ from permanent licenses by the inclusion of a predefined expiration date.

Note Cisco IPICS does not overwrite older license files with newer license files. As a best practice, Cisco recommends that you remove the old license file(s) from the directory where Cisco IPICS stores the license(s).

After you remove the old license(s), restart the server by entering the following command:

*[root]# **service ipics restart***

For more detailed information and guidelines about time-bound licenses, see *Cisco IPICS Server Installation and Upgrade Guide* for this release.

About 30 days before a time-bound license is to expire, Cisco IPICS displays a warning message to alert you. You can dismiss this warning by clicking the **Dismiss** button.

When a license feature expires, the relevant functionality of that license becomes disabled. If the license is an uncounted license, the feature is disabled; however, if the license is a counted license, the number of ports that correspond to that license type is reduced by the count of the expired license feature. In this case, Cisco IPICS reloads all of the license features when it detects that one or more license features has expired. Expired license features display in the license detail area as flagged items.

Uploading a License File

After you obtain a new Cisco IPICS license file, you must upload it to the Cisco IPICS server before it becomes effective. This procedure copies a license file from the server location where you stored it to the Cisco IPICS server.

Note After you upload the license file, Cisco IPICS places the file in the following directory: **/opt/cisco/ipics/tomcat/versions/current/webapps/license/**

To upload a license file, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > License Management** window.

Step 2 In the License File field, enter the path name and file name of the license file to upload to the Cisco IPICS server.

To locate this file in a Choose File window, click **Browse**.

Note If you do not know the path name and file name of the license file, you can click Browse and navigate to the file in the Choose File window.

Step 3 Click **Upload** to upload the file to the Cisco IPICS database.

Step 4 Click **Apply** for the new license to become effective.

Cisco IPICS associates the license file with the server and restarts the license manager.

Note There may be a delay of a few minutes before you can access the Cisco IPICS Administration Console after you click the **Apply** button.

For more information about Cisco IPICS licenses, see *Cisco IPICS Server Installation and Upgrade Guide* for this release.

Viewing Active Users

As a Cisco IPICS system administrator, you can view the activity for users who are logged in to the system via an IDC, mobile client, Cisco Unified IP Phone, or dial-in, and users who are participating in a VTG by accessing the Administration > Active Users window. This window contains information about each type of user who is logged in to the system, such as the identification of the user, the location of the user, and ops views to which the user belongs. Using this window, you can also manually force logged-in and dialed-in users to log out of Cisco IPICS, if necessary.

To view active users and the associated information for each user, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Active Users** window.

Step 2 From the View drop-down list, choose one of following types of users that you want to view:

- **Logged-in Users**—Users who are logged in to Cisco IPICS
- **IDC**—Users who connected to Cisco IPICS through an IDC
- **Mobile**—Users who connected to Cisco IPICS through a Cisco IPICS Mobile Client.
- **Cisco Unified IP Phone Users**—Users who are connected to Cisco IPICS via a Cisco Unified IP Phone
- **Dialed-in Users**—Users who are connected to Cisco IPICS by using the dial-in/invite feature

A window displays a list of the type of users that you chose. See Table 2-30 for a description of the fields in the Active Users window.

You can specify the number of rows of active users that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Table 2-30 Active Users Window Fields

Field	Description
Logged-in Users	
User	User ID of user who is logged in to Cisco IPICS.
Date	Date and time that the user logged in to the Cisco IPICS system.
IDC Users	
User	User ID of the active IDC user.
IDC ID	Identification of the IDC for the session.
Version	Version of the IDC.
Address	IP address of the IDC client machine.
Location	Cisco IPICS location of the IDC user.
Belongs To	Ops view to which the IDC user belongs.
Last Activity	Date and time of the last IDC activity.
Mobile Users	
User	User ID of the active mobile client user.
Mobile ID	Identification of the mobile client for the session.

Table 2-30 Active Users Window Fields (continued)

Field	Description
Version	Version of the mobile client.
Address	IP address of the mobile client.
Location	Cisco IPICS location of the mobile client.
Last Activity	Date and time of the last mobile client activity.
Cisco Unified IP Phone Users	
User	Name or user ID of the active Cisco Unified IP Phone user.
Digit ID	Digit identification number of the active Cisco Unified IP Phone user.
Location	Location of the active Cisco Unified IP Phone user.
Active	Indicates whether the Cisco Unified IP Phone user is currently active.
Remote	Indicates whether the Cisco Unified IP Phone user is dialed in using a remote connection.
Dialed-in Users	
User	Name or user ID of the active dialed-in user.
Dial Number	Number that the user dialed when dialing in to Cisco IPICS.
Digit ID	Digit identification of the active dialed-in user.
Type	Type of talk group. This field is empty if the user is dialed in but has not joined any talk group. Type can indicate one of the following resources: • Channel • VTG
Talk Group	Name of the talk group (channel or VTG) that the user has joined. This field is empty if the user is dialed in but has not joined any talk group.
Status	Status of the dialed-in user and can be one of the following statuses: • Not Joined—The user is dialed in but has not joined a channel or VTG. • Listening—The user is dialed in and has joined a channel or VTG and is listening to that channel or VTG. • Talking—The user is dialed in, has joined a channel or VTG, and is currently talking (pressing the PTT button) on that channel or VTG.

Step 3 To manually disconnect a logged-in, IDC, mobile client, or dialed-in user from Cisco IPICS, take any of the following actions:

- To log out a logged-in user, click the **Logged-in** tab. Check the check box to the left of each logged-in user that you want to log out and click **Logout**.
- To log out an IDC user, click the **IDC** tab. Check the check box to the left of each IDC user that you want to log out and click **Logout**.

When you log out an IDC user, all resources, including licenses and RMS resources, are deallocated immediately.

If the IDC is running in offline mode, multicast audio for the IDC continues to work after you log out an IDC user if the Cisco IPICS server cannot reach the IDC to inform it of the logout and a channel or VTG is active. However, if the IDC was REMOTE (that is, using a unicast SIP call to the RMS), the server tears down the dedicated SIP connection for that IDC upon when you click **Logout** on the IDC tab.

- To log out a mobile client user, click the **Mobile** tab. Check the check box to the left of each mobile user that you want to log out and click **Logout**.

  When you log out a mobile client user, all resources, including licenses and RMS resources, are deallocated immediately.

- To log out a dialed-in user, click the **Dialed-in** tab. Check the check box to the left of each dialed-in user that you want to log out and click **Logout**.

Tip You can log out all users in each tab by checking the check box at the top of each user list and clicking **Logout**.

Step 4 To refresh the window of any tab, click the **Refresh** button at the bottom of the list.

Managing Activity Logs

The Cisco IPICS logs store a variety of information about activities relating to VTGs, such as the ops view for each channel, user, and VTG, the creator of log entries, and the time that log activities occurred. You can review this information at any time. Log activity information is also used for historical reporting.

