



# CHAPTER 7

## Configuring and Managing Cisco IPICS 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:

- [Managing Cisco IPICS Ops Views, page 7-1](#)
- [Understanding Ops Views Caveats, page 7-7](#)
- [Performing Ops Views Tasks, page 7-11](#)

### Managing 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 Cisco IPICS Administration Console. Ops views do not affect the way in which channels and VTGs display on the IDC or Cisco Unified IP Phone.

When you purchase a Cisco IPICS license, you receive a license with a specified number of ops views. In the License Management window, Cisco IPICS displays the total number of ops view ports, current usage, as well as individual port usage per ops view.

To see detailed information about license limits in the Ops Views configuration window, navigate to the Configuration drawer in the Cisco IPICS Administration Console and click **Ops Views**. See the “[Understanding the Ops Views Window](#)” section on page 7-2 for more information.

For more information about Cisco IPICS license information, see the “[Understanding the License Management Window](#)” section on page 2-64.

When you access the **Ops Views** window, the server displays the SYSTEM ops view by default. The SYSTEM ops view is the home base or system-wide view to which the Cisco IPICS administrators belong. When new ops views are created, ports are reallocated from the SYSTEM ops view to the new ops view, and any additional ops views that you create.

**Note**

Cisco IPICS displays the number of available licenses and concurrent usage information in the License Management 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 2-63](#). For detailed information about how to obtain licenses in this release of Cisco IPICS, see *Cisco IPICS Server Installation and Upgrade Guide*.

This section describes the Cisco IPICS ops view management functions and includes the following topics:

- [Understanding the Ops Views Window, page 7-2](#)
- [Creating New Ops Views, page 7-3](#)
- [Assigning Ops Views Resources, page 7-4](#)
- [The Benefits of Using Ops Views, page 7-4](#)
- [Understanding Ops Views Attributes, page 7-4](#)
- [Understanding Ops Views User Roles, page 7-6](#)

## Understanding the Ops Views Window

The Ops Views window lists information about each of the ops views that have been added in Cisco IPICS. It also lets you perform several ops views management functions.

To display the Ops Views window, navigate to **Configuration > Ops Views**.

[Table 7-1](#) describes the items in the Ops Views window.

**Table 7-1** *Items in the Ops Views Window*

Item	Description	Reference
Name field	Unique identification name that is assigned to the ops view.	See the <a href="#">“Performing Ops Views Tasks” section on page 7-11</a> .
LDAP Enabled field	Indicates whether LDAP is enabled for this ops view. When LDAP is enabled, LDAP is used for authenticating Cisco IPICS users.	
Dial Number field	Number that is configured in the ops view and which users dial to access Cisco IPICS from an IP phone.	
LMR Ports Limit field	Maximum number of land mobile radio (LMR) license ports that are allocated to this ops view.	
Multicast Ports Limit field	Maximum number of multicast license ports that are allocated to this ops view.	
IDC Users Limit field	Maximum number of IDC users license ports that are allocated to this ops view.	

**Table 7-1** *Items in the Ops Views Window (continued)*

Item	Description	Reference
Cisco Unified IP Phones Limit field	Maximum number of Cisco Unified IP Phone license ports that are allocated to this ops view.	See the “ <a href="#">Performing Ops Views Tasks</a> ” section on page 7-11.
Dial Ports Limit field	Maximum number of dial ports that are allocated to this ops view.	
Add button	Click this button to add an ops view.	See the “ <a href="#">Adding Ops Views</a> ” section on page 7-11.
Delete button	Click this button to delete an ops view.	See the “ <a href="#">Deleting Ops Views</a> ” section on page 7-21.
Resources button	Click this button to view the resources that belong to or are accessible to the ops view.	See the “ <a href="#">Viewing Resources That Belong To and are Accessible To Ops Views</a> ” section on page 7-15.

## Creating New Ops Views

Only the system administrator can create new ops views on the server. The number of ops views that can be created depends on the number of ops view ports that the Cisco IPICS license provides. You can view the number of ops view ports that are in the system by accessing the Administration > License Management window in the Cisco IPICS Administration Console. For more information about ops view ports, see the “[Understanding the License Management Window](#)” section on page 2-64 to view ops view ports.

After a new ops view has been created, you can associate resources, such as channels, to the ops view. 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. For more information, see [Table 7-3 on page 7-6](#).

When a resource contains or is associated to another resource that belongs to the ops view of a user, the user has the ability to remove the associated resource but cannot modify it in any other way.

For example, a VTG that belongs to an ops view called A Team contains a channel that belongs to an ops view called B Team. A dispatcher, who belongs to the A Team ops view, has the ability to modify any resources in the VTG including adding or removing participants who are accessible to the A Team ops view. The dispatcher can also activate or deactivate the VTG.

