



# 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 channels. The system administrator also manages the Cisco IPICS licenses and PMC versions, monitors the status of the system, reviews log files, as needed, and creates operational views.

In addition, the system administrator is responsible for performing backup and restore operations. For more information, see [Chapter 9, “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 1-11, 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 PTT Channels and Channel Groups, page 2-2](#)
- [Managing Locations, page 2-38](#)

- [Managing the Multicast Pool, page 2-47](#)
- [Managing the RMS, page 2-56](#)
- [Managing Licenses, page 2-72](#)
- [Viewing Active Users, page 2-79](#)
- [Managing Activity Logs, page 2-83](#)
- [Managing Activity Log Options Per Ops View, page 2-89](#)
- [Managing Cisco IPICS Options, page 2-91](#)
- [Managing PMC Versions, page 2-106](#)
- [Managing PMC Alert Tones, page 2-112](#)
- [Managing PMC Skins, page 2-119](#)
- [Managing the PMC Installer, page 2-122](#)

For information about managing operational views in the Ops Views window, see [Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”](#)

For information about managing database backup and restore operations in the Database Management window, see [Chapter 9, “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 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 2-7](#)
- [Viewing and Editing Channel Details, page 2-8](#)
- [Changing the Status of a PTT Channel, page 2-20](#)
- [Understanding Association Attribute Behaviors, page 2-21](#)
- [Associating PTT Channels to Ops Views, page 2-23](#)
- [Associating Users to PTT Channels, page 2-24](#)
- [Viewing Channel Associations, page 2-26](#)
- [Deleting a PTT Channel, page 2-27](#)

### Channel Group Management Tasks

- [Adding a Channel Group, page 2-30](#)
- [Viewing and Editing Channel Group Details, page 2-31](#)
- [Viewing Channel Group Associations, page 2-34](#)
- [Removing a PTT Channel from a Channel Group, page 2-35](#)
- [Associating Ops Views to Channel Groups, page 2-36](#)
- [Deleting a Channel Group, page 2-37](#)

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 2-28.

## 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 box 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
<b>Filter</b>		
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 and then click <b>Go</b> .
Ops View drop-down list box	This field allows you to display only channels for which the associated ops view matches the information that you choose.	
<b>Go</b> button	Click this button to display channels by the filters that you choose.	
<b>Clear Filter</b> button	Click this button to remove filter selections and display an empty list of channels.  Click the <b>Channels</b> link again to display the full list of entries.	
<b>Channel Information</b>		
Channel Name field	This field allows you to assign a unique identification to the channel.	See the “ <a href="#">Viewing and Editing Channel Details</a> ” section on page 2-8 and the “ <a href="#">Adding a PTT Channel</a> ” section on page 2-7

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

Item	Description	Reference
Ops View field	This field indicates the ops view to which the channel belongs.	See the <a href="#">“Associating PTT Channels to Ops Views”</a> section on page 2-23
Secure field	This field indicates whether the channel is secure.	See the <a href="#">“Viewing and Editing Channel Details”</a> section on page 2-8
Codec field	This field specifies the codec (G.711 or G.729) that is used by this channel.	
VTG field	This field indicates whether the channel is allowed in a Virtual Talk Group (VTG).	See the <a href="#">“Viewing and Editing Channel Details”</a> section on page 2-8 and the <a href="#">“Adding a PTT Channel”</a> section on page 2-7
Users field	This field indicates whether the channel is allowed to be associated to users to affect all endpoints such as the PMC and IP phone.	
Channel Status field	This field indicates whether the channel is enabled, disabled, or active.	See the <a href="#">“Changing the Status of a PTT Channel”</a> section on page 2-20
Prompt field	<p>This field indicates whether a spoken name prompt is recorded for the channel.</p> <p>This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface.</p> <p>You can record the spoken name prompt for a user by clicking the <b>Not Recorded</b> or the <b>Recorded</b> link in the Prompt column. When you click a link in the Prompt column, the Spoken Names window displays.</p>	See Chapter 8, <a href="#">“Configuring and Managing the Cisco IPICS Policy Engine”</a>
Add button	Click this button to add a new channel in Cisco IPICS.	See the <a href="#">“Adding a PTT Channel”</a> section on page 2-7
Delete button	Click this button to delete the specified channel(s).	See the <a href="#">“Deleting a PTT Channel”</a> section on page 2-27

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

Item	Description	Reference
Change Status drop-down list box	Choose from the enable or disable option to change the status of a channel.	See the “ <a href="#">Changing the Status of a PTT Channel</a> ” section on page 2-20
<b>Associations</b> button	Click this button to view associations for the specified channel.	See the “ <a href="#">Associating Users to PTT Channels</a> ” section on page 2-24 and the “ <a href="#">Viewing Channel Associations</a> ” section on page 2-26

For information about the icons that appear in the Channels and Channel Groups windows, see the “[Understanding the Channels and Channel Groups Window Icons](#)” section on page 2-6.

## Understanding the Channels and Channel Groups Window Icons

Icons in the Channels and Channel Groups windows provide information about each channel name and channel group, as described in [Table 2-2](#).

**Table 2-2** *Channel Group and Channel Icons*

Icon	Meaning
	PTT channel
	Channel group
	Busy PTT channel A channel is busy when it is use by an active VTG
	Secure PTT channel You can designate a PTT channel as secure when you add the channel in Cisco IPICS

**Table 2-2** Channel Group and Channel Icons

Icon	Meaning
	Unavailable PTT channel A channel is unavailable when it is disabled.
	PTT Channel Not Present—A channel is not present when it is used by an active VTG
	VTG
	User

## 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 [“Managing Locations”](#) section on page 2-38.

To add a new channel, perform the following procedure:

### Procedure

- 
- Step 1** From the Cisco IPICS Administration Console, navigate to **Configuration > Channels**.
  - 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 2-8.
  - Step 4** Enter appropriate information in the Ops Views fields as described in the [“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 **Configuration > Channels**.
- 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 2-3](#) provides descriptions of the fields in the General tab.



**Note** If an endpoint, such as the PMC or dial engine, does not support the attributes that are described in [Table 2-3](#), then the attributes will not display in the General tab of the Channels window.

---

**Table 2-3** General Tab Fields in Channels Window

Field	Description
<b>Channel Information</b>	
Channel Name	<p>This field represents the name of the channel.</p> <p>The name can include alphanumeric characters, spaces, and any of these characters: “. , - ‘ # ( ) / : _”.</p> <p>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 will use it, or for a particular geographic region (for example <i>Fire Department</i> or <i>North Area</i>).</p> <hr/> <p> <b>Note</b> The PMC may truncate the channel name if the name includes more characters than the PMC can display.</p> <hr/>
Description— <i>Optional</i>	This field allows you to enter a description for this channel.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Preferred Codec	<p>This drop-down list box allows you to choose the Codec (G.711 or G.729) that will be used by this channel.</p> <p>Use G.711 if this channel should be available to Cisco Unified IP Phone users or if it will be part of a VTG.</p> <p>Use G.711 or G.729 if this channel will be available to PMC users. G.729 requires digital signal processor (DSP) resources for transcoding.</p> <hr/> <p> <b>Note</b> The codec and media connection attributes cannot be edited if users, who are associated to the channel, are logged in to an IP phone or a PMC.</p> <hr/> <p>For more information about codecs, refer to the <a href="#">Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)</a>.</p>
Secure Channel	<p>This drop-down list box allows you to specify whether this channel is a secure channel.</p> <p>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.</p> <hr/> <p> <b>Note</b> This field displays as read-only if the channel is a participant in an active VTG. To make the field editable, either disable the channel, or deactivate the VTG of which the channel is a participant.</p>

**Table 2-3** *General Tab Fields in Channels Window (continued)*

Field	Description
Allow association to users	<p>This check box allows you to indicate whether this channel is available to PMC users. It is used to prevent certain channels from being associated to users.</p> <p>If the channel is configured to disallow association to a user (attribute check box is not checked), then the channel does not display as available to users in the User window and is not available on the PMC. The User tab, in the channel Association window, is removed.</p> <hr/> <p> <b>Note</b> If you change the channel status such that the channel can no longer be associated with a user and the channel was previously associated to one or more users, Cisco IPICS automatically removes the channel associations from the users. This attribute is checked by default upon creation of the channel.</p>

**Table 2-3** General Tab Fields in Channels Window (continued)

Field	Description
Allow use in VTGs	<p data-bbox="628 293 1224 380">This check box allows you to indicate whether this channel is an available resource for participation in a VTG</p> <p data-bbox="628 402 1224 740">This setting is used to prevent certain channels from being included in a VTG. For example, a PMC user interacting with a handset user may wish to hear all the call progress tones that the handset generates, to give feedback when a radio channel is available. These types of progress tones can be assigned to this certain 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 it to be used in VTGs.</p> <p data-bbox="628 763 1224 1010">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 the VTGs. The channel can, however, display as available for association to users and user groups, in the User and User Groups windows.</p> <p data-bbox="628 1032 1224 1151">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.</p> <p data-bbox="628 1174 673 1211"></p> <p data-bbox="628 1218 1224 1276"><b>Note</b> This attribute is checked by default upon creation of the channel.</p>

