Operational Views

This chapter describes the Cisco IPICS operational view functionality and it includes information about relevant terminology, caveats, and administration tasks.

This chapter includes the following sections:

Overview of Cisco IPICS Operational Views

This section provides an overview of Cisco IPICS operational views; it includes the following topics:

Introducing Cisco IPICS Ops Views

Cisco IPICS provides the ability for you to organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other. In Cisco IPICS, these separate views are known as operational views, or ops views. While these views are maintained separately by the Cisco IPICS system administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

Note The use of ops views allows segmentation of resources that authorized Cisco IPICS users may see on the Administration Console. Ops views does not affect the way in which channels and VTGs display on the PMC or Cisco IP Phone.

This section provides an overview of the Cisco IPICS ops view functionality. It includes the following topics:

Enabling Ops Views

By default, Cisco IPICS disables the ops views functionality on the server. To enable this feature, you must purchase and install a Cisco IPICS license that includes a license for the ops views functionality; then, restart the server. You install this ops view license by uploading it to the server. Navigate to the **System Administrator > License** window in the Administration Console to view the license information.

Note Although the Ops Views check box is checked in the **System Administrator > Options** window by default, the feature is not actually enabled until you upload the license and restart the server. For more information about enabling ops views, see the "Activating the Ops View Feature" section on page 6-18.

When the ops view feature has been enabled on the server, the system displays a Cisco Ops View entry under the Configured License area in the License window, along with the word "Licensed" to indicate that the ops view functionality has been enabled. (When ops views is not enabled, this entry displays "Not Licensed.") Cisco IPICS also displays the number of available licenses and current usage in this window. For more detailed information about license limits and current usage, navigate to the **System Administrator > Ops Views** window. (For more information, see the "Viewing Ops Views Details" section on page 6-10.)

After you have installed the necessary license and restarted the server, the Ops Views window displays on the Administration Console and the ops views functionality becomes available for your use. To access the ops views window from the Administration Console, navigate to **System Administrator > Ops Views**. When you click **Ops Views**, the server displays the SYSTEM ops view by default. The SYSTEM ops view is the home base or system-wide view that Cisco IPICS administrators belong to; this view provides visibility across all of the ops views.

Tip Cisco IPICS users who belong to the SYSTEM ops view have visibility to all ops views resources that are configured on the system.

Note Cisco IPICS displays the number of available licenses and concurrent usage information in the License browser window. As a best practice, make sure that you update your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative update in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.

For more information about managing licenses in Cisco IPICS, see the "Managing Licenses" section on page 2-45. For detailed information about licenses and how to obtain them, refer to *Cisco IPICS PMC Installation and User Guide*.

Creating New Ops Views

Only the system administrator can create new ops views on the server. Cisco IPICS allows the system administrator to create an unlimited number of ops views by navigating to the **System Administrator > Ops Views** link in the Administration Console.

After a new ops view has been created, the system administrator can associate resources, such as channels, to the ops view, while the operator creates an operator user who belongs to that ops view and who can manage the ops view resources that are visible within the specific ops view.

Note Although operators and dispatchers cannot create ops views, these users may assign resources, and define the resources that are accessible to, different ops views if they have the necessary permissions. Cisco recommends that each ops view contain at least one dispatcher and one operator to manage the resources that are visible to these roles.

For information about assigning the relevant Cisco IPICS resources to ops views, see the "Performing Ops Views Tasks" section on page 6-18.

Assigning Ops Views Resources

Table 6-1 shows the Cisco IPICS resources that you can associate or assign to different ops views.

Table 6-1 Cisco IPICS Ops View Resources

Resource	Where to Find More Information
Users	Creating a User Who Belongs to an Ops View, page 6-21
User groups	Configuring Ops Views for Existing Users or User Groups, page 6-23
Channels/ Channel groups	Associating a Channel or Channel Group to an Ops View, page 6-25
VTGs	How Ops Views Affect VTGs, page 6-27
Policies	How Ops Views Affect Policies, page 6-28

The Benefits of Using Ops Views

By allowing you to segment your resources, the use of ops views enables greater flexibility and enhanced manageability of Cisco IPICS resources. The ops views feature may provide the following organizational benefits:

- Enhanced management of Cisco IPICS resources, such as users, channels, and VTGs for dispatchers by allowing the creation of customized ops views that enable interoperability.
- Increased security by limiting operator and dispatcher access to certain Cisco IPICS resources and isolating certain Cisco IPICS resources from the view of other users.
- Extended functionality by allowing multiple virtual instances of Cisco IPICS on the server.
- Simplified dispatcher and operator responsibilities by limiting access to only those resources that they need to manage.
- Expanded levels of responsibility by authorizing specific operators or dispatchers for the SYSTEM ops view so that these users can manage resources for the entire system.