You search for and download activity logs in the Activity Log Management window. This window contains a **Logs** tab and an **Archives** tab. See the "Understanding the Activity Log Management Window" section on page 2-85 for more information about the Activity Log Management window.

Cisco IPICS tracks and logs the date and time that certain types of activities occur. For detailed information about the activity types that are logged in Cisco IPICS, and how to specify what activity types get logged per ops view, see the "Managing Activity Log Options Per Ops View" section on page 2-88.

You can choose how to view activity logs:

- By ops view—Ops views to which the resource belongs
- By channel—Users and VTGs that used that PTT channel
- By radio—Channels, users, and VTGs that used that radio
- By user—PTT channels and VTGs in which that user was involved
- By VTG—Users and PTT channels that were participants in that VTG

To view and download activity logs. See the "Viewing and Downloading Activity Logs" section on page 2-85 for more information.

Understanding the Activity Log Management Window

The Activity Log Management window displays each channel, radio, user, or VTG that is configured in Cisco IPICS, depending on the information that you choose to view. It also allows you to perform the activity logs management functions.

The Activity Log Management window contains two tabs, in which you can manage activity log information: the **Logs** tab and the **Archives** tab.

In the **Logs** tab, you can choose to view logs by ops view and resource type (such as channel, radio, user, and VTG), and search for particular logs based on a date range. If you are assigned the system administrator and/or ops view administrator role, you can also apply the date range filter to minimize the logs that get returned from the system. After filtering the activity log resource list by ops view and resource type, you can then choose one of the resources from a single list. For more information about using the search filters, see Chapter 1, "Using Search Windows."

Note Users who are assigned the ops view administrator role can monitor only the activity logs of the ops view to which that user belongs. If a particular ops view is disabled, all the activity logging is done by using the SYSTEM default ops view. The system administrator is allowed to monitor logs of all the ops views. For more information about Cisco IPICS roles, see the "Cisco IPICS Roles" section on page 1-6.

For information about viewing and downloading Cisco IPICS activity logs, see the "Viewing and Downloading Activity Logs" section on page 2-85.

In the **Archives** tab, you can download activity log files that have been archived according to the threshold limits that are configured in the Administration > Options window. For more information about managing Cisco IPICS options, see the "Managing Cisco IPICS Options" section on page 2-89. For information about downloading archived activity logs, see the "Downloading Archived Activity Logs" section on page 2-87.

For information on the display controls, see the "Navigating Item Lists" section on page 1-13.

To open the Activity Logs Management window, navigate to the **Administration > Activity Log Management** window.

Viewing and Downloading Activity Logs

To perform detailed analysis of activities, you can view and download activity logs. You can view activity logs for any channel, radio, user, or VTG, based on ops views and resource type. You view and download activity logs in the Activity Log Management window.

When you download activity logs, Cisco IPICS takes these actions:

- Creates an .xml file that contains all activity logs in the period, ops view, and resource type that you designate
- Downloads the .xml file to the location that you specify on the computer from which you are accessing the Administration Console.

The file includes information about the related log entries for the search criteria that you specify (such as ops view, resource type, and date range).

To view and download activity logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Activity Log Management** window.

Step 2 From the drop-down list in the **Logs** tab, choose the ops view for the activity logs that you want to view and/or download.

Step 3 From the Resource Type drop-down list, choose the resource type for the activity logs that you want to view and/or download.

Step 4 To view and/or download only the activity logs for a specific resource, enter the name of the resource of the activity logs in the Resource Name field.

Step 5 From the Sort By drop-down list, choose one of the following options:

- **Date-and-Time**—This option sorts the logs by the date and time of the logs.
- **Initiator-User-ID**—This option sorts the logs by the user who initiated the log entry.
- **Affected-Source-Resource**—This option sorts by the name of the affected resource.
- **Affected-Target-Resource**—This option sorts by the name of the affected target resource.

Step 6 In the From field, specify the beginning date and time of the of the activity logs that you want to view or download.

Step 7 In the To field, specify the ending date and time of the activity logs that you want to view or download.

Step 8 Click **Go**.

The activity logs display according to the criteria that you choose.

Note You can specify the number of rows of activity logs that display per results page by choosing from the Rows per page drop-down list at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Step 9 To clear your search criteria, click the **Clear Filter** button.

Step 10 To download the logs to your PC, click **Download Activity Logs**.

Step 11 To open the file immediately, click **Open**. To save the file to your PC, click **Save**.

Note The activity log file is in .xml format.

Step 12 To view the activity logs in Microsoft Excel, save the file to a desired location and perform one of the following actions:

Note The following steps were performed by using Microsoft Office Excel 2007.

- Use Microsoft Excel application to open the .xml file. In the Open XML dialog box, click the **As an XML Table** radio button.

  Microsoft Excel creates a schema that is based on the .xml file source data.
- Navigate to the location where you saved the .xml file and take these actions:
  - Right-click the file.
  - Choose **Open With > Choose Program**.

- Choose **Microsoft Excel** in the Open With dialog box. (If the Excel application does not display in the list of programs, click **Browse** and locate the application.)
- Click **OK**.
- From the Open XML dialog box, click the **As a read-only workbook** radio button.

Step 13 To view or download archived activity logs, perform the steps in the "Downloading Archived Activity Logs" section on page 2-87.

Downloading Archived Activity Logs

You can download archived activity logs. Cisco IPICS archives the activity logs based on the thresholds that you assigned in the Administration > Options window in the Administration Console. For more information about the Options window, see the "Managing Cisco IPICS Options" section on page 2-89.

To download archived activity logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Activity Log Management** window.

Step 2 Click the **Archives** tab.

Table 2-31 shows the fields in the Archive Status pane.

Table 2-31 Archive WIndow Fields

Field	Description
Archive Time *Display only*	Time when the activity log files were archived in Cisco IPICS
Archive Status *Display only*	Indicates whether log files were archived successfully
Archive Count *Display only*	Number of log entries that were archived during the last archive
Archived Files drop-down list	The file names of the archived files
Download button	Click this button to download archived Cisco IPICS activity logs

Step 3 From the Archived Files drop-down list, choose the archived activity log file that you want to download.

Note If no log files have been archived, the Archived Files drop-down list and the Download button are disabled and display as dimmed.

Step 4 Click **Download**.

Step 5 To open this file immediately, click **Open**. To save the file to your PC, click **Save**.

Note Because Microsoft Excel does not support multi-root .xml documents, you can add the text "<activity_logs>" to the beginning and "</activity_logs>" to the end of the downloaded archived activity log file before opening the file. Adding the text changes the file to have only one root element.

If the name of the downloaded archived activity log file is "ipics_activity.xml.<1-24>", rename the file to "ipics_Activity<1-24>.xml" making sure that the .xml extension appears at the end of the file name, before opening in Microsoft Excel. Renaming the file ensures that Excel recognizes the file as an .xml file.