**Table 2-3** General Tab Fields in Channels Window (continued)

Field	Description
Status— <i>Display only</i>	<p>This field displays one the following channel states:</p> <ul style="list-style-type: none"><li>• Active—Channel is connected to a VTG</li><li>• Inactive—Channel is not connected to a VTG but could potentially be in use by PMC users or IP phone users</li><li>• Enabled—Channel is available (channel can be connected to a VTG) and PMC clients can use the channel</li><li>• Disabled—Channel is not in use and PMC 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.</li></ul>

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
<b>Media Connection Assignments</b>	
Location	<p>Channels or users who are associated with the same location can communicate with each other without additional network configuration. Users from other locations can only access this channel through a SIP connection.</p> <p></p> <p><b>Note</b> Channels achieve media connectivity by being mapped to a multicast address in a location. A channel can be assigned to multiple locations. In this case, a channel can have more than one media connection. The count in the <b>Serviceability &gt; Dashboard</b> window reflects the total number of media connections. See the <a href="#">“Viewing the Information in the Dashboard Window” section on page 10-2</a> for more information about the Dashboard window.</p> <p>If the network is configured so that the channel can be accessed by users in every location, set this value to <b>All</b>.</p> <p>See the <a href="#">“Managing Locations” section on page 2-38</a> for more detailed information about how to configure locations.</p>
Type	<p>This field specifies the type of connection that Cisco IPICS and devices use to connect to this channel when connecting from the corresponding location.</p> <p></p> <p><b>Note</b> The multicast connection type is currently the only type that is available and is selected by default.</p>

**Table 2-3** General Tab Fields in Channels Window (continued)

Field	Description
Address	<p>This field specifies the multicast address, in the corresponding location, that is used to connect to this channel</p>  <hr/> <p><b>Note</b> 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 <a href="#">“Guidelines for Using IP Multicast Addresses with Cisco IPICS”</a> section on page 2-51.</p> <hr/> <p>Two channels in the same location cannot have the same multicast address. See the <a href="#">“Managing Locations”</a> section on page 2-38 for more detailed information about locations.</p>
Port	<p>This field specifies the multicast address port number, in the corresponding location, that is used to connect to this channel.</p> <p>This value must be an even number in the range of 21000 through 65534.</p>  <hr/> <p><b>Note</b> Cisco IPICS does not allow the configuration of ports below 21000 or any odd ports.</p>

**Ops Views**

**Table 2-3** General Tab Fields in Channels Window (continued)

Field	Description
Belongs To	<p>This drop-down list box allows you to choose the ops view to which you want to associate this channel. See the <a href="#">“Associating PTT Channels to Ops Views”</a> section on page 2-23 for detailed information.</p> <hr/> <p> <b>Note</b> To associate a channel to an ops view, you must belong to the SYSTEM ops view.</p> <hr/> <p>For general information about ops views, see <a href="#">Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”</a></p>
Accessible To	<p>This drop-down list box allows you to choose the ops views to which you want this channel to be accessible. See the <a href="#">“Associating PTT Channels to Ops Views”</a> section on page 2-23 for information about how to associate ops views to channels.</p> <p>For general information about ops views, see <a href="#">Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”</a></p>
Edit button	<p>This button allows you to make this channel accessible to ops views.</p> <p>See the <a href="#">“Associating PTT Channels to Ops Views”</a> section on page 2-23 for more information.</p> <p>For general information about ops views, see <a href="#">Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”</a></p>

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

The PMC tab for the selected channel displays. This window contains PMC information for this channel. [Table 2-4](#) provides descriptions of the fields in the PMC tab.

Table 2-4 *PMC Tab Fields in Channels Window*

Field	Description
<b>PMC</b>	
RX Mute During PTT	<p>This attribute specifies the transmission settings for all channels or only one channel; it controls the audio for the active channels while you are transmitting.</p> <p>The following values affect how the mute functionality is configured on the PMC:</p> <ul style="list-style-type: none"> <li>• None—When PTT is engaged, the channel is muted.</li> <li>• All—When PTT is engaged, RX (receive transmission) is muted on all channels.</li> <li>• Channel—When PTT is engaged, RX is muted for this channel only.</li> </ul> <p> <b>Note</b> When you initially assign a channel to the PMC, the RX mute settings that you have configured apply. The PMC user can modify this setting, however, if you change the setting after the channel has been assigned to the user, the changes do not become effective.</p>
Enable Voice Activity Detection (VAD)	<p>When VAD is enabled on Cisco IPICS, the PMC only sends voice traffic when it detects a voice packet.</p> <p>When this attribute is set to true (attribute check box is checked) on a channel/VTG, VAD will be used by the PMC while communicating with the channel/VTG.</p> <p>By default, this attribute is set to true (attribute check box is checked).</p>
Allow Latch	<p>When set to true (attribute check box is checked) on a channel/VTG, the user can use latch (lock in channels) on any channel that you specify.</p> <p>By default, this attribute is set to true (attribute check box is checked).</p>

**Table 2-4** *PMC Tab Fields in Channels Window (continued)*

Field	Description
Listen Only	When set to true (attribute check box is checked), the user can hear, but cannot talk, on the channel.
Channel Color	Color tag that you can choose from a drop-down list box  This setting uniquely 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 box.
	 <p><b>Note</b> If you do not want the channel to be tagged with a color, then you can choose <b>Not colored</b> from the drop-down list box.</p>

**Step 4** To view channel associations, click the **Associations** button that appears at the bottom of the window.

**Step 5** To view channel associations, from the Associations window take either 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 with this channel display. The Users window lists information about each of the users who are associated to the channel.

[Table 2-5](#) describes the items in the Users window.

**Table 2-5** *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.

**Table 2-5** *Items in the Users Window*

Item	Description
First Name field	This field specifies the first name of the user.
Status field	This field indicates whether the user is enabled or disabled.
<b>Association Attributes</b>	
Latchable field	This field indicates whether the user can latch (lock in) channels on the PMC.
Disable Audio field	This field indicates whether audio is disabled on the PMC.
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 will be appended with a superscript (1) if they are configured as a customized value. See the [“Understanding Association Attribute Behaviors”](#) section on page 2-21 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 2-24.

- Click the **Virtual Talk Groups** tab—This tab displays the VTGs in which this channel participates.

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

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



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

- Step 7** From the Change End Device Status drop-down list box, choose one of the available options:
- **Allow Latch**—PMC user can latch, or lock in, channels
  - **Disallow Latch**—PMC user cannot latch channels
  - **Set Listen Only**—PMC user can only listen on the channel; transmission is not allowed
  - **Unset Listen Only**—PMC user can listen and transmit on the channel
  - **Enable Audio**—Audio is enabled on the PMC
  - **Disable Audio**—Audio is disabled on the PMC



---

**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 (PMC, 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.

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

For more information about the PMC, refer to the [Cisco IPICS PMC Installation and User Guide](#).

A channel can have either of the following statuses:

- **Enabled**—Channel is available for use
- **Disabled**—Channel is not available for use

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 **Configuration > Channels**.

**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**, and 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 box.
- 

## 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 PMC 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 2-22](#).

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 will be 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 2-22 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 2-24.

## User-Channel Association Example

The following example describes different user-channel association scenarios 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 the User A is not allowed to latch on Channel A on the PMC. 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 > PMC** window. Because the association settings have not been customized, Cisco IPICS automatically updates the User A-Channel A association. The PMC 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 PMC 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 PMC 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 will override the custom PMC 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 PMC.

See the [“Viewing and Editing Channel Details” section on page 2-8](#) 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 2-24](#).

For more information about the PMC, refer to the [Cisco IPICS PMC Installation and User Guide](#).

## 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 6, “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 **Configuration > Channels**.
- 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 and then click > or <, or double-click the ops view.
  - To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click > or <.
  - To move all ops views from one list to the other at one time, click >> or <<.
- Step 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 box.
- 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 a PMC or a properly-configured Cisco Unified IP Phone.

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 2-7](#) for more information.

To associate users to channels, perform the following procedure:

**Procedure**

- 
- Step 1** From the Administration Console, navigate to **Configuration > Channels**.
- 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 that 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 box—Choose from a list of locations

See the “[Managing Locations](#)” section on page 2-38 for detailed information about how to configure locations.

- Role drop-down list box—Choose from a list of Cisco IPICS roles
- Ops View drop-down list box—Choose from a list of ops views

**Step 4** To search for a user, enter your search criteria and 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 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.

## Viewing Channel Associations

You can view channel associations by performing the following procedure:

### Procedure

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

**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 is 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 2-24.

---

- **Virtual Talk Groups**—View the VTGs in which this channel is participating
- 

## 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:

### Procedure

---

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

**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 box 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 2-6](#) describes the items in the Channel Groups window.