Specific Cisco IPICS users are authorized to set up and use ops views. The "Ops Views User Roles" section on page 6-7 explains the ops view user roles.

Ops Views Terminology

When activated, the Cisco IPICS ops views feature adds attributes to various resources so that these resources can be owned and shared by different ops views. Ops views attributes apply to users, user groups, channels, channel groups, VTGs, and policies. You can view these attributes in the Ops View Attributes area of the Administration Console Edit (User/Channel) Details pane.

To access this information for users, navigate to **Operator > Manage Users**. Click to highlight a specific user name; then, click **Details** to display the user information.

To access this information for channels, navigate to **System Administrator > Channels**. Click to highlight a specific channel; then click **Details** to display the channel information.

For information about the Belongs To and Accessible To attributes that Cisco IPICS supports for use with ops views, see the "Ops Views Attributes" section on page 6-6.

Ops Views Attributes

This section describes the ops views attributes that Cisco IPICS supports:

Belongs To

- This attribute determines the ops view that the resource belongs to. In other words, the ops view that you specify for this attribute is the ops view that owns this resource.
- A resource belongs to only one ops view.
- For users, the Belongs To attribute determines the resources that users see when they log in to the Cisco IPICS system. A user can view only those resources that are accessible to the ops view to which they belong.
- A VTG belongs to the same ops view as the dispatcher who created the VTG. A dispatcher who belongs to a specific ops view will always have visibility to the VTGs that belong to that same ops view.
- A policy belongs to the same ops view as the dispatcher who created the policy. A dispatcher who belongs to a specific ops view will always have visibility to the policies that belong to that same ops view.
- When a user logs in to a PMC or a Cisco IP Phone, that user consumes a PMC or Cisco IP Phone usage license. Cisco IPICS calculates this license usage against the license limit of the ops view that the user currently belongs to.
- When a dispatcher activates a VTG, or when an enabled policy activates a VTG, that VTG consumes a Cisco IPICS port license. Cisco IPICS calculates this license usage against the license limit of the ops view that the dispatcher belongs to. When an enabled policy activates a VTG, the ops view that the policy belongs to will be charged the license usage for activation of that VTG.
- Cisco IPICS calculates license usage for a Cisco IPICS port against the license limit of the ops view that a channel belongs to. This usage is calculated on a per-connection basis. For more information about license usage, see the "Ops Views License Usage and Limits" section on page 6-10.

- With the exception of VTGs and policies, the Belongs To attribute does not imply that the specified resource can be accessed by this ops view. However, Cisco IPICS automatically adds the Belongs To attribute to the list of ops views that can access this list for users, user groups, channels, and channel groups.

Note By default, all resources that were added to Cisco IPICS before the ops view feature was enabled belong to the SYSTEM ops view.

Accessible To

- This attribute specifies that the resource is accessible to, or visible to, the ops view(s) that Cisco IPICS displays in this field.
- Users have access only to the resources that are accessible to the ops view to which they belong.
- A resource can be accessible to an unlimited number of ops views or no ops views at all.
- The SYSTEM ops view can always access a resource whether or not the SYSTEM ops view is explicitly added to the list of accessible to ops views.

Note

- When you configure a resource to belong to a specific ops view, Cisco IPICS automatically adds that resource as being accessible to the same ops view.
- When you reconfigure the belongs to field for a resource to a different ops view, Cisco IPICS adds the newly-configured ops view to the accessible to list for that resource. However, Cisco IPICS does not remove, from the list of accessible ops views, the ops view that was previously configured.

Ops Views User Roles

When the ops views functionality is enabled, some Cisco IPICS user roles expand to assume additional responsibilities. Table 6-2 describes the various Cisco IPICS ops view user roles and their associated responsibilities.

Note Operators and dispatchers who belong to an ops view can view the VTGs that also belong to that ops view. In addition, they can also view all resources that are accessible to that ops view. These users may not view any resources that do not belong to, or are not accessible to, that ops view.

Note An operator or a dispatcher who belongs to the SYSTEM ops view can view all resources in all ops views.

Table 6-2 Cisco IPICS Ops View User Roles

Cisco IPICS User Role	Responsibilities
System administrator	• The system administrator can add and delete ops views and can also modify the attributes of ops views. • This system administrator can associate an ops view to a channel and a channel group. • As part of the SYSTEM ops view, the system enables full access to the system administrator (and all users who belong to the SYSTEM ops view); that is, these users can see all of the resources in all of the ops views that are configured on the system. • Only those users who belong to the SYSTEM ops view can be assigned the system administrator or all roles.