Managing Activity Log Options Per Ops View

You can specify the activities that you want Cisco IPICS to log, by ops view, in the Activity Log Options window. For example, if you want Cisco IPICS to only log when a VTG gets activated in a particular ops view, and no other activities, you would choose the Resource Creation and Deletion activity type for that ops view.

Table 2-32 describes the types of activities that can be logged in by ops views.

Table 2-32 Activity Log Types By Ops View

Activity Type	Description
Cisco Unified IP Phone Activities	Logs are created whenever Cisco Unified IP Phone activities occur in Cisco IPICS.
Dial-in Activities	Logs are created whenever dial-in activities occur in Cisco IPICS.
HAACTIONS	Logs are created whenever a high-availability activity occurs.
IDC Activities	Logs are created whenever IDC activities occur in Cisco IPICS.
Licensable Feature Activities	Logs are created whenever feature activities occur, for features that have been licensed in Cisco IPICS.
Resource Association Activities	Logs are created whenever resources are associated in Cisco IPICS.
Resource Creation and Deletion Activities	Logs are created whenever resources, such as VTGs, users, and channels are created or deleted from Cisco IPICS.
System Activities	Logs are created whenever system activities, such as voice resource activities, occur in Cisco IPICS.
Virtual Talk Group Activities	Logs are created whenever VTG activities occur in Cisco IPICS.

You can access the Activity Log Options window in the Administration Console by navigating to **Administration > Activity Log Options**.

To manage activity logs per ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Activity Log Options** window.

Step 2 From the Ops View drop-down list, choose the ops view for which you want to specify the activities to be logged.

Note All the activity types that are available to be logged in Cisco IPICS are listed in the Unselected Activity Types area. In order to specify particular activity types that you want to be logged in Cisco IPICS, for this ops view, you must move them to the Selected Activity Types list. If you do not move any activity types to the Selected Activity Types list, all activity types are logged in this ops view. If you move an activity type to the Unselected Activity Types list, the previously-logged activities of that type are not deleted from the system but they are prevented from being logged in the future.

Step 3 To select the activity types that you want to log in Cisco IPICS for an ops view, take any of the following actions:

- To move an activity type from one list to the other, click the activity type to highlight it; then, click **>** or **<**. Or, double-click the activity type.
- To move several activity types from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the activity types; then, click **>** or **<**.
- To move all activity types 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 Cisco IPICS Options

Cisco IPICS provides you with the ability to adjust system preferences and turn on or off certain options in the Options window. Cisco IPICS allows you to restore default settings at any time.

Information in the Options window is contained in the following information tabs:

- **General** tab—Choose this tab to set various options that affect the system and devices.
- **Passwords** tab—Choose this tab to set the password options for users.
- **Client** tab—Choose this tab to set IDC client configuration options.
- **SNMP** tab—Choose this tab to set SNMP options for Cisco IPICS.

Note Cisco IPICS provides a MIB that defines the data that is published via SNMP, and the traps (events) the Cisco IPICS server can send. The MIB is named CISCO-IPICS-MIB.my and is stored on the Cisco IPICS server in the /usr/share/snmp/mibs folder.

Cisco IPICS detects changes that are made to the system options and immediately makes the adjustments for those changes. You do not have to take any further action for the changes to take effect.

You can access the Options window in the Administration Console by navigating to **Administration > Options**.

You can use the options in the Options window in the following ways:

- You can customize the Cisco IPICS option settings by editing the fields in the General, Passwords, and IDC tabs.

  Note Ensure that you click **Save** after each change that you make to the settings.

- To restore all settings to the default values, click **Restore Defaults**.

The following tables describe the fields in the Options window:

- Table 2-33 on page 2-90—General Tab in the Options Window
- Table 2-34 on page 2-92—Passwords Tab in the Options Window
- Table 2-35 on page 2-96—Client in the Options Window
- Table 2-36 on page 2-99—Table 2-36 on page 2-99

Table 2-33 General Tab in the Options Window

Setting	Description	Default Setting
RMS Pane		
Disable RMS Comparator	The RMS comparator is the mechanism that checks the responsiveness of the RMS and if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. Because the RMS comparator can interject delays, you can disable it by checking this check box. **Note** If you connect via a high latency, low bandwidth connection, such as a satellite link, you should check this check box.	This check box is unchecked by default. If the Disable RMS Comparator check box is selected, the RMS Polling Frequency field displays as dimmed.
RMS Polling Frequency	The RMS comparator functionality includes a polling mechanism that regularly checks whether the server can reach all of the RMS components that are listed in the RMS window. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 1 through 32767.	The default interval between checks specifies 10 minutes.
Activity Logs Pane		

Table 2-33 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Activity Logs	This setting the maximum amount of database space that may be used by Cisco IPICS activity logs. For more information, see Chapter 12, "Understanding Cisco IPICS Serviceability and Diagnostic Information." This setting specifies a value in megabytes (MB). To change the default, double-click the current value and enter a new value. Valid values: 1 through 250.	The default maximum space for activity logs specifies 50 MB.
Activity Log Retention Period	This setting specifies the number of days that Cisco IPICS retains activity log entries. When this number has been reached, the logs get written to a rolling archive log. The archive log files are preserved until they get overwritten when the number of rolling files reaches the maximum number of archive files limit that is set by the system. Valid values: 1 through 365.	The default setting specifies 90 days.
Cisco Unified IP Phone Pane		
Cisco Unified IP Phone Timeout Period	This setting specifies whether a Cisco Unified IP Phone times out after a configured period of inactivity, forcing a user to log in again. **Note** To disable the timeout period, set the value to 0. This setting specifies a value in minutes. To change the default, double-click the current value and enter a new value. Valid values: 0 through 99999.	The default setting specifies 30 minutes.
Cisco IPICS Session Pane		
Cisco IPICS Session Timeout Period	This setting specifies whether a Cisco IPICS session times out after a configured period of inactivity, forcing a user to log in again. **Note** To disable the timeout period, set the value to 0. This setting specifies a value in minutes. To change the default, double-click the current value and enter a new value. Valid values: 0 through 99999.	The default setting specifies 30 minutes.
Incident Archive Pane		
Maximum File Size	This field specifies the maximum size of archive file, in MB. When an archive file reaches this size, older information is deleted.	The default setting specifies 50 MB.
Retention Period	This field specifies how many days Cisco IPICS retains an inactive incident before archiving the incident. Until a incident is archived, you can reactivate it from the Incidents window.	The default setting specifies 30 day.