**Table 2-6** *Items in the Channel Groups Window*

<b>Item</b>	<b>Description</b>	<b>Reference</b>
<b>Filter</b>		
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 and then click <b>Go</b> .
Ops View drop-down list box	Allows you to display only channel groups for which the associated ops view matches the information that you choose	
<b>Go</b> button	Displays channel groups by the filters that you choose	
<b>Clear Filter</b> button	Removes filter selections and displays an empty list of channel groups	
<b>Channel Group Information</b>		
Channel Group Name field	Name that is assigned to the channel group	See the <a href="#">“Viewing and Editing Channel Group Details”</a> section on page 2-31 and the <a href="#">“Removing a PTT Channel from a Channel Group”</a> section on page 2-35
Ops View field	Ops view to which the channel group belongs	See the <a href="#">“Associating Ops Views to Channel Groups”</a> section on page 2-36

**Table 2-6** *Items in the Channel Groups Window (continued)*

<b>Item</b>	<b>Description</b>	<b>Reference</b>
<b>Add</b> button	Allows you to add a new channel group in Cisco IPICS	See the “ <a href="#">Removing a PTT Channel from a Channel Group</a> ” section on page 2-35
<b>Copy</b> button	Allows you to copy information from an existing channel group when you add a new channel group	
<b>Delete</b> button	Allows you to delete a channel group	See the “ <a href="#">Deleting a Channel Group</a> ” section on page 2-37
<b>Associations</b> button	Displays the Associations window for a channel group	See the “ <a href="#">Associating Ops Views to Channel Groups</a> ” section on page 2-36 and the “ <a href="#">Viewing Channel Group Associations</a> ” section on page 2-34

## Adding a Channel Group

A channel group provides a way to organize channels. You may find it useful to create and name channel groups according to location (for example, South Area PTT Channels) or function (for example, Executive PTT Channels).

To create a channel group, perform the following procedure:

### Procedure

- 
- Step 1** From the Administration Console, navigate to **Configuration > Channel Groups**.
- 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 add a channel group starting with a New Channel Group window that includes information based on an existing channel group, check the check box next to the existing channel group; then click **Copy**.



---

**Note** The **Copy** button is 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 2-31, 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 or VTG template, see the “[Managing VTGs](#)” section on page 4-2.

## 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 2-30.

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

**Procedure**

- Step 1** From the Administration Console, navigate to **Configuration > Channel Groups**.
- 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 2-7](#) provides a description of the fields in the General tab.

**Table 2-7 General Tab Fields in Channel Groups Window**

<b>Field</b>	<b>Description</b>
<b>Channel Group Information</b>	
Channel Group Name	Name of the channel group The name can include alphanumeric characters, spaces, and any of these characters: “. , - ‘ # ( ) / : _”.
Description	<i>Optional.</i> Description of the channel group
<b>Ops View</b>	
Belongs To	Name of the ops view to which you want to associate this channel group.  For general information about ops views, see <a href="#">Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”</a>

**Table 2-7** General Tab Fields in Channel Groups Window (continued)

Field	Description
Accessible To	Name of the ops view to which you want this channel group to be accessible.  For general information about ops views, see <a href="#">Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”</a>
<b>Edit</b> button	Click this button to associate ops views to the channel group. See the <a href="#">“Associating Ops Views to Channel Groups”</a> section on page 2-36 for detailed information.
	 <p><b>Note</b> To associate a channel group to an ops view, you must belong to the SYSTEM ops view.</p>

- Step 4** To view or update members who are associated with this channel group, click the **Members** tab. [Table 2-8](#) provides a description of the fields in the Members tab.

**Table 2-8** 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
Codec	Represents the preferred codec of the channel member
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 box—Allows you to choose from a list of ops views
- Step 6** To search for a channel, enter your search criteria and 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 2-34.
- 

## Viewing Channel Group Associations

To view channel group associations, perform the following procedure:

### Procedure

---

- Step 1** From the Administration Console, navigate to **Configuration > Channel Groups**.
- 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 2-9 provides descriptions of the fields in the Associations window.

**Table 2-9** *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: <ul style="list-style-type: none"> <li>• Active—Channel group is a participant in an active VTG</li> <li>• Idle—Channel group is a member of a VTG template</li> </ul>

## 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 **Configuration > Channel Groups**.
- 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 2-31.

---

## 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 6, “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 **Configuration > Channel Groups**.

- 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 and then click > or <, or double-click the ops view.
  - To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click > or <.
  - To move all ops views from one list to the other at one time, click >> or <<.
- Step 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 box, 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 **Configuration > Channel Groups**.
- 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. This section includes the following topics:

- [Predefined Cisco IPICS Locations, page 2-38](#)
- [Location Associations, page 2-40](#)
- [Summary of Access Types and Connections, page 2-43](#)

## 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.

**Note**

---

The ALL defines the scope or reachability of a multicast address. For this reason, the ALL location is applicable 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.

---

- 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 PMC users. When a PMC user chooses the REMOTE location from the Location drop-down list box, 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 PMC 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 PMC 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 PMC 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 PMC user activates the channel or VTG, the PMC 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 PMC 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: PMC 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: PMC 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: PMC 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.
  - PMC—During the login process, the PMC user chooses their 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 PMC 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—IP phones only support 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 10](#) shows a summary of the Cisco IPICS access types and connections, as they pertain to locations.

**Table 10** Cisco IPICS Access Types and Connections

<b>Access</b>	<b>Type of Connection</b>	<b>Description</b>
IP Phone	Multicast (in all cases)	<ul style="list-style-type: none"> <li>• Can connect to any VTG that the IP phone user is associated with.</li> <li>• 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.</li> </ul>
Dial-in	Unicast to the dial engine (in all cases)	<ul style="list-style-type: none"> <li>• Can connect to any channel or VTG that the dial-in user is associated with.</li> </ul>
PMC (remote login)	Unicast	<ul style="list-style-type: none"> <li>• All channels and VTGs are unicast calls to the appropriate RMS.</li> </ul>
PMC (non-remote login)	Multicast	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Can connect to any VTG that the user is associated with.</li> </ul>
PMC (non-remote login)	Unicast	<ul style="list-style-type: none"> <li>• Can connect to any channel that is configured with a location that is different from the location that was chosen at login.</li> </ul>

You can perform the following location-related management tasks:

- [Understanding the Locations Window, page 2-45](#)
- [Adding a Location, page 2-45](#)
- [Viewing or Editing a Location, page 2-46](#)
- [Deleting a Location, page 2-47](#)

## 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 **Configuration > Locations** link.



### Note

By default, location names appear in ascending alphanumeric order.

[Table 2-11](#) describes the items in the Locations window.

**Table 2-11** *Items in the Locations Window*

Item	Description	Reference
Location Name field	Specifies the name that is assigned to the location	See the <a href="#">“Viewing or Editing a Location”</a> section on page 2-46
<b>Add</b> button	Allows you to add a new location in Cisco IPICS	See the <a href="#">“Adding a Location”</a> section on page 2-45
<b>Delete</b> button	Allows you to delete a location	See the <a href="#">“Deleting a Location”</a> section on page 2-47

## Adding a Location

You can add locations to Cisco IPICS, as needed.

To add a location, perform the following procedure:

### Procedure

- 
- Step 1** From the Administration Console, navigate to **Configuration > Locations**.
  - Step 2** To add a location starting with a blank New Location window, 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 PMC may truncate the location name if the name includes more characters than the PMC can display.

---

**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 **Configuration > Locations**.

**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: . , - ' # ( ) / : \_ .

---




---

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

---

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

---

To add a location, see the [“Adding a Location” section on page 2-45](#). To delete a location, see the [“Deleting a Location” section on page 2-47](#).

## 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.



---

**Note**

You 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 **Configuration > Locations**.
  - 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 2-51](#)
- [Viewing and Editing Multicast Address Information, page 2-53](#)
- [Deleting a Multicast Address, page 2-55](#)

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 2-51.

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 2-48.

## 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 2-51 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 2-12](#) describes the items in the Multicast Pool window.

**Table 2-12** *Items in the Multicast Pool Window*

Item	Description	Reference
Address field	This field specifies the multicast address and port.	See the <a href="#">“Guidelines for Using IP Multicast Addresses with Cisco IPICS”</a> section on page 2-51

Table 2-12 Items in the Multicast Pool Window (continued)

Item	Description	Reference
Location field	<p>This field specifies the location that is assigned to this multicast address.</p> <p>The location name can include alphanumeric characters, spaces, and any of these characters: . , - ' # ( ) / : _ .</p>	See the “ <a href="#">Viewing and Editing Multicast Address Information</a> ” section on page 2-53 and the “ <a href="#">Deleting a Multicast Address</a> ” section on page 2-55
Status field	<p>Either of the following designations can display in this field:</p> <ul style="list-style-type: none"> <li>• Active—Address is assigned to an active VTG</li> <li>• Idle—Address is not assigned to an active VTG</li> </ul>	See the “ <a href="#">Managing Locations</a> ” section on page 2-38 for more detailed information about locations.
Connection Type field	<p>Either of the following designations can display in this field:</p> <ul style="list-style-type: none"> <li>• Used by Channel—Multicast address is assigned to a PTT channel.</li> <li>• 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.</li> </ul>	
Used By field	This field specifies the name of the active channel or VTG that is using the multicast address, if applicable.	
<b>Add</b> button	Click this button to add a multicast address.	See the “ <a href="#">Adding Multicast Addresses</a> ” section on page 2-51
<b>Delete</b> button	Click this button to delete a multicast address.	See the “ <a href="#">Deleting a Multicast Address</a> ” section on page 2-55

## 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, refer to 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, refer to the following URL:

[http://www.cisco.com/en/US/tech/tk828/tsd\\_technology\\_support\\_protocol\\_home.html](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 will no longer be available for use by active VTGs.

Before you add a multicast address, configure locations, as described in the “Managing Locations” section on page 2-38.

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

### Procedure

---

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

**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 2-51.

---

- 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 2-55.

---

- 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 **Configuration > Multicast Pool**.
- 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 2-13](#).