Table 6-2 Cisco IPICS Ops View User Roles (continued)

Cisco IPICS User Role	Responsibilities
Operator	• Operators who belong to the SYSTEM ops view must create at least one operator per ops view (for all ops views except the SYSTEM ops view) and define each operator as belonging to a specific ops view. These definitions allow the operators who belong to specific ops view(s) to manage the resources for their individual ops view(s). • The operator can add, edit, and delete users and user groups and assign ops views to users and user groups. • The operator can assign each user or user group to any ops view as long as the operator belongs to the SYSTEM ops view. • The operator can only belong to one ops view. Unless the operator belongs to the SYSTEM ops view, this user is limited to only viewing and managing the resources that belong to the ops views that the operator belongs to or other ops views that are accessible to the operator.
Dispatcher	• The dispatcher can belong to only one ops view. Unless the dispatcher belongs to the SYSTEM ops view, this user is limited to only viewing and managing the resources that are accessible to the ops views that the dispatcher belongs to. • The dispatcher manages VTGs but otherwise cannot make changes that affect ops views. • The dispatcher can share management of a VTG with another dispatcher, even if the dispatchers are in different ops views, if the VTG contains resources that are accessible to each of the ops views. • The dispatcher manages policies that belong to the same ops view as the dispatcher or are associated to VTGs that are accessible to the ops view that the dispatcher can access.

Viewing Ops Views Details

This section includes information about how to view the details about each ops view and how to configure the licenses. It includes the following topics:

- Ops Views License Usage and Limits, page 6-10
- Configuring Licenses for Ops Views Usage, page 6-12

From the **System Administrator > Ops Views** link, you can access the detailed information for each ops view. In the Manage Ops Views pane, click the name of an ops view to highlight it; then, click **Details**. The system displays the details for the specific ops view in the Edit Ops View Details pane.

The Manage Ops Views pane includes information about the number of available license limits for licensable features, which includes Cisco IPICS ports, PMC users, and Cisco IP Phone users. The number in each column represents the number of users or ports that can use Cisco IPICS per the license configuration. For example, the number 50 indicates that 50 ports or users are licensed to use the system; the number 0 indicates that no ports or users are licensed to use the system. In this window, the system also displays, via collapsible lists, the resources that belong to, and the resources that are accessible to, the ops view that you are viewing.

Ops Views License Usage and Limits

Cisco IPICS displays detailed license information for current usage and license limits for licensable features in the Edit Ops Views Details pane. To see this information, click the name of an ops view in the Manage Ops Views pane; then, click **Details**.

Note Be aware that Cisco IPICS displays this information in a browser window. As a best practice, make sure that you update your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative update in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.

Cisco IPICS uses the following criteria to determine license consumption for ports and PMC usage:

- Cisco IPICS Ports Usage—Cisco IPICS ports determine the number of enabled channels and active VTGs that the system can use. An enabled channel or activated VTG consumes a port license. After the channel is deleted or disabled or the VTG is deactivated, the server releases the license and makes it available for use.
  - Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location; that is, if a channel has two multicast addresses that are assigned to the channel, two licenses are used. If one of the multicast addresses is removed, the system releases one of the licenses so that the port now consumes one license.

Note Be aware that VTGs can be automatically activated by an enabled policy and, therefore, consume a license. The ops view that a policy belongs to will be charged the license usage for activation of that VTG. 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.

- Cisco IPICS PMC Usage—A PMC user consumes a license each time that the user logs in to a PMC session. This license is consumed against the ops view that the user belongs to.

  If the same PMC user logs in to multiple PMC sessions from different PMC client machines, that user will consume multiple licenses (one for each PMC session).

Note If all Cisco IPICS licenses have been used, PMC user access to the system will be interrupted. Make sure that you are aware of the current status of PMC licenses and that additional user licenses are purchased and installed immediately if this situation occurs.

Configuring Licenses for Ops Views Usage

In the Edit Ops Views Details pane, the system administrator can configure the number of licenses that should be allocated to ports, PMC users, and Cisco IP Phone users on a per ops view basis by entering the values under the License Limits area.

Note The allocation of licenses per ops view is dependent on the installation of a valid ops view license and ennoblement of the ops view functionality on the server. For more information, see the "Enabling Ops Views" section on page 6-2.

The ability to configure these license limits allows the administrator to distribute and balance the licenses amongst the ops views. This distribution ensures that no one ops view can use more licenses than it has configured. The total number of licenses that can be allocated for each licensable feature cannot exceed the total number of licenses that are available for the entire system.