Table 2-33 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Archive File Name	This field specifies the location on the Cisco IPICS server where the archive file is stored, and the name of the archive file.	The default location and file name is /idspri/archive/incident/ipics_incident_archive.zip
Run at	The server time at which Cisco IPICS runs the archive process each day. At this time, Cisco IPICS archives any incidents have been inactive for 30 days (by default) or for the retention period that you configured.	The default time is 00:00 (midnight), server time.
Operator Role Assignments Pane		
Restrict Operator Role assignments	If you check this box, users with the operator role can grant users (including themselves) the operator, dispatcher, or Ops view administrator roles only.	Not checked.
CUCM Settings for IDC Dialer		
CUCM Host Name or IP Address	Host name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express that the IDC uses for the dialer functionality.	—

Table 2-34 Passwords Tab in the Options Window

Setting	Description	Default Setting
User Passwords Pane		
Minimum Password Length	This setting specifies the minimum number of characters that a user can enter when creating or changing the Cisco IPICS password in the **Home > My Profile** window. See the "Managing Your User Profile" section on page 4-2. Use the drop-down list to choose a new setting. The minimum length can range from 4 to 20 characters. To ensure a strong password, you must create a password that is at least eight characters long, and includes the following elements: • At least one lower case letter • At least one upper case letter • At least one number • At least one of the following special characters: @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ? Valid values: 4 through 20.	The default setting specifies 8 characters.

Table 2-34 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Digit Password Length	This setting specifies the minimum number of numeric characters that a user can enter when creating or changing the digit password in the My Profile window, in the Home drawer of the Administration Console. Use the drop-down list to choose a new setting. The minimum length can range from 4 to 10 characters. Valid values: 4 through 10.	The default setting specifies 4 characters.
Minimum Lower Case Letter Count	This setting specifies the minimum number of lower case letters that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is set in the Minimum Password Length field. Valid values: 0 through 20.	The default setting specifies 1 character.
Minimum Upper Case Letter Count	This setting specifies the minimum number of upper case letters that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is specified in the Minimum Password Length field. Valid values: 0 through 20.	The default setting specifies 1 character.
Minimum Numeric Character Count	This setting specifies the minimum numeric character that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is specified in the Minimum Digit Password Length field. Valid values: 0 through 20.	The default setting specifies 1 character.

Table 2-34 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Special Character Count	This setting specifies the minimum special character that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. Valid values: 0 through 20.	The default setting specifies 1 character.
Password History Count	This setting specifies the number of passwords that Cisco IPICS marks as previously used, and that the user is not able to use again. For example, if the Password History Count is set to 5, the user is not able to use any of the passwords that they have used for the previous five times. **Note** This field does not apply to the ipics or ipicsadmin user IDs. Valid values: 0 through 999.	The default setting specifies 5 previous passwords.
Password Expiration Pane		
Apply User Password Expiration	This check box specifies whether Cisco IPICS applies the value that is specified in the Password Expiration field. If this check box is unchecked, there is no user password or digit expiration applied. Valid values: true or false.	This check box is unchecked by default. If this check box is not selected, the Password Expiration and Password Expiration Notification fields display as dimmed.
Password Expiration	This setting specifies the number of days before a Cisco IPICS login password and the digit password expire. For example, if the value is 180 days, the password expires after 180 days from the date that the password was created. To prevent the password from expiring, uncheck the check box in the Apply User Password Expiration setting. The Never Expired message displays in the Password Expiration Date field, in the My Profile window for the user. After a Cisco IPICS migration occurs, you may want to require all users to update their login passwords for enhanced password security. To force a login password update after a migration, configure the Password Expiration Days setting to 1; then once that one day has passed you can change the setting back to 180 days, or whatever setting you want to specify. This action forces users who log in to Cisco IPICS during that day (after the migration) to change their login passwords. Valid values: 1 through 999.	The default setting specifies 180 days.

Table 2-34 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration Notification	This setting specifies the number of days before the password expires that the user receives a warning. For example, if the specified number of days is set to 3, the user receives the warning 3 days before password expiration. **Note** This field does not apply to the ipics or ipicsadmin user IDs. **Tip** To expire passwords quickly, set the value to 1 day. The user will be forced to change the password when logging in to Cisco IPICS the following day. Valid values: 1 through 999.	The default setting specifies 3 days.
User Account Lockout Pane		
Apply User Account Lockout	This check box specifies whether Cisco IPICS applies the value that is specified in the Maximum Invalid Login Attempts Allowed field. When this check box is checked and a user exceeds the number of invalid login attempts that is specified, the user account is locked and the user can no longer log in to Cisco IPICS until the account is unlocked. For information about how to unlock an account that has been locked, see Chapter 3, "Performing Cisco IPICS Operator Tasks." **Note** This field does not apply to the ipics or ipicsadmin user IDs. If this check box is unchecked, there is no account lockout applied. Valid values: true or false.	This check box is unchecked by default. If this check box is not selected, the Maximum Invalid Login Attempts Allowed and the Failed Password Attempt Expiration fields display as dimmed.

Table 2-34 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Invalid Login Attempts Allowed	This setting specifies the maximum number of times a user can attempt to log in to Cisco IPICS with invalid login information (user name/password) before the user account gets locked out. The failed login attempts are consecutive. Valid values: 1 through 999. **Note** The user password invalid attempt count is a separate entity from the digit password invalid attempt count; however, if either password invalid attempt is exceeded, the user account is locked. When the user account is unlocked, both invalid attempt counts is reset to 0. When a user gets locked out of Cisco IPICS, a message displays stating that the user ID has been locked and that the user should contact the system administrator or operator for assistance. To unlock a user account, see Chapter 3, "Performing Cisco IPICS Operator Tasks."	The default setting specifies 5 attempts.
Failed Password Attempt Expiration	This setting specifies the number of hours that Cisco IPICS resets the Maximum Invalid Login Attempts Allowed field back to 0 once a user has reached the maximum invalid login attempts. Valid values: 1 through 999.	The default setting specifies 8 hours.

Table 2-35 Client Tab in the Options Window

Setting	Description	Default Setting
Configuration Pane		
Client Update Poll	This setting specifies the frequency that the IDC uses to poll the server for updates. For more information, see *IPICS Dispatch Console User Guide*. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 3 through 3600.	The default polling interval specifies 5 seconds.

Table 2-35 Client Tab in the Options Window (continued)

Setting	Description	Default Setting
Logout Client After	This setting configures the number of seconds an IDC client can be offline before the session expires and is forced to log out. **Note** Quick patch VTGs that are created by an IDC client session are associated to the session on the server. They are deleted from the server when the session expires and is forced to log out. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 0 through 99999. A value of 0 specifies that IDC client sessions never expire and are never forced to log out.	The default client logout interval specifies 900 seconds (15 minutes).
Maximum Video Size	This setting configures the maximum video file size that can be uploaded to the IPICS server. This setting specifies a value in MB. To change the default, double-click the current setting and enter a new value. Valid values: 1 through 2048.	The default maximum video size specifies 4 MB.
IDC Activity Logs Pane		
Disable IDC Activity Log Upload	When you check this check box, the IDC does not upload logs to the server. If you connect via a high latency (high delay), low bandwidth connection, such as a satellite link, you should check this check box. Valid values: true or false.	This check box is unchecked by default. If this check box is checked the IDC Log Upload Frequency field and the IDC Send Logs on Rollover fields are dimmed.