A dispatcher, who belongs to the B Team ops view, has the ability to view the VTG and remove the channel from the VTG, but cannot modify any resources.



### 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 7-11.

## Assigning Ops Views Resources

Table 7-2 shows the Cisco IPICS resources that you can associate or assign to different ops views and where you can find additional information about assigning ops view to resources.

**Table 7-2** Cisco IPICS Ops View Resources

Resource	Where to Find More Information
Users	<a href="#">Managing Ops Views for a User, page 3-24</a>
User groups	<a href="#">Managing Ops Views for a User Group, page 3-32</a>
Channels	<a href="#">Associating Users to PTT Channels, page 2-17</a>
Channel groups	<a href="#">Associating Ops Views to Channel Groups, page 2-26</a>
VTGs	<a href="#">Managing VTGs, page 5-2</a> and <a href="#">Understanding VTG and Sub-VTG Caveats, page 7-8</a>
Policies	<a href="#">Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine,”</a> and <a href="#">Chapter 6, “Using the Cisco IPICS Policy Engine.”</a>

## 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

User roles determine which users can do various ops view-related activities. The [“Understanding Ops Views User Roles”](#) section on page 7-6 explains the ops view user roles.

## Understanding Ops Views Attributes

This section describes the following 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.

**Note**

Only an operator or a dispatcher who belongs to a certain ops view should create, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are associated with that ops view. This situation can cause inconsistencies when users view policies. For more information, see [Chapter 6, “Using the Cisco IPICS Policy Engine,”](#) and [Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine.”](#)

- When a user logs in to an IDC or a Cisco Unified IP Phone, that user uses an IDC or Cisco Unified IP Phone 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 uses a concurrent multicast 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 is charged the license usage for activation of that VTG.
- Cisco IPICS calculates license usage for a concurrent LMR 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 [“Managing Ops Views License Usage and Limits” section on page 7-16.](#)

**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.
- The SYSTEM ops view can always access all resources even if it does not explicitly appear in the list of accessible 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 that 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 the previously-configured ops view from the list of accessible ops views. The resource is accessible to the previous ops view, as well as the newly-configured ops view.

## Understanding Ops Views User Roles

Some Cisco IPICS user roles expand to assume additional responsibilities. [Table 7-3](#) 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.

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

**Table 7-3** Cisco IPICS Ops View User Roles

Cisco IPICS User Role	Responsibilities
System Administrator	<ul style="list-style-type: none"> <li>The system administrator can add and delete ops views and can also modify the attributes of ops views.</li> <li>This system administrator can associate an ops view to a channel and a channel group.</li> <li>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.</li> <li>Only those users who belong to the SYSTEM ops view can be assigned the system administrator or all roles.</li> </ul>
Operator	<ul style="list-style-type: none"> <li>Operators who belong to the SYSTEM ops view should 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).</li> <li>The operator can add, edit, and delete users and user groups and assign ops views to users and user groups.</li> <li>The operator can assign each user or user group to any ops view as long as the operator belongs to the SYSTEM ops view.</li> <li>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.</li> </ul>

Table 7-3 Cisco IPICS Ops View User Roles (continued)

Cisco IPICS User Role	Responsibilities
Dispatcher	<ul style="list-style-type: none"> <li>• 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.</li> <li>• The dispatcher manages VTGs but otherwise cannot make changes that affect ops views.</li> <li>• 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.</li> <li>• 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.</li> </ul>
Ops View Administrator	<p>The ops view administrator is allowed to access the following Cisco IPICS windows:</p> <ul style="list-style-type: none"> <li>• Activity Logs—Accessed by navigating to <b>Administration &gt; Activity Log Management</b> (includes downloading activity logs)</li> <li>• Activity Log Options—Accessed by navigating to <b>Administration &gt; Activity Log Options</b></li> <li>• Policies—Accessed by navigating to <b>Policy Engine &gt; Policy Management</b> (includes Associations window)</li> </ul>

## Understanding 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 [“Understanding VTG and Sub-VTG Caveats” section on page 7-8](#).

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

- 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 who 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.

**Note**

Only an operator or a dispatcher who belongs to a certain ops view should create, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are associated with that ops view. This situation can cause inconsistencies when users view policies. For more information, see [Chapter 6, “Using the Cisco IPICS Policy Engine,”](#) and [Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine.”](#)

## Understanding 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.

For example, if a resource, (user, channel, or VTG) from ops view 1 is within a VTG and the VTG was activated by dispatcher 2 who belongs to ops view 2, the VTG is accessible to ops view 2. However, dispatcher 1 who belongs to ops view 1 is also able to access that VTG because at least one of the VTG resources is accessible 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 a dispatcher who belongs to the SYSTEM ops view creates a VTG, 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 7-4](#) shows an example of VTG ops view accessibility.