Note Cisco IPICS automatically computes any available licenses that are not being used in other ops views and allocates them to the SYSTEM ops view.

At any time, the administrator can add and/or remove ops views. When this activity occurs, the available licenses may be taken from the SYSTEM ops view (if available) or added to the SYSTEM ops view. The system administrator can also modify the allocation of ops views licenses to allow redistribution among features or ops views. When the license limits are modified, Cisco IPICS assigns to the SYSTEM ops view any licensable features that are not assigned to a specific ops view.

Additional licenses may be purchased for some or all of the licensable features. If the new license includes a greater number of licenses, Cisco IPICS allocates the additional licenses to the SYSTEM ops view.

Note Cisco IPICS does not support removal or reduction of the number of licenses.

Caution Cisco IPICS does not support the edit or modification of the license file name or file contents in any capacity. If you change or overwrite the license file name, you may invalidate your license and cause the system to become inoperable.

Ops Views Caveats

This section includes information about ops views caveats that apply to this release of Cisco IPICS. For specific information about the caveats that apply to VTGs and sub-VTGs, see the "VTG and Sub-VTG Caveats" section on page 6-14.

The following caveats pertain to the use of Cisco IPICS ops views:

- When you are logged in to Cisco IPICS as a user who belongs to the SYSTEM ops view, or when there are no ops views currently in use, the system does not perform any ops view filtering.
- Users who do not belong to a specific ops view default to the SYSTEM ops view.
- As a Cisco IPICS operator, the system allows you to view and modify only those users that either belong to or are accessible to your ops view. As a Cisco IPICS dispatcher, the system allows you to view and modify only those VTGs that contain resources that either belong to or are accessible to your ops view. You can view only those users and channels that either belong to or are accessible to your ops view.
- VTGs and policies always belong to the ops view of the user who created the VTG or the policy.
- The dispatcher can see all of the resources in a VTG as long as one of the VTG resources is in the same ops view as the dispatcher or if the VTG belongs to the same ops view as the dispatcher. If the remaining resources are not in the same ops view, the system does not display these resources in the Users or Channels panes.
- The system displays only resources that either belong to or are accessible to your specific ops view.
- Members of channel and user groups do not inherit accessibility from the groups; therefore, the system displays all of these resources whether or not they are individually accessible to the specific ops view.

- When you search for a resource by using the search functionality in the Channels, Users, and VTGs panes, the system displays only the resources that are accessible to the specific ops view.
- The policies information that the system displays in the Ops Views window reflects the policies that belong to or are accessible to the specific ops view; that is, the policies that the system shows in this area are those policies that were created by someone who belongs to this ops view.
  - Cisco IPICS enables users who belong to the SYSTEM ops view to view all of the policies that are configured on the server.
  - You can view a policy if the policy contains a VTG and that VTG contains a resource that belongs to or is accessible to your ops view.
  - You cannot view a policy that controls a VTG if that VTG does not contain resources that belongs to or is accessible to your ops view.

VTG and Sub-VTG Caveats

The Cisco IPICS implementation of ops view access for VTGs enables resource sharing among multiple ops views. The ops view functionality allows any dispatcher, who has access to shared resources within a VTG that belongs to a different ops view, to fully access that VTG.

Note When a dispatcher has access to shared resources within a VTG, Cisco IPICS also provides that dispatcher with full control over any of the shared resources in that VTG, such that resources that do not belong to the dispatcher can be modified or deleted.

For example, if a resource (user, channel, or VTG) from ops view 1 is shared within a VTG and the VTG was activated by dispatcher 2 who belongs to a ops view 2, then the VTG belongs to ops view 2. However, dispatcher 1 who belongs to ops view 1 will also be able to access that VTG because at least one of the VTG resources is in the same ops view as the dispatcher who belongs to ops view 1.

The following caveats pertain to VTGs and sub-VTGs when you use ops views:

- As a general rule, VTGs inherit accessibility from the resources that it contains. That is, VTGs belong to the same ops view as the dispatcher who created them.

The following examples depict this rule:

a. If an operator who belongs to the SYSTEM ops view creates a VTG or policy, that VTG or policy belongs to the SYSTEM ops view. The system displays this information in the ops view details pane only for the SYSTEM ops view (it does not display in other ops views).

b. If VTG 1 contains only a single channel (channel 1) and that channel is accessible to ops view 1 and ops view 2, then VTG 1 is also accessible to ops view 1 and ops view 2.

   Table 6-3 shows an example of VTG ops view accessibility.