Table 2-35 Client Tab in the Options Window (continued)

Setting	Description	Default Setting
IDC Log Upload Frequency (IDC to server)	When an IDC client has activity logs ready to upload to the Cisco IPICS server, the IDC application places the logs in a queue. At regular intervals, the IDC client checks the queue and uploads to the server any logs that are waiting to be uploaded. Log files are copied to the **$TOMCAT_HOME/webapps/ ipics_server/pmclogs** directory, and are based on user ID and IDC ID. Log files that are not successfully uploaded get put back in to the queue and are uploaded at a later time. This setting specifies the upload interval in seconds. To change the default, double-click the current setting and enter a new value. Uploaded IDC log files are archived. Once a day, an archive utility checks for log files that are older than 14 days old and deletes them. If the total file size of the files is over 5GB, the oldest files are deleted until the total size drops below 5GB. For detailed information about IDC log files, see "Managing an End Device from the IDC Tab" section on page 3-11. Valid values: 60 through 32767.	The default upload frequency specifies 600 seconds (10 minutes).
IDC Send Logs on Rollover	Cisco IPICS defines the IDC UserInterface.log, Authentication.log, and ChannelStatistics.log log files based on a maximum size of 1MB. When any one of these log files reaches the size limit, the system creates a new log file. When you enable this option, the Cisco IPICS server retrieves the log files from the IDC based on file size rollover and renames the uploaded log file to reflect an archive copy. If you do not enable this option, the IDC deletes the log files when they reach their maximum size limit. Be aware of the following caveats: • The DebugLog.txt file does not have a size limit of 1MB, and is only uploaded to the server on request or when the IDC is started if this check box is checked (set to true). If this check box is unchecked, the DebugLog.txt file is not uploaded. • The ChannelActivity.log file is uploaded to the server every 10 minutes (or the interval that you configure in the IDC Log Upload Frequency field). Valid values: true or false.	The IDC uploads files on rollover (the check box is checked).

Table 2-35 Client Tab in the Options Window (continued)

Setting	Description	Default Setting
IDC Activity Log Update	The Cisco IPICS server retrieves activity logs from the IDC clients and updates the database with this information at regular intervals. The information is available for queries from the Activity Log window. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 30 through 32767.	The default update frequency specifies 600 seconds (10 minutes).
User Configuration Overrides		
Patch Secure Channels	This setting allows you to patch a secure channel to any other secure or unsecure channel, or to any incident or VTG. Disallowing this option prevents secure channels from being patched. **Note** Patching a secure channel into an incident is considered secure and is allowed even if patching secure channels is disallowed. You can also configure secure channel patching on a per-user basis. For more information, see the "Managing Your User Profile" section on page 4-2. Valid values: allow or disallow.	Patching secure channels is allowed.
Complex Key Settings	This setting allows or disallows all IDC clients to configure keyboard hot keys (key assignments) for individual PTT buttons and for the All Talk button. You can also configure complex key settings on a per-user basis. For more information, see the "Managing Your User Profile" section on page 4-2. Valid values: allow or disallow.	Complex key settings are allowed.

Table 2-36 SNMP Tab in the Options Window

Setting	Description	Default Setting
SNMP Thresholds: SNMP traps triggered for values above threshold		
Current Activity Log Size Threshold:	This setting specifies that an SNMP trap is sent when the activity log file reaches the designated percentage of its total allowable size. If you receive this trap, consider increasing the value in the Max Activity Logs field in the Administration > Options window.	The default setting is 80%
Used Memory Threshold	This setting specifies that an SNMP trap is sent when the root partition of a VM or the /opt partition of an MSP that is running the Cisco IPCIS server software reaches the designated percentage of its total memory.	The default setting is 80%

Table 2-36 SNMP Tab in the Options Window (continued)

Setting	Description	Default Setting
Disk Usage Threshold	This setting specifies that an SNMP trap is sent when the disk on the Cisco IPCIS server software reaches the designated percentage of its total size.	The default setting is 80%
Number Of Enabled Channels Threshold	This setting specifies that an SNMP trap is sent when the number of enabled channels reaches the designated percentage of the total number of channels that are configured.	The default setting is 80%
Number Of Active Channels Threshold	This setting specifies that an SNMP trap is sent when the number of active channels reaches the designated percentage of the total number of channels that are configured.	The default setting is 80%
Number Of Active Incident Threshold	This setting specifies that an SNMP trap is sent when the number of active incident reaches the designated percentage of the total number of incidents in the system.	The default setting is 80%
Number Of Inactive Incident Threshold	This setting specifies that an SNMP trap is sent when the number of inactive incident reaches the designated percentage of the total number of incidents in the system.	The default setting is 80%
Number Of Active VTGs Threshold	This setting specifies that an SNMP trap is sent when the number of active VTGs reaches the designated percentage of the total number of VTGs in the system.	The default setting is 80%
Number Of Users Logged In To Administration Console Threshold	This setting specifies that an SNMP trap is sent when the number of users who are logged in to the Cisco IPICS Administration Console reaches the designated percentage of the total number of Cisco IPICS users.	The default setting is 80%
Number Of Cisco Unified IP Phone Users Logged In Threshold	This setting specifies that an SNMP trap is sent when the number of Cisco IPCIS Phone users who are logged in to Cisco IPICS reaches the designated percentage of the total number of Cisco IPICS users.	The default setting is 80%
Number Of IDC Users Logged In Threshold	This setting specifies that an SNMP trap is sent when the number of IDC users who are logged in to Cisco IPICS reaches the designated percentage of the total number of Cisco IPICS users.	The default setting is 80%
Number Of Users Dialed Threshold	This setting specifies that an SNMP trap is sent when the number of users who are an a dial engine call reaches the designated percentage of the total number of Cisco IPICS users.	The default setting is 80%
SNMP Thresholds: SNMP traps triggered for values below threshold		
Free Memory Threshold	This setting specifies that an SNMP trap is sent when the root partition of a VM or the /opt partition of an MSP that is running the Cisco IPCIS server software has the designated percentage of its total memory available.	The default setting is 20%
Number of Available Voice Ports Threshold	This setting specifies that an SNMP trap is sent when the number of available voice ports is less than the designated percentage of the total number of voice ports in the system.	The default setting is 20%

Table 2-36 SNMP Tab in the Options Window (continued)

Setting	Description	Default Setting
SNMP Administration Configurations		
SNMP Version	Version of SNMP to use.	Only V2 is currently supported
SNMP Port	SNMP port on which Cisco IPICS communicates with the network management software.	The default port number is 1610
SNMP Trap Receiver	Comma delimited list of hostnames or IP addresses of the recipients of an SNMP trap event.	—
SNMP Trap Port	Port that receives SNMP traps on the network management software.	The default port number is 1620
SNMP Security Configurations		
SNMP Host	Comma delimited list of hostnames or IP addresses of the SNMP software that pools the server to fetch data.	—
SNMP Community String	Password that is required to fetch data from Cisco IPICS via SNMP.	—

Managing IDC Versions

The Cisco IPICS server maintains a repository of one or more versions of the IDC. Users can update their IDC clients at their convenience by downloading the current version of the ID utility, as described in the "Downloading the IDC" section on page 4-17.