**Table 2-13** Multicast Address Details Area Fields

Field	Description
Address	<p>This field represents the multicast address.</p> <p>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.</p>  <p><b>Note</b> 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 <a href="#">“Guidelines for Using IP Multicast Addresses with Cisco IPICS”</a> section on page 2-51.</p>
Port	<p>This field represents the port number assigned to the multicast address.</p> <p>This value must be an even number in the range of 21000 through 65534.</p>  <p><b>Note</b> Cisco IPICS does not allow the configuration of any port below 21000 or any odd ports.</p>
Connection Type— <i>Display only</i>	<p>This field can include either of the following designations:</p> <ul style="list-style-type: none"> <li>• Used by Channel—Address is assigned to a PTT channel.</li> <li>• 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.</li> </ul>
Status— <i>Display only</i>	<p>This field can include either of the following states:</p> <ul style="list-style-type: none"> <li>• Active—Address is assigned to an active VTG</li> <li>• Idle—Address is not assigned to an active VTG</li> </ul>

**Table 2-13** Multicast Address Details Area Fields (continued)

Field	Description
Location— <i>Display only</i>	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 <a href="#">“Managing Locations” section on page 2-38</a> for more detailed information about locations.
Used By— <i>Display only</i>	Name of the active channel or VTG that is using the multicast address, if applicable
Last Released— <i>Display only</i>	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 **Configuration > Multicast Pool**.
- 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 PMC 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 2-59](#)
- [Adding an RMS, page 2-64](#)
- [Viewing and Configuring Loopbacks, page 2-66](#)
- [Deleting an RMS, page 2-69](#)
- [Managing the RMS Configuration, page 2-70](#)

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 2-57](#).

**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 **Configuration > RMS**.

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 the [Appendix A, “Configuring the Cisco IPICS RMS Component.”](#)

[Table 2-14](#) describes the items in the RMS window.

**Table 2-14** *Items in the RMS Window*

<b>Item</b>	<b>Description</b>	<b>Reference</b>
RMS Name field	This field specifies a unique name that is assigned to the RMS.	See the <a href="#">“Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS”</a> section on page 2-59 and the <a href="#">“Adding an RMS”</a> section on page 2-64  See the <a href="#">“Managing Locations”</a> section on page 2-38 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	
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	

## 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 2-91.)



### Tip

---

Because the RMS comparator mechanism can interject delays, you can disable it by navigating to **Administration > Options** and checking the **Disable RMS Comparator** check box. You should check this check box if you 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 2-70. For more complete configuration and deployment details, refer to the *Solution Reference Network Design (SRND) for Cisco IPICS, Release 2.0(1)*.

---



### 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 **Configuration > RMS**.
- 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 2-20. For information about how to deactivate a VTG, [“Changing the Status of a VTG Template”](#) section on page 4-19.

- Step 4** To view or update the information in the General tab, see [Table 2-15](#).

**Table 2-15** *Fields in the General Tab of the RMS Window*

Field	Description
<b>Identification</b>	
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 <a href="#">“Managing Locations”</a> section on page 2-38 for detailed information about locations.
Description	This field specifies a description for the RMS.

Table 2-15 Fields in the General Tab of the RMS Window (continued)

Field	Description
Status— <i>Display only</i>	<p>This field can include any of the following statuses:</p> <ul style="list-style-type: none"> <li>Operational—RMS has at least one loopback configured and that is operating.</li> <li>Unconfigured—RMS has no loopbacks.</li> <li>Stopping—RMS has been deactivated but has at least one DS0 in use by Cisco IPICS. The RMS will become deactivated when Cisco IPICS no longer uses any of its voice ports.</li> </ul>
	<p> <b>Note</b> 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 <a href="#">“Changing the Status of a VTG Template”</a> section on page 4-19.</p>
	<ul style="list-style-type: none"> <li>Deactivated—RMS has been deactivated and has no DS0s in use.</li> </ul>
	<p> <b>Note</b> You can change the user name, password, multicast address, or location of the RMS only when it is in the Deactivated state.</p>
	<ul style="list-style-type: none"> <li>Unreachable—RMS cannot be reached by the Cisco IPICS server.</li> </ul>
<b>Hardware Settings</b>	
IP Address	This field specifies the IP address of the Loopback interface.
Host Name— <i>Display only</i>	This field specifies the host name of the RMS.

**Table 2-15** Fields in the General Tab of the RMS Window (continued)

Field	Description
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— <i>Display only</i>	This field specifies the model number of the RMS.
<b>Controllers</b> — <i>Display only</i>	This field displays the T1/E1 connections on the RMS. The number in parentheses is the number of ports on the corresponding controller.
<b>Loopbacks</b> —(Click the <b>Loopbacks</b> Tab to access the Loopback information)	<p>This field specifies the mappings between two controllers that are physically connected.</p> <p>To change a loopback, choose a pair of controllers from the two Loopback drop-down list boxes and click <b>Add</b>. A controller appears in gray if it is in use.</p> <p>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.</p> <p>To see detailed information about all loopbacks, click <b>Expand All</b>. To collapse an expanded view of a loopback, click the down arrow next to its name. To collapse detailed information about all loopbacks, click <b>Collapse All</b>.</p> <p>For an explanation of the detailed loopback information, see the <a href="#">“Viewing and Configuring Loopbacks” section on page 2-66</a>.</p>

- 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 2-70](#).

**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 2-91](#).

---

## 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 2-59](#).

**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 PMC 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 Template” section on page 4-19](#).

---

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 **Configuration > RMS**.

- 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 will occur in the Cisco IPICS database, but will not be 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 2-38](#)

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

### Procedure

---

- Step 1** From the Administration Console, navigate to **Configuration > RMS**.
- 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 2-15](#).

- 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 box, choose a location that is defined by the IP address that you entered for the router.

See the “[Managing Locations](#)” section on page 2-38 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 (DSOs) for each loopback as described in the “[Viewing and Configuring Loopbacks](#)” section on page 2-66.
- 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 2-70.

## 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, page 2-67](#)
- [Enabling DSOs in a Loopback, page 2-67](#)
- [Disabling DSOs in a Loopback, page 2-68](#)
- [Removing a Loopback, page 2-69](#)

## 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 2-57](#).

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 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 **Configuration > RMS**.
- 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 clear 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 **Configuration > RMS**.
- 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 clear 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; and 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 **Configuration > RMS**.
- 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 2-59 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 2-64 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 **Configuration > RMS**.
- 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 box, take any of the following actions:
- To merge the RMS configuration, choose **Merge**.
  - To update the RMS configuration, choose **Update**.
  - 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 box.

---

# Managing Licenses

The Cisco IPICS license determines the number of concurrent land mobile radio (LMR) ports, multicast ports, PMC users, IP phone users, dial users, and ops views that are available for your system. The total number of LMR and multicast ports, PMC, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased.

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, refer to the *Cisco IPICS Server Installation and Upgrade Guide*.

**Note**

---

Before you can upgrade from a previous Cisco IPICS release to Cisco IPICS, release 2.0(1), you must purchase a Cisco IPICS, release 2.0(1) license.

---

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 2-78](#).

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 2-72](#).

## 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 2-78](#) for information about uploading licenses.

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

In this window, 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. See [Table 2-16](#) for a description of the licenses that can display in this tab.

The **Usage Per Ops View** tab provides license information per ops view. This tab displays types of licenses, the ops view, and current license usage information. See [Table 2-17](#) for a description of the licenses, per ops view, that can display in this tab and the criteria that Cisco IPICS uses to determine license consumption for ports, PMC, IP phone, policy engine, and ops view usage.

**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, then the update does not succeed and Cisco IPICS displays an error. If you receive an error, refresh your browser window and retry the operation.

**Table 2-16** Summary Tab Fields in the License Management Window

Field	Description
<b>Feature Name</b>	
Concurrent LMR Ports	<p>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.</p> <p>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, then the single channel uses two licenses. If one of the multicast addresses is removed, then the system releases one of the licenses so that the port will then only use one license.</p>

**Table 2-16 Summary Tab Fields in the License Management Window**

Field	Description
Concurrent Multicast Ports	<p>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.</p> <hr/>  <p><b>Note</b> Be aware that an inactive VTG (VTG template) uses a license when a policy triggers (activates) that VTG; therefore, if the number of licenses has been exceeded, the policy will not be able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.</p>
Concurrent PMC Users	<p>A PMC user uses a license each time that the user logs in to a PMC session.</p> <p>If the same PMC user logs in to multiple PMC sessions from different PMC client machines, that user uses multiple licenses (one for each PMC session).</p> <hr/>  <p><b>Note</b> If you use all of the available PMC licenses, Cisco IPICS interrupts PMC user access to the system. Make sure that you are aware of the current status of PMC licenses, and that you purchase and install additional licenses immediately if you use all of the available PMC licenses.</p>
Concurrent IP Phone Users	<p>An IP phone user uses a license each time that a user logs in to Cisco IPICS from the phone. If you use all of the IP phone licenses, then no more IP phone users can dial in.</p>

**Table 2-16** Summary Tab Fields in the License Management Window

Field	Description
Concurrent Dial Users	<p>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.</p> <p> <b>Note</b> 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 will be 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 will not be able to access the policy engine windows.</p>
Cisco IPICS Ops View	<p>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.</p> <p> <b>Note</b> To create additional ops views, you must purchase and install a Cisco IPICS license that includes additional ops view ports.</p>
Cisco IPICS Base Server License	<p>License usage does not apply to this field. This field displays whether you have a base license for Cisco IPICS.</p>

**Table 2-16 Summary Tab Fields in the License Management Window**

Field	Description
Policy Engine Base License	<p>License usage does not apply to this field. This field displays whether Cisco IPICS policy engine is enabled.</p> <p>When the policy engine is enabled, the Summary tab displays <b>Licensed</b>.</p> <p>When the policy engine is not enabled, the Summary tab displays <b>Not Licensed</b>.</p>

**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 6, “Configuring and Managing Cisco IPICS Operational Views”](#) for more information about ops views.