Table 6-3 VTG Ops View Accessibility

Resource	Contents	Accessibility
VTG 1	Contains a single channel (channel 1)	
Channel 1		Accessible to ops view 1 and ops view 2
VTG 1		Accessible to ops view 1 and ops view 2

- This same general rule applies to VTGs that contain other VTGs (also known as sub-VTGs), depending on their states (see the next bullet for more information about this dependency).

  For example, if VTG 1 contains only VTG 2 and VTG 2 is accessible to ops view 1, then VTG 1 is also accessible to ops view 1 (because VTG 1 contains VTG 2, which is accessible to ops view 1).

  Table 6-4 shows an example of sub-VTG ops view accessibility.

Table 6-4 Sub-VTG Ops View Accessibility

Resource (state)	Contents	Accessibility
VTG 1 (active)	Contains sub-VTG (VTG 2)	
VTG 2 (active)		Accessible to ops view 1
VTG 1		Accessible to ops view 1

- With sub-VTGs, there is a dependency on the active/inactive state of the sub-VTG for purposes of determining accessibility. That is, an active VTG can only inherit accessibility from an active sub-VTG and an inactive VTG can only inherit accessibility from an inactive sub-VTG.

  By using the previous example, this means that if VTG 1 is active and VTG 2 is inactive, then VTG 1 will not be accessible to ops view 1.

  Table 6-5 shows an example of active/inactive state dependency on sub-VTG ops view accessibility.

Table 6-5 Active/Inactive Sub-VTG Ops View Accessibility

Resource (state)	Contents	Accessibility
VTG 1 (active)	Contains sub-VTG (VTG 2)	
VTG 2 (inactive)		Accessible to ops view 1
VTG 1		Not accessible to ops view 1

- An ops view that can access a sub-VTG can also access the resources in the VTG that contains the sub-VTG.
- However, an ops view that can access a VTG that contains a sub-VTG may not be able to access that sub-VTG unless there is a resource in the sub-VTG that provides access to the ops view.

  Table 6-6 shows an example of how resources in sub-VTGs can affect ops view accessibility.

Table 6-6 Sub-VTG Resources for Ops View Accessibility

VTG 1	VTG 2

Table 6-6 Sub-VTG Resources for Ops View Accessibility (continued)

VTG 1 contains the following resources: • User 1, who is accessible to ops view 1 • VTG 2 (sub-VTG)	VTG 2 contains the following resource: • User 2, who is accessible to ops view 2
VTG 1 becomes accessible to the following ops views: • Ops view 1—VTG 1 inherits accessibility from User 1 • Ops view 2—VTG 1 inherits accessibility from VTG 2, which contains User 2	VTG 2 becomes accessible to the following ops view: • Ops view 2—VTG 2 inherits accessibility from User 2
Ops View 1 Dispatcher	**Ops View 2 Dispatcher**
The ops view 1 dispatcher can see the details for the following resources: • VTG 1—User 1, who is accessible to ops view 1, is in VTG 1 (The ops view 1 dispatcher has no access to the contents in VTG 2 because ops view 1 does not have access to ops view 2)	The ops view 2 dispatcher can see the details for the following resources: • VTG 2—User 2, who is accessible to ops view 2, is in VTG 2 • VTG 1—VTG 2 is a sub-VTG of VTG 1

  - The ops view 1 dispatcher can see the details for VTG 1 and can add or remove resources from VTG 1. Because a sub-VTG shows as a resource in a VTG, the ops view 1 dispatcher can also remove the sub-VTG (VTG 2) even though the ops view 1 dispatcher cannot see the details of VTG 2. (The ops view 1 dispatcher can see that VTG 2 is contained in VTG 1 and this dispatcher can make changes even though the contents of VTG 2 cannot be seen.)

- You can use sub-VTGs as a way to shield the participants in the sub-VTG from other resources who should not be able to see them.
- When you associate VTGs to policies, the system displays only the VTG templates that are accessible to the ops view.

- The VTG Workspace pane displays the VTGs that belong to the specific ops view or the VTGs that contain resources that are accessible to the specific ops view. The system displays all contents of a highlighted VTG in this workspace, but the Channels, Users, and VTGs panes display only the resources that are accessible to this specific ops view.

Performing Ops Views Tasks

There are several tasks that must be performed to activate, create, and configure ops views for use on the server. You can also edit or remove ops views, as needed. This section describes these ops views-related tasks and the affect that ops views has on Cisco IPICS resources, such as VTGs and policies.