Note You must perform the IDC configuration procedures that are in this section before users can download and install an IDC on their PC clients.

When you initially install Cisco IPICS, an IDC package is included with the server. You must generate the IDC Installer for that version to be available for download to IDC users.

When subsequent versions of the IDC becomes available, you upload the new IDC package to the Cisco IPICS server making it available for the IDC users to download to their IDC clients.

When you log in to the Cisco IPICS server from the IDC, the IDC determines whether there is a new version to which it can or must update. You configure IDC versions to designate whether an update is required or recommended. For more information about configuring the IDC versions, see the "Changing the State of IDC Versions" section on page 2-103.

As a Cisco IPICS system administrator, you can perform the following IDC version management tasks:

- Uploading IDC Versions to the Cisco IPICS Server, page 2-103
- Changing the State of IDC Versions, page 2-103
- Deleting IDC Versions, page 2-104
- Deleting IDC Versions, page 2-104

You perform the IDC version update tasks in the IDC Versions window. For more information about this window, including how to access it, see the "Understanding the IDC Versions Window" section on page 2-102.

Understanding the IDC Versions Window

The IDC Versions window allows you to specify information about IDC versions to use for IDC updates. It also enables you to upload new IDC versions to the Cisco IPICS server, and it lists information about each of the IDC versions that have been uploaded to the Cisco IPICS server.

To display the IDC Versions window in the Administration Console, navigate to **IDC Management > IDC Versions**.

Table 2-37 describes the items in the IDC Versions window.

Table 2-37 Items in the IDC Versions Window

Item	Description	Reference
Upgrade Package field	This field identifies the IDC version to be uploaded to the Cisco IPICS server.	See the "Uploading IDC Versions to the Cisco IPICS Server" section on page 2-103
Browse button	Click this button to browse to the location that contains the IDC version upgrade package to upload to the Cisco IPICS server.	
Upload button	Click this button to upload a new IDC version to the Cisco IPICS server.	
Priority field	Specifies the order of preference for IDC versions.	
Version field	This field specifies a unique version number that is assigned to the IDC version upgrade package.	
Name field	This field allows you to assign a unique identification to the IDC version upgrade package.	
State field	This field specifies the priority (state) that is assigned to the upgrade package.	See the "Changing the State of IDC Versions" section on page 2-103
Delete button	Click this button to delete an IDC version from the Cisco IPICS server.	See the "Deleting IDC Versions" section on page 2-104
drop-down list for IDC version states	Choose from this list box to configure the state for the IDC versions.	See the "Changing the State of IDC Versions" section on page 2-103
Change State button	Click this button to change the state of the IDC version.	

Uploading IDC Versions to the Cisco IPICS Server

When you upload a new IDC version, the upgrade package file is copied from a specified location on your PC to the Cisco IPICS server.

To upload an IDC version to the Cisco IPICS server, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Versions** window.

Step 2 To locate the IDC version upgrade package that you obtained from Cisco click **Browse**.

Step 3 In the Choose File window, browse to the IDC version that you want to upload and click **Open**.

The file that you choose displays in the Upgrade Package field.

Step 4 Click **Upload**.

Cisco IPICS uploads the file from your PC to the Cisco IPICS server. The IDC version displays in the IDC Versions list.

Note All new IDC versions are saved, by default, in a non-operational state. IDC users cannot download the version until you change the state to Recommended or Mandatory. See the "Changing the State of IDC Versions" section on page 2-103 for more information.

Changing the State of IDC Versions

The IDC Versions window enables you to specify various states for IDC versions. You can use states to designate whether in IDC version is a recommended or required update for an IDC user. IDC states are:

- **Recommended**—When you choose this state, the next time that an IDC client polls the Cisco IPICS server, it compares the IDC version that it is running with the recommended IDC version. If the IDC client does not match the recommended version, the IDC provides the option of upgrading to the recommended version. If a user declines to upgrade, the existing IDC version continues to work.
- **Mandatory—**When you choose this state, the next time that an IDC client polls the Cisco IPICS server, it compares the IDC version that it is running with the recommended IDC version. If the IDC client does not match the mandatory version, the IDC requires upgrading to this version.
- **Not Specified**—When you choose this state, an IDC client does not compare the IDC version that it is running with this IDC version. IDC users cannot update to an IDC version that is in the Not Specified state.

You must upload an IDC version to the Cisco IPICS server before it becomes available in any of the fields in the IDC Versions window.

To change the state of IDC versions for automatic updates, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Versions** window.

Step 2 Check the check box next to the IDC version that you want to change.

Step 3 From the drop-down list, choose the desired state.

Step 4 Click the **Change State** button.

Deleting IDC Versions

To delete IDCC versions, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Versions** window.

Step 2 Check the check box of the IDC version that you want to delete.

Step 3 Click **Delete**.

A message displays asking if you want to delete the selected version.

Step 4 Click **OK** to delete the IDC version.

This version of the IDC is completely removed from the server.

If you do not want to delete the IDC version, click **Cancel**.

Managing IDC Alert Tones

IDC tone broadcast wave (.wav) files contain alerting tones, hereafter referred to as *alert tones*, that can be broadcast to a variety of Cisco IPICS users at the same time. Cisco IPICS stores alert tones in a set on the Cisco IPICS server. The alert tone set is packaged in a .zip file that you can upload to the server and that IDC users can then download on to their client machines.

An alert tone set is associated with an ops view; therefore, each IDC user can see only one tone set based on the ops view association. For more information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

The IDC alert tone feature requires the use of compatible alerting tone files. These files must be:

- Pulse Code modulation (PCM) .wav files
- 8 bits monaural samples at 8000 Hz sampling rate
- Little Endian, 16-bit mono codec
- Normalized to –2 db
- Begin and end with silence (zero deflection) to eliminate or minimize "popping" or "clicking" sounds

As a Cisco IPICS system administrator, you can perform the following alert tone management functions:

- Creating an IDC Alert Tone Set, page 2-105
- Adding IDC Alert Tone Sets, page 2-106
- Viewing or Editing IDC Alert Tone Sets, page 2-106
- Associating an Alert Tone Set to an Ops View, page 2-107

- Deleting IDC Alert Tones, page 2-108

Creating an IDC Alert Tone Set

To provide the alert tones that get downloaded to the IDC, you must first create an IDC alert tone set and upload it to the Cisco IPICS server.