The **Usage Per Ops View** tab provides license information per ops view. This tab displays the types of licenses, the ops view, current license usage, and the allocated ports. See [Table 2-17](#) for a description of the information in this tab.

**Table 2-17 Usage Per Ops View Tab in the License Management Window**

Field	Description
<b>License Type</b>	
PMC Ports	<p>Ops View—Ops view to which this license belongs</p> <p>Current Usage—Number of PMC ports that are in use for this ops view</p> <p>Allocated Ports—Number of PMC ports that have been allocated to this ops view</p>

**Table 2-17 Usage Per Ops View Tab in the License Management Window**

Field	Description
LMR Ports	<p>Ops View—Ops view to which this license belongs</p> <p>Current Usage—Number of LMR ports that are in use for this ops view</p> <p>Allocated Ports—Number of LMR ports that have been allocated to this ops view</p>
IP phone Ports	<p>Ops View—Ops view to which this license belongs</p> <p>Current Usage—Number of IP phone ports in use for this ops view</p> <p>Allocated Ports—Number of IP phone ports that have been allocated to this ops view</p>
Multicast Ports	<p>Ops view—Ops view to which this license belongs</p> <p>Current Usage—Number of multicast ports that are in use for this ops view</p> <p>Allocated Ports—Number of multicast ports that have been allocated to this ops view</p>
Dial Ports	<p>Ops View—Ops view to which this license belongs</p> <p>Current Usage—Number of dial ports that are in use for this ops view</p> <p>Allocated Ports—Number of dial ports that have been allocated to this ops view</p>

## Understanding Time-bound License Behavior

Time-bound, or evaluation, licenses differ from permanent licenses by the inclusion of a predefined expiration date. For more detailed information and guidelines about time-bound licenses, refer to the [Cisco IPICS Server Installation and Upgrade Guide](#).