This section includes the following topics:

Activating the Ops View Feature

To activate the Cisco IPICS ops views feature, you must upload and install the Cisco Ops View license on the server. For information about uploading the license, see the "Uploading the License to the Server" section on page 6-19.

Uploading the License to the Server

To upload the Cisco Ops View license to the server, perform the following procedure:

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 In the Location or Address field, enter the following URL, replacing *IP address* with the IP address of the Cisco IPICS server:

http://<*IP address***>**

Step 3 Log in to the Cisco IPICS server by using the system administrator user name and password.

Tip Be aware that user names and passwords are case-sensitive.

The User menu on the Cisco IPICS server displays.

Step 4 Click the **System Administrator** tab; then click **License**.

The system license information displays.

Step 5 In the Add a License area, click the **Browse** button to locate the license file that you want to upload to the server. Alternatively, you can enter the path for the file in the License File field.

Step 6 Click **Upload** to upload the license file to the server.

Step 7 Click **Apply** to enable the changes to become effective.

If you are uploading a new ops views license, you must restart the server.

Note Step 8 to Step 10 document the procedure for restarting the server. These steps apply only if the ops view license status has changed from "not licensed" to "licensed."

Step 8 To restart the server, connect to the Cisco IPICS server by using SSH Secure Shell client software (or equivalent software).

Step 9 Log in to the server with root user privileges.

Step 10 From root, enter the following command to restart the Tomcat web server:

[root]# service ipics_tomcat restart

The system restarts the Tomcat web server.

With the Cisco Ops View license installed, the ops view functionality is activated and you are ready to use ops views. From this point, you can add new ops views and assign users and resources to the ops views.

Step 11 To create an ops view, continue with the "Creating Ops Views" section on page 6-20.

Note To view the Cisco Ops View license on the server, navigate to **System Administrator > License** and locate the ops view license entry under the Configured License area. For more information about this license, see the "Enabling Ops Views" section on page 6-2.

Creating Ops Views

After you have enabled the ops view feature, you can begin to create ops views.

The system displays the ops views that the system administrator creates and allows Cisco IPICS resources, such as users, user groups, channels, channel groups, VTGs, and policies, to be assigned to these ops views.

Note By default, Cisco IPICS includes a SYSTEM ops view. You cannot delete or edit the SYSTEM ops view.

To create an ops view, perform the following procedure:

Procedure

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

Step 2 From the System Administrator tab, click the **Ops Views** link.

The Manage Ops Views window displays.

Note When you open the Manage Ops Views window for the first time, the system displays the SYSTEM ops view as the default ops view.

Step 3 To add a new ops view, click **Add**.

The Edit Details pane displays.

Step 4 In the Edit Details pane, enter a name for the ops view.

Tip The name that you enter for the ops view should be descriptive to reflect the nature of its use.

Step 5 Enter the applicable license information, as described in the "Configuring Licenses for Ops Views Usage" section on page 6-12.

Step 6 Click **Save**.

The newly-created ops view displays in the Manage Ops Views window.

Creating a User Who Belongs to an Ops View

After the system administrator creates the ops view, an operator must be defined as belonging to the specific ops view.

Note To add the first operator to an ops view, you must be logged in to the server with operator privileges and belong to the SYSTEM ops view.

To create a user who belongs to an ops view, perform the following procedure:

Procedure

Step 1 From the Operator tab, click the **Manage Users** link.

The Manage Users window displays.

Step 2 To add a new user, click the **Add** button that displays under the Users pane.

The Edit User Details pane displays.

Step 3 Enter the user information in the fields that display along the left side of the pane.

Tip User names, including VTG, channel groups, and user groups, must be unique across all ops views that are configured on the server.

Step 4 Click **Save** to apply your changes and save them to the database.

Step 5 In the Ops View Attributes area, complete the **Belongs To** field by choosing an ops view, from the drop-down list box, that the user will belong to.

Note Operators who do not belong to the SYSTEM ops view cannot set the belongs to field to any ops view other than the one to which they belong.

Step 6 In the Ops View Attributes area, complete the **Accessible To** field by clicking the **Edit** button to associate an ops view to this user.

Note When you create a new user, the **Edit** button does not display until you complete the user profile by clicking **Save**.

The Associate Ops Views window displays to show the ops views that this user is visible to and the available ops views.

Step 7 From the list of Available Ops Views, click to highlight the individual ops view that you want to assign to this user. Then, drag the ops view to the User Visible by Ops Views pane.

The system highlights, in green text, the ops view that you dragged.

Step 8 Repeat Step 6 for each ops view that you want to associate to this user.

Step 9 Click **Save** to associate this ops view to the user.

To discard your changes, click **Revert**.