To create the tone set, perform the following procedure:

Procedure

Step 1 From any PC on which the Cisco IPICS IDC is installed, navigate to the following directory:

C:\Program Files\Cisco Systems\Cisco IDC 4.5

Step 2 Create a new empty directory and extract the example-toneset.zip file and all its contents in to the new director.

This file contains a sample alert tone set.

Step 3 Add any desired sound files in .wav format to this directory.

These files must be normalized to –2 db and must be PCM 8KHz signed, Little Endian, 16-bit mono codec.

Step 4 Open the sample alert tone .xml file by using Notepad.

Note The order in which the .wav files appear in the .xml file determine the order in which the alert tones display on the IDC.

Step 5 In Notepad, add new alert tones or delete existing alert tones by following the example below:

```
<file item="1" name="stop.wav" displayName="STOP" type="tone" priority="required" />
<file item="2" name="message.wav" displayName="Message" type="tone" priority="required" />
<file item="3" name="siren.wav" displayName="Siren" type="tone" priority="required" />
<file item="4" name="alert.wav" displayName="Alert" type="tone" priority="required" />
<file item="5" name="urgent.wav" displayName="URGENT" type="tone" priority="required" />
```

where:

"*name*" represents the .wav file to be played, and "*displayName*" is the text that displays on the IDC.

Step 6 Save the example tone set .xml file and rename the .xml file to a name that identifies the tone set to you.

Note You must save the .xml file in UTF-8 format. If you are using Notepad, choose UTF-8 from the Encoding drop-down menu in the Save As dialog box.

Step 7 Delete any files that you do not want from the directory.

Step 8 Navigate to the directory that contains the .xml and .wav files and select all of the .wav files and the .xml file.

Step 9 Right-click the selected files and choose **Send To > Compressed Folder**.

Tip You can also use WinZip or a similar utility to compress the files.

Step 10 To enable an IDC user to press a button on the IDC to stop an alert tone from playing, for displayName enter the name "STOP" but give the name an invalid file name, such as "stopplayout.wav," then edit the alert tone file with this information, as if it were a real alert tone.

Step 11 You can now upload the compressed IDC alert tone set to the Cisco IPICS server.

See the "Associating an Alert Tone Set to an Ops View" section on page 2-107 for information about how to upload a tone set.

Note You can use Windows Sound Recorder to save .wav files in the required format.

Adding IDC Alert Tone Sets

To add a new IDC alert tone set, perform the following procedure.

Tip The Stop alert tone should be included in each tone set that you upload to the Cisco IPICS server. This alert tone allows users to press the Stop alert tone to stop an alert tone that is currently playing. You should ensure that the Stop alert tone is included in an alert tone set that you upload to the Cisco IPICS server. If your tone set does not contain a .wav file called Stop, you can use an alert tone that is named something similar, such as Silence. See the "Creating an IDC Alert Tone Set" section on page 2-105 for information about how to create an alert tone set.

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

Step 2 Click **Add**.

A blank alert tone detail window displays.

Step 3 In the Set Name field, enter a name for the alert tone set.

Step 4 In the Description field, enter a description for the alert tone set.

Step 5 Click the **Browse** button use the File Upload pop-up window to identify the files to upload.

Step 6 Click **Save**.

The tone set gets uploaded to the server and is available for use by IDC users.

The alert tone set name, file size, and MD5 summary information of the new alert tone set also displays.

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

Step 7 To associate an alert tone set to an ops view, click the Ops View tab and follow the steps in the "Associating an Alert Tone Set to an Ops View" section on page 2-107.

Viewing or Editing IDC Alert Tone Sets

To view or edit the IDC alert tone sets that are available for use in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

Step 2 Click the link in the Name column for the alert tone set that you want to view or edit.

An alert tones detail window displays current information about the tone set that you chose.

Step 3 To download the alert tone set without making any changes, click the **Download** button.

Step 4 To edit the information for the alert tone set, take any of the following actions:

- In the Name field, enter a new name for the alert tone set.
- In the Description field, enter a new description for the tone set.
- Click the **Browse** button to upload and overwrite the existing tone set.

Step 5 Click **Save**.

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

Step 6 To associate an alert tone set to an ops view, click the Ops View tab and follow the steps in the "Associating an Alert Tone Set to an Ops View" section on page 2-107.

Associating an Alert Tone Set to an Ops View

You can associate an alert tone set to an ops view while you are adding a new alert tone set, or you can associate an ops view to an existing tone set. Associating an alert tone set to an ops view ensures that IDC users can see only the tone set that is associated with the ops view to which they belong.

To associate an alert tone set to an ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

Step 2 In the Name column, click the alert tone set link that you want to associate with an ops view.

Step 3 Click the **Ops Views** tab.

Step 4 Take any of the following actions:

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

Step 5 Click **Save** to save the ops view that you want to associate to the alert tone set in the Associated Ops Views list.

IDC users can now only see the alert tone set that is in the ops view to which they belong.

Note The user(s) that you want to have access to the tone set must be assigned the appropriate permissions in Cisco IPICS to see the tone set, and must also belong to the same ops view to which the tone set is associated.

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

Deleting IDC Alert Tones

To delete IDC tones, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

Step 2 Check the check box to the left of the name of the tone that you want to delete.

Step 3 Click **Delete**.

The alert tone that you deleted is no longer available for use by the IDC users.

Note If you want to delete all of the existing alert tones, check the check box at the top of the alert tones list and click **Delete**.

Managing the IDC Installer

Before an IDC user can download a new IDC version to a clients, you must configure the IDC Installer.

The IDC Installer installs the IDC on IDC client machines. The IDC installer, called idcsetup.exe, downloads to an IDC client when a IDC user clicks the **Download IDC** link in the Home drawer, as described in the "Downloading the IDC" section on page 4-17.

As a Cisco IPICS system administrator, you can upload a new IDC package and generate the IDC Installer as described in the "Generating the IDC Installer" section on page 2-109.

You perform these tasks in the IDC Installer window. For more information about this window, including how to access it, see the "Using the IDC Installer Window" section on page 2-108.

Using the IDC Installer Window

The IDC Installer window contains configuration information that is necessary to generate an IDC installer.

To display the IDC Installer window, navigate to the IDC Management drawer in the Cisco IPICS Administration Console and click the **IDC Installer** link.

The Installer Status field displays the date and time that an idcsetup.exe file was last generated, and displays the IP address defined by the bundled idc.ini file. These files are used to install the IDC.

Generating the IDC Installer

Generating an IDC Installer installs a new IDC version package. It also makes the IDC version package available for download from the **Download IDC** link in the Home drawer (see the "Downloading the IDC" section on page 4-17).

For information about configuring additional IDC options, see the "Managing Cisco IPICS Options" section on page 2-89.

To generate an IDC Installer, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Installer** window.

Step 2 Take one of these actions to specify the IP address that the IDC uses to contact the Cisco IPICS server:

- To specify the IP address of the Cisco IPICS server that you are accessing to generate the IDC installer, choose the radio button that appears next to the IP address.
- To choose a different IP address, click the **Other** radio button and enter the IP address.