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 will be 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/5.5.9/webapps/license/
```

To upload a license file, perform the following procedure:

**Procedure**

- Step 1** From the Administration Console, navigate to **Administration > License Management**.
- 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, refer to the [Cisco IPICS Server Installation and Upgrade Guide](#).

## Viewing Active Users

As a Cisco IPICS system administrator, you can view the activity for users who are logged in to the system via PMC and IP phone, 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 access the Active Users window, navigate to Administration > Active Users.

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

### Procedure

---

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

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

- **Logged-in Users**—Users who are logged in to Cisco IPICS
- **PMC Users**—Users who are connected to Cisco IPICS via the PMC
- **IP Phone Users**—Users who are connected to Cisco IPICS via an 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 2-18](#) for a description of the fields in the Active Users window.



**Note** 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 box 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 2-18 Active Users Window Fields**

Field	Description
<b>Logged-in Users</b>	
User	Name or user ID of user who is logged in to the Cisco IPICS system
Date	Date that the user logged in to the Cisco IPICS system
<b>PMC Users</b>	
User	Name or user ID of the active PMC user
PMC ID	Identification of the PMC for the session
Version	PMC version information that the user is using
Address	IP address of the PMC client machine
Location	Location of the user
Belongs To	Ops view to which the active PMC user belongs
Last Activity	Date and time of the last PMC activity of the PMC user

**Table 2-18 Active Users Window Fields (continued)**

<b>Field</b>	<b>Description</b>
Status	<p>Indicates the status of a PMC</p> <p>The Status column can contain a status of either Logged-in or Logging-out.</p> <p>The Logging-out status means that the PMC has not yet contacted the server to finalize the PMC session. All resources, including licenses and RMS resources, are deallocated immediately when a user is disabled, or when a PMC session is logged out by using the <b>Logout</b> button in the PMC tab in the Active Users window. The PMC session is retained until the server can provide detailed information to the PMC about the conditions of the logout.</p> <p>The server removes logging-out sessions in the following conditions:</p> <ul style="list-style-type: none"> <li>• The PMC contacts the server.</li> <li>• The server periodically checks (every 60 seconds by default) for sessions which have been active for 10 minutes and removes them in the event of a PMC crash or if the PMC is in offline mode.</li> <li>• At the startup of the Cisco IPICS server.</li> </ul>
<b>IP Phone Users</b>	
User	Name or user ID of the active IP phone user
Digit ID	Digit identification number of the active IP phone user
Location	Location of the active IP phone user
Active	Indicates whether the IP phone user is currently active
Remote	Indicates whether the IP phone user is dialed in using a remote connection
<b>Dialed-in Users</b>	

**Table 2-18 Active Users Window Fields (continued)**

Field	Description
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: <ul style="list-style-type: none"> <li>• Channel</li> <li>• VTG</li> </ul>
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: <ul style="list-style-type: none"> <li>• Not Joined—The user is dialed in but has not joined a channel or VTG</li> <li>• Listening—The user is dialed in and has joined a channel or VTG and is listening to that channel or VTG</li> <li>• 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</li> </ul>

**Step 3** To manually disconnect a logged-in, PMC, 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 a PMC user, click the **PMC** tab.
  - Check the check box to the left of each PMC user that you want to log out and click **Logout**.

When you log out a PMC user, the session is ended and the action cleans up all the PMC resources and marks the session accordingly. If the PMC is not running, the cleanup action completes.

If the PMC is running and connected to the server, the PMC gets the logout update from the server and logs out accordingly, redisplaying the Login dialog.

If the PMC is running in offline mode, the PMC continues to run. If the PMC uses multicast communications, there are no effects on the channel. If the PMC uses SIP-based communications, the SIP channels become disconnected.

- 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 then click **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.

In Cisco IPICS, an activity gets logged once and the log entry remains indefinitely. When entities such as users, locations, channels, and VTGs, get deleted from Cisco IPICS, the corresponding log entries do not get deleted from the activity log table to provide a historical record if needed.

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 2-84 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 2-89.

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 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, 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, 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, then 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 2-91](#). For information about downloading archived activity logs, see the [“Downloading Archived Activity Logs” section on page 2-88](#).

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

## 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, 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 **Administration > Activity Log Management**.
- Step 2** From the drop-down list box 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 box, 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 box, 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 and/or download.
- Step 7** In the To field, specify the ending date and time of the activity logs that you want to view and/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 box 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 examples were performed by using Microsoft Office Excel 2003.

---

- Open the Microsoft Excel application and from the File drop-down menu click **Open**.
  - Navigate to the .xml file, highlight the file and click **Open**.
  - In the Open XML dialog box, click the **As an XML List** 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, select the file and right-click it.
  - Choose **Open With** and then **Choose Program**.
  - Choose **Microsoft Excel** in the Open With dialog box.



---

**Note** 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 2-88](#).

---

## 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. For more information about the Options window, see the [“Managing Cisco IPICS Options”](#) section on page 2-91.

To download archived activity logs, perform the following procedure:

### Procedure

- Step 1** From the Administration Console, navigate to **Administration > Activity Log Management**.
- Step 2** Click the **Archives** tab.
- [Table 2-19](#) shows the fields in the Archive Status pane.

**Table 2-19** *Archive Window Fields*

Field	Description
Archive Time— <i>Display only</i>	Time when the activity log files were archived in Cisco IPICS
Archive Status— <i>Display only</i>	Indicates whether log files were archived successfully
Archive Count— <i>Display only</i>	Number of log entries that were archived during the last archive
Archived Files drop-down list box	The file names of the archived files
<b>Download</b> button	Click this button to download archived Cisco IPICS activity logs

- Step 3** From the Archived Files drop-down list box, 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 box 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 2-20](#) describes the types of activities that can be logged in by ops views.

**Table 2-20** 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.

**Table 2-20 Activity Log Types By Ops View (continued)**

<b>Activity Type</b>	<b>Description</b>
Licensable Feature Activities	Logs are created whenever feature activities occur, for features that have been licensed in Cisco IPICS.
PMC Activities	Logs are created whenever PMC activities occur 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 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 **Administration > Activity Log Options**.
- Step 2** From the Ops View drop-down list box, 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 and then click > or <. Or, double-click the activity type.
  - To move several activity types from one list to the other at one time, Shift+click or Ctrl+click to select the activity types and 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 RMS and activity log options.
- **Passwords** tab—Choose this tab to set the password options for users.
- **PMC** tab—Choose this tab to set PMC configuration options.

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 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 PMC 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**.

[Table 2-21](#), [Table 2-22](#), and [Table 2-23](#) describe the fields in the Options window.

**Table 2-21** General Tab in the Options Window

Setting	Description	Default Setting
Disable RMS Comparator (in the RMS pane)	<p>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.</p> <p>Because the RMS comparator can interject delays, you can disable it by checking this check box.</p>  <p><b>Note</b> If you connect via a high latency, low bandwidth connection, such as a satellite link, you should check this check box.</p>	<p>This check box is unchecked by default.</p> <p>If the Disable RMS Comparator check box is selected, the RMS Polling Frequency field displays as dimmed.</p>
RMS Polling Frequency	<p>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.</p> <p>This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.</p> <p>Valid values: 1-32767</p>	<p>The default interval between checks specifies 10 minutes.</p>

**Table 2-21**      **General Tab in the Options Window (continued)**

Setting	Description	Default Setting
Maximum Activity Logs (in the Activity Logs pane)	<p>This setting the maximum amount of database space that may be used by Cisco IPICS activity logs. For more information, see <a href="#">Chapter 10, “Understanding Cisco IPICS Serviceability and Diagnostic Information.”</a></p> <p>This setting specifies a value in megabytes (MB). To change the default, double-click the current value and enter a new value.</p> <p>Valid values: 1-250</p>	The default maximum space for activity logs specifies 50 MB.
Activity Log Retention Period	<p>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.</p> <p>Valid values: 1-365</p>	The default setting specifies 90 days.

**Table 2-22 Passwords Tab in the Options Window**

Setting	Description	Default Setting
Minimum Password Length (in the User Passwords pane)	<p>This setting specifies the minimum number of characters that a user can enter when creating or changing the Cisco IPICS password in the <b>Home &gt; My Profile</b> window. See the <a href="#">“Managing Your User Profile”</a> section on page 5-2.</p> <p>Use the drop-down list box to choose a new setting. The minimum length can range from 4 to 80 characters.</p> <p>To ensure a strong password, you must create a password that is at least eight characters long, and includes the following elements:</p> <ul style="list-style-type: none"> <li>• At least one lower case letter</li> <li>• At least one upper case letter</li> <li>• At least one number</li> <li>• At least one of the following special characters:</li> </ul> <p style="text-align: center;">@ [ ] ^ _ ` ! " # \$ % &amp; ' ( ) * + , - . / : ; { &lt;   = } &gt; ~ ?</p> <p>Valid values: 4-20</p>	The default setting specifies 8 characters.
Minimum Digit Password Length	<p>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.</p> <p>Use the drop-down list to choose a new setting. The minimum length can range from 4 to 10 characters.</p> <p>Valid values: 4-10</p>	The default setting specifies 4 characters.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Lower Case Letter Count	<p>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.</p> <p>The range of this field is from 0 to whatever number is specified in the Minimum Password Length field.</p>  <p><b>Note</b> The total number in this field cannot exceed the number that is set in the Minimum Password Length field.</p> <hr/> <p>Valid values: 0-76</p>	The default setting specifies 1 character.
Minimum Upper Case Letter Count	<p>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.</p> <p>The range of this field is from 0 to whatever number is specified in the Minimum Password Length field.</p>  <p><b>Note</b> The total number in this field cannot exceed the number that is specified in the Minimum Password Length field.</p> <hr/> <p>Valid values: 0-76</p>	The default setting specifies 1 character.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Numeric Character Count	<p>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.</p> <p>The range of this field is from 0 to whatever number is specified in the Minimum Password Length field.</p>  <p><b>Note</b> The total number in this field cannot exceed the number that is specified in the Minimum Digit Password Length field.</p> <hr/> <p>Valid values: 0-76</p>	The default setting specifies 1 character.
Minimum Special Character Count	<p>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.</p> <p>The range of this field is from 0 to whatever number is specified in the Minimum Password Length field.</p> <p>Valid values: 0-76</p>	The default setting specifies 1 character.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password History Count	<p>This setting specifies the number of passwords that Cisco IPICS will mark as previously used, and that the user will not be able to use again.</p> <p>For example, if the Password History Count is set to 5, then the user will not be able to use any of the passwords that they have used for the previous five times.</p>  <p><b>Note</b> This field does not apply to the ipics or ipicsadmin user IDs.</p> <hr/> <p>Valid values: 0-999</p>	The default setting specifies 5 previous passwords.
Apply User Password Expiration (in Password Expiration pane)	<p>This check box specifies whether Cisco IPICS applies the value that is specified in the Password Expiration field.</p> <p>If this check box is unchecked, then there will be no user password or digit expiration applied.</p> <p>Valid values: true or false</p>	<p>This check box is unchecked by default.</p> <p>If this check box is not selected, the Password Expiration and Password Expiration Notification fields display as dimmed.</p>