The Associate Ops Views to User window closes. The system displays the ops views that you associated to the user in the Accessible To field.

Note Users who are in the system administrator or all roles must belong to the SYSTEM ops view.

Note Operators who do not belong to the SYSTEM ops view cannot assign the system administrator or all roles to users.

Operators who do belong to the SYSTEM ops view cannot change a user who is in the system administrator or all role to belong to or be accessible to an ops view.

Configuring Ops Views for Existing Users or User Groups

When you configure ops views to users or user groups, the system displays only those users or user groups who are accessible to the specific ops view.

Note You must perform this procedure as a Cisco IPICS operator.

The Cisco IPICS operator may add only those users or user groups who belong to the specific ops view of which the operator is a member.

To configure ops views to a user or user group, perform the following procedure:

Procedure

Step 1 From the Operator tab, click the **Manage Users** link.

The Manage Users window displays.

Step 2 In the User area, click a user name to highlight it; then click **Details**. (To add a user group, click a user group name to highlight it; then, click **Details**.)

The Edit User (or User Group) Details pane displays.

Step 3 In the Ops View Attributes area, complete the **Belongs To** field by choosing an ops view, from the drop-down list box, that this user (or user group) belongs to.

Note The system automatically adds to the accessible to field the ops view that you choose in the belongs to field.

Step 4 In the Ops View Attributes area, complete the **Accessible To** field by clicking the **Edit** button to associate this user (or user group) to an ops view.

The Associate Ops Views window displays to show the ops views that the user (or user group) is visible by and the available ops views.

Note In this window, you can also change the associated ops views that have access to this user or user group.

Step 5 From the list of Available Ops Views, click to highlight the individual ops view that you want to associate to this user (or user group). Then, drag the ops view to the User (or User Group) Visible by Ops Views pane.

The system highlights, in green text, the ops view that you dragged.

Note From the list of Visible Ops Views, you can also click to highlight the individual ops view that you want to disassociate from this user or user group. Then, drag the ops view to the Available Ops Views pane. The system highlights, in red text, the ops view that you dragged.

Step 6 Repeat Step 5 for each ops view that you want to associate (or disassociate).

Step 7 Click **Save** to associate this user or user group to the ops view (or to remove the association between this ops view and the user or user group).

To discard your changes, click **Revert**.

The Associate Ops Views to User (or User Group) window closes. The system displays the updated list of ops views that are associated to the user or user group in the Accessible To field.

Note Users do not inherit accessibility from user groups and user groups do not inherit accessibility from users.

Associating a Channel or Channel Group to an Ops View

When you associate a channel or channel group to an ops view, you must also specify the belongs to and the accessible to fields in the Ops View Attributes area.

Note You must perform this procedure as a Cisco IPICS system administrator and belong to the SYSTEM ops view.

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

Procedure

Step 1 From the System Administrator tab, click the **Channels** link.

The Manage Channels window displays.

Step 2 In the Channels pane, click to highlight a channel (for channel groups, click to highlight a channel group in the Channel Groups pane); then, click **Details**.

The Edit Channel (or Channel Group) Details window displays.

Step 3 In the Ops View Attributes area, complete the **Belongs To** field by choosing an ops view, from the drop-down list box, that this channel (or channel group) belongs to.

Note The system automatically adds to the accessible to field the ops view that you choose in the belongs to field.

Step 4 In the Ops View Attributes area, complete the **Accessible To** field by clicking the **Edit** button to associate the channel (or channel group) to an ops view. Choose the ops views that the channel (or channel group) is accessible to. (This entry defines which ops views can view and manage the channel or channel group.)

The Associate Ops Views window displays to show the associated and available ops views for this channel (or channel group). In this window, you can associate the channel (or channel group) that can has access the ops views.

Note In this window, you can also change the associated ops views that have access to this channel or channel group.

Step 5 From the list of Available Ops Views, click to highlight the individual ops view that you want to associate to this channel. Then, drag the ops view to the Associated Ops Views pane.

The system highlights, in green text, the ops view that you dragged.

Note From the list of Associated Ops Views, you can also click to highlight the individual ops view that you want to disassociate from this channel or channel group. Then, drag the ops view to the Available Ops Views pane. The system highlights, in red text, the ops view that you dragged.

Step 6 Repeat Step 5 for each ops view that you want to associate (or disassociate).

Step 7 Click **Save** to associate this ops view to this channel.

To discard your changes, click **Revert**.

The Associate Ops Views window closes. The system displays the updated list of ops views that are associated to the channel (or channel group) in the Accessible To field.