**Table 7-4 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 7-5 shows an example of sub-VTG ops view accessibility.

**Table 7-5 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 7-6 shows an example of active/inactive state dependency on sub-VTG ops view accessibility.

**Table 7-6 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 7-7 shows an example of how resources in sub-VTGs can affect ops view accessibility.

**Table 7-7 Sub-VTG Resources for Ops View Accessibility**

<b>VTG 1</b>	<b>VTG 2</b>
VTG 1 contains the following resources: <ul style="list-style-type: none"> <li>User 1, who is accessible to ops view 1</li> <li>VTG 2 (sub-VTG)</li> </ul>	VTG 2 contains the following resource: <ul style="list-style-type: none"> <li>User 2, who is accessible to ops view 2</li> </ul>
VTG 1 becomes accessible to the following ops views: <ul style="list-style-type: none"> <li>Ops view 1—VTG 1 inherits accessibility from User 1</li> <li>Ops view 2—VTG 1 inherits accessibility from VTG 2, which contains User 2</li> </ul>	VTG 2 becomes accessible to the following ops view: <ul style="list-style-type: none"> <li>Ops view 2—VTG 2 inherits accessibility from User 2</li> </ul>
<b>Ops View 1 Dispatcher</b>	<b>Ops View 2 Dispatcher</b>
The ops view 1 dispatcher can see the details for the following resources: <ul style="list-style-type: none"> <li>VTG 1—User 1, who is accessible to ops view 1, is in VTG 1</li> </ul> <p>(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)</p>	The ops view 2 dispatcher can see the details for the following resources: <ul style="list-style-type: none"> <li>VTG 2—User 2, who is accessible to ops view 2, is in VTG 2</li> <li>VTG 1—VTG 2 is a sub-VTG of VTG 1</li> </ul>

- 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 VTGs that are accessible to the ops view.
- The Virtual Talk Groups window 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 window, but the Channels, Users, and VTGs windows display only the resources that are accessible to this specific ops view.

## Understanding How Ops Views Affect VTGs

This section describes the affect that ops views have on VTGs. For information about additional caveats, see the [“Understanding VTG and Sub-VTG Caveats” section on page 7-8](#).

VTGs do not require a dispatcher to associate ops views. Cisco IPICS 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.

---

## VTG Caveats

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

- The Virtual Talk Groups 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 window.
- 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. For more information, see the [“Managing Ops Views License Usage and Limits”](#) section on page 7-16.

---

## Performing Ops Views Tasks

There are several tasks that must be performed to 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:

- [Adding Ops Views, page 7-11](#)
- [Viewing Resources That Belong To and are Accessible To Ops Views, page 7-15](#)
- [Viewing Ops Views License Details, page 7-16](#)
- [Deleting Ops Views, page 7-21](#)

## Adding 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.

To add an ops view, perform the following procedure:

**Procedure**

**Step 1** From the Configuration drawer in the Cisco IPICS Administration Console, click **Ops Views**.



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

**Step 2** To add a new ops view, click **Add**.

**Step 3** In the Name field, 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 4** In the Description field, enter a description for the new ops view that you are adding.  
The Description field is an optional field.

**Step 5** In the **License Allocation** pane, enter applicable license information in the fields, as described in the [Table 7-8](#).



**Note** The Current Usage values in the License Allocation pane indicate the number of license ports for the feature that are currently in use.

**Table 7-8 License Allocation Fields in the Ops View Window**

Feature	Limit
LMR Ports	Number of LMR license ports that you allocate for this ops view. Enter the number of LMR ports in the Limit field.
Multicast Ports	Number of multicast license ports that you allocate for this ops view. Enter the number of multicast ports in the Limit field.
IDC Silver Users	Number of IDC silver users ports that you allocate for this ops view. Enter the number of IDC silver users ports in the Limit field.
IDC Platinum Users	Number of IDC platinum users ports that you allocate for this ops view. Enter the number of IDC platinum users ports in the Limit field.
IDC Mobile Users	Number of IDC mobile users ports that you allocate for this ops view. Enter the number of IDC mobile users ports in the Limit field.
Cisco Unified IP Phones	Number of Cisco Unified IP Phone ports that you allocate for this ops view. Enter the number of Cisco Unified IP Phone ports in the Limit field.
Dial Ports	Total number of dial ports that you allocate for this ops view. These ports are used for both the dial-in/invite and notification features. Enter the number of dial ports in the Limit field.

For more information about managing licenses for ops views, see the [“Viewing Ops Views License Details”](#) section on page 7-16.

**Step 6** In the **Dial Information and Dial Port Resource Allocation** pane, enter applicable dial information in the fields, as described in the [Table 7-9](#).