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration	<p>This setting specifies the number of days in which the Cisco IPICS login password and the digit password will expire. For example, if the value is 180 days, then the password will expire after 180 days from the date that the password was created.</p> <p> <b>Note</b> If the value is specified as 0, the password never expires and the message Never Expired displays in the Password Expiration Date field, in the My Profile window for the user.</p> <p> <b>Tip</b> After a Cisco IPICS migration occurs, you may want to require all users to update their login passwords for enhanced password security.</p> <p>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 will force users who log in to Cisco IPICS during that day (after the migration) to change their login passwords.</p> <p>Valid values: 1-999</p>	The default setting specifies 180 days.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration Notification	<p>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.</p> <p> <b>Note</b> This field does not apply to the ipics or ipicsadmin user IDs.</p> <p> <b>Tip</b> If the number in this field is specified as 0, the current password expires on the actual password expiration date, and the user will be forced to create a new password at the next Cisco IPICS login.</p> <p>Valid values: 0-999</p>	The default setting specifies 3 days.

**Table 2-22** Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Apply User Account Lockout (in the User Account Lockout pane)	<p>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.</p> <p>For information about how to unlock an account that has been locked, see <a href="#">Chapter 3, “Performing Cisco IPICS Operator Tasks.”</a></p>  <p><b>Note</b> This field does not apply to the ipics or ipicsadmin user IDs.</p> <hr/> <p>If this check box is unchecked, there will be no account lockout applied.</p> <p>Valid values: true or false</p>	<p>This check box is unchecked by default.</p> <p>If this check box is not selected, the Maximum Invalid Login Attempts Allowed and the Failed Password Attempt Expiration fields display as dimmed.</p>

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Invalid Login Attempts Allowed	<p>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.</p> <p>Valid values: 1-999</p>  <p><b>Note</b> 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 will be locked. When the user account is unlocked, both invalid attempt counts will be reset to 0.</p> <hr/> <p>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.</p> <p>To unlock a user account, see <a href="#">Chapter 3, “Performing Cisco IPICS Operator Tasks.”</a></p> <p>You can also re-enable a user account by using the enableuser tool. The enableuser tool clears the value that is specified in the Maximum Invalid Login Attempts Allowed field and unlocks the user account. To re-enable a user ID using the enableuser tool, refer to the <a href="#">Cisco IPICS Troubleshooting Guide, Release 2.0(1)</a>.</p>	The default setting specifies 5 attempts.

**Table 2-22 Passwords Tab in the Options Window (continued)**

Setting	Description	Default Setting
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: 1-999	The default setting specifies 8 hours.

**Table 2-23 PMC Tab in the Options Window**

Setting	Description	Default Setting
PMC Update Poll (in the Configuration pane)	This setting specifies the frequency that the PMC uses to poll the server for updates. For more information, refer to the <i>Cisco IPICS PMC Installation and User Guide</i> .  This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.  Valid values: 3-3600	The default polling interval specifies 5 seconds.
Disable PMC Activity Log Upload (in the PMC Activity Logs pane)	When you check this check box, the PMC does not upload logs to the server.   <b>Note</b> 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 PMC Log Upload Frequency field and the PMC Send Logs on Rollover fields/check box display as dimmed.

Table 2-23 *PMC Tab in the Options Window (continued)*

Setting	Description	Default Setting
PMC Log Upload Frequency (PMC to server)	<p>When a PMC client has activity logs ready to upload to the Cisco IPICS server, the PMC application places the logs in a queue. At regular intervals, the PMC client checks the queue and uploads to the server any logs that are waiting to be uploaded. Log files are copied to the <b>\$TOMCAT_HOME/webapps/ipics_server/pmclogs</b> directory, and are based on user ID and PMC ID. Log files that are not successfully uploaded get put back in to the queue and are uploaded at a later time.</p> <p>This setting specifies the interval between these checks. For more information, refer to the <a href="#">Cisco IPICS PMC Installation and User Guide</a>.</p> <p>This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.</p> <p> <b>Note</b> Cisco IPICS archives or deletes PMC log files that have been uploaded to the server, such as debug logs, by using an archive utility. This utility runs once a day and 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.</p> <p>For detailed information about PMC log files, see <a href="#">“Managing an End Device from the PMC Tab” section on page 3-19</a>.</p> <p>Valid values: 60-32767</p>	The default upload frequency specifies 600 seconds (10 minutes).

Table 2-23 *PMC Tab in the Options Window (continued)*

Setting	Description	Default Setting
PMC Send Logs on Rollover	<p>Cisco IPICS defines the PMC UserInterface.log, Authentication.log, and ChannelStatistics.log log files based on a maximum size of 1MB. When any one of these log files reaches this predefined limit, the system creates a new log file.</p> <p>When you enable this option, the Cisco IPICS server retrieves the log files from the PMC based on file size rollover and renames the uploaded log file to reflect an archive copy. If you do not enable this option, the PMC deletes the log files when they reach their maximum size limit.</p> <p>Be aware of the following caveats:</p> <ul style="list-style-type: none"> <li>• The DebugLog.txt file does not have a size limit of 1MB, and is only uploaded to the server on request or when the PMC is started if this check box is checked (set to true). If this check box is unchecked, the DebugLog.txt file is not uploaded.</li> <li>• The ChannelActivity.log file is uploaded to the server every 10 minutes (or the interval that you configure in the PMC Log Upload Frequency field).</li> </ul> <p>Valid values: true or false</p>	<p>The PMC uploads files on rollover (the check box is checked).</p>

Table 2-23 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Activity Log Update	<p>The Cisco IPICS server gathers activity logs from the PMC client machines and updates the database with this information at regular intervals. In the Cisco IPICS database, this data is parsed, organized, and made available for queries from the Activity Log window of the Administration Console.</p> <p>This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value.</p> <p>Valid values: 30-32767</p>	The default update frequency specifies 600 seconds (10 minutes).

## Managing PMC Versions

The Cisco IPICS server maintains a repository of one or more versions of the PMC. PMC updates can be assembled into upgrade packages that you can upload to the Cisco IPICS server.

These updates of the PMC application add features and resolve issues. Users can upgrade their PMC clients at their convenience by downloading the current version of the PMC utility, as described in the [“Downloading the PMC” section on page 5-19](#).



### Note

You must perform the PMC configuration procedures that are in this section before users can download and install a PMC on their PC clients.

When you initially install Cisco IPICS, a PMC package is included with the server. You must configure the PMC download configuration and generate the PMC Installer in order for that version to be available for download to PMC users.

When a new version of the PMC becomes available, you upload the new PMC package to the Cisco IPICS server making it available for the PMC users to download to their PMC clients. PMC packages are contained in .zip files and can include alert tones and skins.

Each PMC client polls the Cisco IPICS server regularly. As part of this process, the PMC client determines whether there is a new version of a PMC upgrade package to which it can or must update. You configure the recommended PMC versions to designate the PMC version that is available for this update, and to designate whether an update is required or recommended. For more information about configuring the PMC versions, see the [“Changing the State of PMC Versions” section on page 2-110](#).

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

- [Uploading PMC Versions to the Cisco IPICS Server, page 2-109](#)
- [Changing the State of PMC Versions, page 2-110](#)
- [Deleting PMC Versions, page 2-112](#)

You perform the PMC version update tasks in the PMC Versions window. For more information about this window, including how to access it, see the [“Understanding the PMC Versions Window” section on page 2-107](#).

## Understanding the PMC Versions Window

The PMC Versions window allows you to specify information about PMC versions to use for automatic updates. It also enables you to upload to the Cisco IPICS server the new PMC versions that are used for these updates.

The PMC Versions window lists information about each of the PMC versions that have been uploaded to the Cisco IPICS server.

To display the PMC Versions window, navigate to **PMC Management > PMC Versions**.

[Table 2-24](#) describes the items in the PMC Versions window.

Table 2-24 Item in the PMC Versions Window

Item	Description	Reference
Upgrade Package field	This field contains the PMC version to be uploaded to the Cisco IPICS server.	See the <a href="#">“Uploading PMC Versions to the Cisco IPICS Server”</a> section on page 2-109
<b>Browse</b> button	Click this button to browse to the location that contains the PMC version upgrade package that you can upload to the Cisco IPICS server.	
<b>Upload</b> button	Click this button to upload a new PMC version to the Cisco IPICS server.	
Name field	This field allows you to assign a unique identification to the PMC version upgrade package.	
Version field	This field specifies a unique version number that is assigned to the PMC version upgrade package.	
State field	This field specifies the priority (state) that is assigned to the upgrade package.	See the <a href="#">“Changing the State of PMC Versions”</a> section on page 2-110
<b>Delete</b> button	Click this button to delete a PMC version from the Cisco IPICS server.	See the <a href="#">“Deleting PMC Versions”</a> section on page 2-112

**Table 2-24** *Item in the PMC Versions Window (continued)*

Item	Description	Reference
Drop-down list box for PMC version states	Choose from this list box to configure the state for the PMC versions.	See the <a href="#">“Changing the State of PMC Versions”</a> section on page 2-110
<b>Change State</b> button	Click this button to change the state of the PMC version.	

## Uploading PMC Versions to the Cisco IPICS Server

When you upload a new PMC version, the upgrade package file is copied from the stored location on your PC to the Cisco IPICS server.

To upload a PMC upgrade version to the Cisco IPICS server, perform the following procedure:

### Procedure

- 
- Step 1** From the Administration Console, navigate to **PMC Management > PMC Versions**.
  - Step 2** To locate the PMC version upgrade package, that you obtained from Cisco, click **Browse**.
  - Step 3** In the Choose File window, browse to the PMC 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 PMC version displays in the PMC Versions list.



**Note** All new PMC versions are saved, by default, in a non-operational state. This means that the PMC users cannot download the version until you change the state. See the [“Changing the State of PMC Versions” section on page 2-110](#) for more information.

## Changing the State of PMC Versions

The PMC Versions window enables you to designate the PMC versions that are used for an automatic update by changing the state of the versions. When you specify a PMC version for the automatic update, be aware of this information:

- If you want to force PMC clients to update as soon as possible, choose **Recommended** from the drop-down list box. When you choose this state, the next time that a PMC client polls the server, it compares the PMC version that it is running with the recommended PMC version. If the PMC client does not match the recommended or operational versions, then it automatically downloads the PMC version that is specified in the drop-down list box, automatically updates to that version, and then automatically restarts.
- To force updates immediately, choose **Not Supported** from the drop-down list box. When you choose this state, PMC users who are running this version are forced to restart and download a newer version.



### Caution

Forcing a PMC automatic update shuts down and then restarts a PMC without warning a user, regardless of the purpose for which the PMC is being used. For this reason, it is recommended that you force an update only when it is absolutely necessary.

- You must upload a PMC version to the Cisco IPICS server before it becomes available in any of the fields in the PMC Versions window.

For more detailed information about the PMC, refer to the [Cisco IPICS PMC Installation and User Guide](#).

To change the state of PMC versions for automatic updates, perform the following procedure:

## Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > PMC Versions**.
- Step 2** Check the check box next to the PMC version that you want to change.
- Step 3** From the drop-down list box, choose any of the following states:
- **Recommended**—This version represents the recommended software version that should be run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform the PMC user. The server then sends this version to the PMC and the PMC installs it after the PMC user responds positively to the message prompt or if other installed versions are not supported.
  - **Staged**—This version represents the software version that the PMC downloads according to the discretion of the administrator. The server sends this version to the PMC for download but the PMC does not install it until the administrator changes the state of this version to recommended or operational. At that time, the PMC may install the new version after the PMC user responds positively to the message prompt or if other installed versions are not installed.  
  
By using the Staged version, the PMC can download the version without installing it. The PMC may download this version but does not install it until the server configuration has been updated to reflect this version as recommended or operational.
  - **Operational**—This version represents a version of PMC software that is operational. This version is supported for use with the server but there may be a later version that is also supported.