Note Channels do not inherit ops view associations from channel groups and channel groups do not inherit ops view associations from channels.

How Ops Views Affect VTGs

This section describes the affect that ops views have on VTGs. For the specific caveats that pertain to this section, see the "Caveats" section on page 6-27. For information about additional caveats, see the "VTG and Sub-VTG Caveats" section on page 6-14.

VTGs do not require a dispatcher to associate ops views. The Cisco IPICS implementation automatically determines the ops views that can access each individual VTG based on the VTG contents and the VTG creator.

VTGs belong to the same ops view as the user who created the VTG. Therefore, you do not need to define the belongs to field for VTGs.

For example, if an operator who belongs to the SYSTEM ops view creates a VTG, that VTG belongs to the SYSTEM ops view. The system displays this VTG in the ops view details pane only for the SYSTEM ops view (it does not display this VTG information in any of the other ops views).

Note VTGs always belong to the ops view of the user who created the VTG.

Caveats

Be aware of the following caveats as you use this ops view functionality:

- The VTG Workspace window displays the VTGs that belong to a specific ops view and the VTGs that contain resources that are accessible to specific ops views.
- The system displays all contents of a highlighted VTG in this workspace area, while the inactive VTG resources, such as channels, users, and VTGs, display only the resources that are accessible to the specific ops view.
- The exception pertains to members of a channel or user group, who the system displays whether or not they are individually accessible to the specific ops view.

Tip If a VTG unexpectedly becomes active or inactive, check for any policies that may be associated to the VTG. An operator in another ops view can create a policy that is associated to any VTG that the operator has access to.

How Ops Views Affect Policies

This section describes how ops views affect policies. For specific caveats that pertain to this section, see the "Caveats" section on page 6-28. For information about additional caveats, see the "Ops Views Caveats" section on page 6-13.

You do not need to take explicit action to assign an ops views to a policy. When you create a new policy, or when you have existing policies, the system displays these policies as resources in the ops view of the user who created the policies.

A policy is accessible to any ops view that has access to the VTGs that are associated to the policy.

Note Policies always belong to the ops view of the user who created the policy.

Caveats

Be aware of the following caveats as you use this ops view functionality:

- The policies information that the system displays as resources for a specific ops view reflects the policies that belong to the specific ops view; that is, the policies that the system shows in this area are those policies that were created by someone who belongs to this ops view.
- When the Cisco IPICS operator views the policies in the Manage Policies window, the system displays only those policies that belong to or are accessible to the specific ops view of which the operator is a member.
- When you associate VTGs to policies, the system displays only those VTG templates that are accessible to the specific ops view.
- Like VTGs, policies belong to the same ops view as the user who created them. For example, if an operator who belongs to the SYSTEM ops view creates a policy, that policy belongs to the SYSTEM ops view. The system displays this information in the ops view details pane only for the SYSTEM ops view (it does not display in any of the other ops views).

Tip If a VTG unexpectedly becomes active or inactive, check for any policies that may be associated to the VTG. An operator in another ops view can create a policy that is associated to any VTG that the operator has access to.

Disabling Ops Views

You can disable the ops views functionality on the server after it has been enabled.

Note You must perform this procedure as a Cisco IPICS system administrator.

To disable ops views, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **System Administrator > Options**.

Step 2 Under Options, check the **Ops Views** check box to disable this feature.

This check box allows you to enable and disable ops views.

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

You must restart the server to complete this task.

Step 4 To restart the server, connect to the Cisco IPICS server by using SSH Secure Shell client software (or equivalent software).

Step 5 Log in to the server with root user privileges.

Step 6 From root, enter the following command to restart the Tomcat web server:

[root]# service ipics_tomcat restart

The system restarts the Tomcat web server.

Note To reenable ops views, check the **Ops Views** check box in the System Administrator > Options window, upload the license, and restart the server.

Recovering a Deleted System Administrator User

You can recover your system if you delete the system administrator user name in error and there are no users who can log in to the server by using the system administrator or all role, and there are no users in the SYSTEM ops view (when ops views are enabled).

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

Procedure

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

Note Cisco IPICS includes a safeguard that prevents all operators from being deleted from the system. Therefore, if you have deleted the system administrator user role in error, the operator maintains the ability to assign another system administrator user role.

Step 2 From the Operator tab, click the **Add** button that displays under the Users pane.

The Edit User Details pane displays.

Step 3 In the required fields, that are indicated by an asterisk, enter the user information.

Step 4 From the Roles drop-down list box, choose **system administrator** or **all** for the user role.

The new user appears in the SYSTEM ops view; this user can access the System Administrator tab to perform administrative tasks.