  If you use this option, the IP address that you enter should be tested in the network domain that is supported with that server to ensure that NAT or firewall restrictions do not prevent the IDC from connecting to that server.

In a high availability deployment, specify the IP address of the primary server. Information about the secondary server is provided to the IDC automatically so that the IDC properly fails over to the secondary server if the primary server goes down.

Step 3 In the HTTP Port field, enter the port number that is used for non-secure HTTP communication between the IDC and the server.

Step 4 In the HTTPS Port field, enter the port number that is used for secure HTTPS communication between the IDC and the server.

Note Cisco recommends that you use the default HTTP and HTTPS ports that are listed in the IDC Installer Configuration area. The IP address, HTTP port, and HTTPS port fields affect only the IDC installer and do not have an immediate effect on IDC clients that have already been installed on user PCs. If you need to change these values, Cisco recommends that you notify all users that they need to download and reinstall the IDC using the new idcsetup.exe that is generated after you save the changes to these values.

Step 5 From the IDC Version To Be Used For The IDC Installer drop-down list, choose the version number of the IDC that you want the users install.

The drop-down list should be populated with the version numbers of the idcinst.exe files that have been uploaded to the Cisco IPICS server. See the "Managing IDC Versions" section on page 2-101 for more information.

Note There is only one IDC installer and all IDC users who use that installer automatically receive a complete application of that IDC version.

Step 6 Click **Save**.

IDC users can now download a new version of the IDC application, as described in the "Downloading the IDC" section on page 4-17.

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

Managing IDC Regions

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

When you configure new regions in the Cisco IPICS server, they are represented by tabs that display in the IDC. The position of the region in the IDC Regions window in the Administration Console determines where the region displays on the IDC.

You create regions in the **IDC Management > IDC Regions** window in the Administration Console. You can configure up to 20 regions.

You can add new IDC regions, as well as edit and delete existing regions, as described in the following procedures:

- Understanding the IDC Regions Window, page 2-110
- Adding IDC Regions, page 2-111
- Viewing or Editing IDC Regions, page 2-112
- Deleting IDC Regions, page 2-112

Understanding the IDC Regions Window

The IDC Regions window allows you to create new IDC regions that display on the IDC. You can also edit and delete existing IDC regions in this window.

The IDC Regions window lists information about each of the IDC regions that have been created in the Cisco IPICS server.

To display the IDC Regions window, navigate to the **IDC Management > IDC Regions** window.

Table 2-38 describes the items in the IDC Regions window.

Table 2-38 Item in the IDC Versions Window

Item	Description	Reference
Name field	This field specifies the name of the IDC regions.	See the "Adding IDC Regions" section on page 2-111 and the "Viewing or Editing IDC Regions" section on page 2-112
Short Name field	This field specifies the shortened name of the regions.	
Position field	This field specifies the position of the regions on the IDC display.	
Add button	Click this button to add a new IDC region to the Cisco IPICS server.	See the "Adding IDC Regions" section on page 2-111

Table 2-38 Item in the IDC Versions Window (continued)

Item	Description	Reference
Delete button	Click this button to delete an IDC region.	See the "Deleting IDC Regions" section on page 2-112

Adding IDC Regions

To add a new IDC region, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Regions** window.

Step 2 Click **Add**.

A blank New IDC Region detail window displays.

Note This button is dimmed if 20 regions are already configured. In this case, you must delete a region before you can add a new one.

Step 3 In the Name field, enter a name for the region.

Step 4 In the Short Name field, enter a condensed name for the region.

Tip The short name can be a shortened version of the full name or the same as the region position.

Step 5 From the Position drop-down list, choose a position for the region.

Position indicates where the region appears in the Regions list in the IDC. Position 1 indicates the top position, and 6 indicates the bottom position. If you want to assign a region to a position that is in use, you must delete the in-use region first, as described in the "Deleting IDC Regions" section on page 2-112.

Step 6 (Optional) In the Description field, enter a description of the region.

Step 7 Click **Save**.

The region displays in the list of IDC regions and is available to assign to a channel/VTG while creating/updating channel/VTGs.

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

Viewing or Editing IDC Regions

To view or edit the IDC regions that are available for use in Cisco IPICS, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Regions** window.

Step 2 In the Name column, click the link for the IDC region to view or edit.

A window displays current information about the region that you choose.

Step 3 To edit the information for the region, take any of the following actions:

- In the Name field, enter a new name for the region.
- In the Short Name field, enter a new condensed name for the region.
- From the Position drop-down list, choose the position that the region appears in the Regions list in the IDC.
- In the Description field, enter a new description for the region.

For a description of the fields in this window, see the "Adding IDC Regions" section on page 2-111.

Step 4 Click **Save**.

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

Deleting IDC Regions

To delete IDC regions, perform the following procedure. When you delete an IDC region, any associated channels and VTGs are moved to region 1.

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Regions** window.

Step 2 Check the check box to the left of the region that you want to delete.

Step 3 Click **Delete**.

The region that you deleted is no longer available for use by the IDC users.

Configuring LDAP

Cisco IPICS lets you use the Lightweight Directory Access Protocol (LDAP) to authenticate against an Active Directory (AD) server users who access Cisco IPICS.

Note The values that are configured in the AD for a user in the **Display name** field in the General tab and the **User logon name** field in the Account tab must be identical. If they are not, the user cannot log in to Cisco IPICS.

This section describes how to configure the general settings that are required for LDAP authentication of users. In addition, you must make the following settings:

- Create an ops view and enable it for LDAP (or enable the System ops view for LDAP). For instructions, see the "Adding Ops Views" section on page 7-12.
- Configure users that are to use LDAP authentication to belong to the ops view that is enabled for LDAP. For instructions, see the "Choosing an Ops View to Which a User Belongs" section on page 3-24.

To configure general settings for LDAP authentication, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > LDAP** window.

Step 2 In the LDAP Configuration window, take these actions:

a. In the Host Name / IP Address field, enter the host name or the IP address of the LDAP server in your network.

b. In the LDAP Port field, enter the port number on the LDAP server that Cisco IPICS uses to communicate with that server.

Typically, this port number is 389 for non-secure communication or 636 for secure communication. The port number that you enter must match the port number that is configured in the LDAP server.

c. In the LDAP Timeout field, enter the maximum number of seconds that can pass before a connection from Cisco IPICS to the LDAP server fails.

The default value is 30. Valid values are 5 through 180.

d. Check the **Use LDAPS** check box if you want to use secure LDAP.

In this case, Cisco IPICS downloads the SSL certificate from the LDAP server and uses this certificate to encrypts data that is sent between Cisco IPICS and the LDAP server. The certificate is downloaded when you save the configuration settings that you are making.

When this check box is checked, the Certificate Security Configuration fields appear, which show the serial number and expiration date of the LDAP certificate

Step 3 Click **Save**.

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