---

**Note** The server always extends priority to the PMC versions that it marks as recommended.

---

- **Not Supported**—This version represents an unsupported PMC software version. The server does not send this version to the PMC so that the PMC users cannot choose an unsupported version from the drop-down list box in the location dialog box.



---

**Note** The server forces an upgrade on any PMC that has installed an unsupported version of software.

---

**Step 4** Click the **Change State** button.

---

## Deleting PMC Versions

To delete PMC versions, perform the following procedure:

### Procedure

---

**Step 1** From the Administration Console, navigate to **PMC Management > PMC Versions**.

**Step 2** Check the check box of the PMC 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 PMC version.

This version of the PMC is completely removed from the server.

If you do not want to delete the PMC version, click **Cancel**.

---

## Managing PMC Alert Tones

PMC 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 server. The alert tone set is packaged in a .zip file that you can upload to the server, and that PMC users can then download on to their client machines.

An alert tone set is associated with an ops view; therefore, each PMC user can see only one tone set based on the ops view association. For more information about ops views, see [Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”](#)

**Note**

---

The PMC alert tone feature requires the use of compatible alerting tone files. These files must be .wav files that are encoded in Pulse Code modulation (PCM), which is a sampling technique that digitizes analog signals. These .wav files must be encoded in PCM format with 8 bits monaural samples at 8000 Hz sampling rate, for a total of 64 kbps. While higher and lower bit rates may seem to work, Cisco IPICS does not support the use of any other encoding or bit rates, as they may produce inferior sound quality. (Any file that is used with the G.729 codec may sound inferior due to its encoding algorithms; for more information, refer to the [Cisco IPICS PMC Installation and User Guide](#).) In addition, all alerting tones should be encoded to a nominal value of -20 decibels relative to one milliwatt (dBm) and begin and end with zero deflection to eliminate or minimize “popping” or “clicking” sounds.

---

As a Cisco IPICS system administrator, you can perform the following alert tone management functions:

- [Creating a PMC Alert Tone Set, page 2-113](#)
- [Adding PMC Alert Tone Sets, page 2-115](#)
- [Viewing or Editing PMC Alert Tone Sets, page 2-117](#)
- [Associating an Alert Tone Set to an Ops View, page 2-117](#)
- [Deleting PMC Alert Tones, page 2-118](#)

## Creating a PMC Alert Tone Set

To provide the alert tones that get downloaded to the PMC, you must first create a PMC 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 PMC is installed, navigate to the following directory:
- [C:\Program Files\Cisco Systems\Cisco IPICS\PMC\Components]**
- Step 2** Create a new empty directory and extract the sample alert tone set zip file, and all its contents, in to the new directory.
- Step 3** Add any desired sound files in .wav format to this directory.



**Note** These files should be normalized to -2 db and should be encoded by using 8 bit PCM at 8000 Hz.

- 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 PMC.

- 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*” is the .wav file to be played, and “*displayName*” is the text that displays on the PMC.



**Note** The PMC displays a maximum of 8 characters for the display name.

- Step 6** Save the example tone set .xml file and rename the .xml file to an appropriate file name.



---

**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 from the directory that you do not want.

- Step 8** Using file explorer, navigate to the directory that contains the .xml and .wav files and select all of the .wav files and the .xml file.



---

**Tip** You can select all of the files by clicking **Ctrl+A**.

---

- 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 the PMC user to press a button on the PMC 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 PMC alert tone set to the Cisco IPICS server. See the [“Associating an Alert Tone Set to an Ops View” section on page 2-117](#) 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 PMC Alert Tone Sets

To add a new PMC alert tone set, perform the following procedure:

## Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > Alert Tones**.
- Step 2** Click **Add**.
- A blank alert tone detail window displays.
- Step 3** To locate and upload the alert tone set that you want to add, click **Browse**.



### Tip

The Stop alert tone should be uploaded to the Cisco IPICS server. This alert tone will allow 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 a PMC Alert Tone Set”](#) section on page 2-113 for information about how to create an alert tone set.

---

- Step 4** In the Set Name field, enter a name for the alert tone set.
- Step 5** In the Description field, enter a description for the alert tone set.
- Step 6** Click the **Browse** button to upload the alert tone set.
- Step 7** Click **Save**.
- The tone set gets uploaded to the server and is available for use by PMC 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 8** 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 2-117.
-

## Viewing or Editing PMC Alert Tone Sets

To view or edit the PMC alert tone sets that are available for use in Cisco IPICS, perform the following procedure:

### Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > Alert Tones**.
- 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 2-117](#).
- 

## 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 PMC 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 **PMC Management > Alert Tones**.
- 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 and then click > or <. Or, double-click the ops view.
  - To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click > or <.
  - To move all ops views from one list to the other at one time, click >> or <<.
- Step 5** Click **Save** to save the ops view that you want to associate to the alert tone set in the Associated Ops Views list.
- PMC users can now only be able to see the alert tone set that is in the ops view to which they belong.
- If you do not want to save you changes, click **Cancel**.
- 

## Deleting PMC Alert Tones

To delete PMC tones, perform the following procedure:

### Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > Alert Tones**.
- 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 PMC 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 PMC Skins

Cisco IPICS supports several different skins that PMC users can use on their PMC. Skins are files, that you create and manage, that are packaged in sets (zip files) that can be downloaded to a PMC, and that form the appearance of the PMC. Once the skin sets are downloaded, PMC users can unpack them and choose from the individual skins, that were contained in the package, to use on their PMCs.

Skins are customizable in Cisco IPICS and are available in various options, including 4, 6, and 18-channel mouse skins and 4 and 8 channel touch screen skins. You control whether PMC users can download only selected PMC skins, or customizable skins.

Cisco IPICS supports only 18 channels to be viewed at a time, and several different skins from which PMC users can choose for the PMC. For more information about using the PMC, refer to the [Cisco IPICS PMC Installation and User Guide](#).

Cisco IPICS enables you to upload and manage skin sets that are available to the PMC users. The information about the skin sets, contained in the Skins window, includes the name of the skin set, files size, and the MD5 summary of each skin set. You can use the MD5 summary field to determine whether skin sets get properly uploaded to the server.



---

**Note** The MD5 value should never be empty after the skin set has been uploaded to the server. It will only display as blank prior to adding the skin set because the server must process the file before producing the MD5 value.

---

You can access all skin sets that are currently available on the server by navigating to the PMC Management drawer in the Cisco IPICS Administration Console and clicking the **Skins** link.

You can view and edit existing skin sets, as well as add and delete skin sets, as described in the following procedures:

- [Adding PMC Skins, page 2-120](#)
- [Viewing or Editing PMC Skins, page 2-120](#)
- [Deleting PMC Skins, page 2-121](#)

## Adding PMC Skins

To add a new PMC skin set, perform the following procedure:

### Procedure

---

**Step 1** From the Administration Console, navigate to **PMC Management > Skins**.

**Step 2** Click **Add**.

A blank New Skin detail window displays.

**Step 3** To locate and upload the skin set that you want to add, click **Browse**.

**Step 4** In the Skin Name field, enter a name for the skin set.

**Step 5** In the Description field, enter a description for the skin set.

**Step 6** Click the **Browse** button to upload the skin set.

**Step 7** Click **Save**.

The skin set gets uploaded to the server and is available for download by PMC users.

The skin name, file size, and MD5 summary information of the new skin set also displays.

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

---

## Viewing or Editing PMC Skins

To view or edit the PMC skins that are available for use in Cisco IPICS, perform the following procedure.



---

**Note** To add a new skin set, see the [“Adding PMC Skins” section on page 2-120](#).

---

### Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > Skins**.
- Step 2** In the Skin Name column, click the link for the skin set that you want to view or edit.
- A skin detail window displays current information about the skin set that you chose.
- Step 3** To download the skin set without making any changes, click the skin name link.
- Step 4** To edit the information for the skin set, take any of the following actions:
- In the Skin Name field, enter a new name for the skin.
  - In the Description field, enter a new description for the skin.
  - Click the **Browse** button to upload and overwrite the existing skin.
- Step 5** Click **Save**.
- If you do not want to save your changes, click **Cancel**.
- 

## Deleting PMC Skins

To delete PMC skins, perform the following procedure:

### Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > Skins**.
- Step 2** Check the check box to the left of the Skin Name of the skin set that you want to delete.
- Step 3** Click **Delete**.
- The skin set that you deleted is no longer available for use by the PMC users.



---

**Note** If you want to delete all of the existing skins, check the check box at the top of the skins list and click **Delete**.

---

## Managing the PMC Installer

Before PMC users can download new PMC versions to their clients, you must configure the PMC Installer.

The PMC Installer installs the PMC on to PMC client machines. The PMC package downloads to a PMC client when a PMC user clicks the **Download PMC** link in the Home drawer, as described in the [“Downloading the PMC”](#) section on page 5-19.

As a Cisco IPICS system administrator, you can upload a new PMC package, as well as generate the PMC Installer as described in the [“Generating the PMC Installer”](#) section on page 2-123.

You perform these tasks in the PMC Installer window. For more information about this window, including how to access it, see the [“Using the PMC Installer Window”](#) section on page 2-122.

## Using the PMC Installer Window

The PMC Installer window contains configuration information that is necessary in order to generate a PMC installer.

To display the PMC Installer window, navigate to the PMC Management drawer in the Cisco IPICS Administration Console and click the **PMC Installer** link.

The Installer Status field displays the date and time that a pmcsetup.exe file was last generated, and displays the IP address defined by the bundled pmc.ini file.

## Generating the PMC Installer

Generating a PMC Installer installs a new PMC version package, and makes it available for download from the **Download PMC** link in the Home drawer, as described in the [“Downloading the PMC” section on page 5-19](#).

To configure additional PMC options, see the [“Managing Cisco IPICS Options” section on page 2-91](#).

To configure a PMC and generate a PMC Installer, perform the following procedure from the PC on which you stored the PMC version package:

### Procedure

---

- Step 1** From the Administration Console, navigate to **PMC Management > PMC Installer**.
- Step 2** To choose the IP address that is listed for Server Address, click the radio button next to the IP address that displays.
- This address is the IP address that the PMC will use to contact the server. The IP address or hostname of the connected NIC hardware should display as a choice.
- Step 3** To configure a different IP address for the PMC, click the **Other** radio button and enter the IP address that you want the PMC to use.



---

**Note** If you choose another IP address instead of the configured IP address, that IP address should be tested in the network domain that will be supported with that server. This is in case the PMC cannot connect to the server due to NAT or firewall restrictions.

---

- Step 4** In the HTTP Port field, enter the port number that will be used for non-secure HTTP communication between the PMC and the server.
- Step 5** In the HTTPS Port field, enter the port number that will be used for secure HTTPS communication between the PMC and the server.



---

**Note** Cisco recommends that you use the default HTTP and HTTPS ports that are listed in the PMC Installer Configuration area. The IP address, HTTP port, and HTTPS port fields affect only the PMC installer and do not have an immediate effect on PMC clients that have already been installed on user PCs. If you need to change these values, then Cisco recommends that you notify all users that they need to download and reinstall the PMC using the new pmcsetup.exe that is generated after you save the changes to these values.

---

**Step 6** In the PMC Version To Be Used For The PMC Installer drop-down list box, choose the version number of the PMC that you want the users to download.

The drop-down list box should be populated with the version numbers of the pmcinst.exe files that have been uploaded to the Cisco IPICS server. See the [“Managing PMC Versions” section on page 2-106](#) for more information.



---

**Note** There is only one PMC installer and all PMC users who use that installer will automatically receive a complete application of that PMC version.

---

**Step 7** Click **Save**.

PMC users can now download a new version of the PMC application, as described in the [“Downloading the PMC” section on page 5-19](#).

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

---