For information about how to allocate dial ports, see the [“Allocating Dial Ports for the Dial-In/Invite and Notification Features” section on page 7-18](#). For more detailed information about the dial-in/invite and notification features, see [Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine,”](#) and [Chapter 6, “Using the Cisco IPICS Policy Engine.”](#)



**Note** When you add dial numbers (DNs) for ops views in a Cisco IPICS deployment that includes the policy engine, and if the new DN falls outside of existing route patterns that are assigned to a SIP trunk (in Cisco Unified Communications Manager) or outside of existing destination patterns that are assigned to a dial peer (in the Cisco IOS SIP gateway), then you must update the SIP provider configuration to include the new DN. For more information, see the [“Configuring the SIP Provider” section on page 8-32](#).

**Table 7-9** *Dial Information and Dial Port Resource Allocation Fields in the Ops View Window*

Field	Description
Dial Number	This field specifies the number that users, who belong to this ops view, will dial in to Cisco IPICS.  <b>Note</b> When the policy engine is installed and you want to assign a DN to allow for dial-in access, you must assign the DN to an ops view.
Email address of the sender	This field specifies the e-mail address that Cisco IPICS uses to send out notifications to users in the ops view. When users who belong to the ops view, receive an e-mail notification, this e-mail address is the address from which Cisco IPICS sends the e-mail message.
Default language	This field specifies the language in which the notifications are sent, as well as the language that is used by the dial engine to determine which voice prompts to play to users who call in to Cisco IPICS.  <b>Note</b> Only Latin-1 supported languages give callers the option to spell the name of the channel/VTG/policy when calling in to Cisco IPICS.
Dial ports reserved for dial-in/invite feature	This field specifies the number of dial ports that you allocate for exclusive use by the dial-in/invite feature for the ops view. Dial ports allocated here are used only by the dial-in/invite feature; they are not used by the notifications feature.  The dial-pool number of ports that you configure in this window are typically allocated for dial-in users who typically engage in long conversations on VTGs or channels.  The dial ports that Cisco IPICS uses for notifications are allocated from the ops view of the policy that includes the notification action (the ops view of the user who created the policy).  <b>Note</b> The number of ports that you allocate in this window cannot exceed the number of dial users who may be allocated from the SYSTEM ops view.

**Table 7-9** Dial Information and Dial Port Resource Allocation Fields in the Ops View Window

Field	Description
Dial ports reserved for notifications	<p>This field specifies the number of dial ports that you allocate for exclusive use by the notifications feature for the ops view. Dial ports that you allocate in this window are not used by the dial-in/invite feature.</p> <p>The dial-pool number of ports that you configure in this window are allocated for blast notification. Blast notifications are sessions that are typically short in duration and play out short messages; then, exit.</p> <p>The dial ports that Cisco IPICS uses for the notifications feature are allocated from the ops view of the policy that includes the notification action (the ops view of the user who created the policy).</p> <p><b>Note</b> The number of ports that you allocate in this window cannot exceed the number of dial ports that may be allocated from the SYSTEM ops view.</p>
Dial ports reserved for dial-in/invite or notifications	<p><i>Display only</i>—This number represents the total number of dial ports that are available for both the dial-in/invite and notification features. If you do not allocate all of the licensed dial ports specifically for dial-in/dial-out or notifications, Cisco IPICS allocates the remainder of the licensed dial ports to this field.</p> <p>This field displays the number of remaining dial ports after subtracting the ports that were configured for both the dial-in/invite and notification features.</p> <p>For information about how to configure dial ports, see the <a href="#">“Allocating Dial Ports for the Dial-In/Invite and Notification Features”</a> section on page 7-18.</p>



**Note** Be aware that when you allocate the number of ports in your dial pool, this number should match the number of outbound/inbound ports that are available on the gateway. The available physical ports should match the total number of outbound and inbound calls. For more information about allocating dial ports, see the [“Allocating Dial Ports for the Dial-In/Invite and Notification Features”](#) section on page 7-18.

For more information about the Cisco dial engine, see [Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine.”](#)

**Step 7** In the LDAP Authentication pane, check the Use LDAP Authentication check box if you want to enable LDAP authentication for users who are associated with this ops view.

For more information about LDAP authentication, see the [“Configuring LDAP”](#) section on page 2-98.

**Step 8** To save your changes, click **Save**.

A Resources button displays at the bottom of the window. You can now view the resources that are accessible to this ops view. See the [“Viewing Resources That Belong To and are Accessible To Ops Views”](#) section on page 7-15.

For information about assigning resources to ops views, see the [“Assigning Ops Views Resources”](#) section on page 7-4.

## Viewing Resources That Belong To and are Accessible To Ops Views

When you have created an ops view in Cisco IPICS, resources can be assigned to the ops view. See the [“Assigning Ops Views Resources” section on page 7-4](#) for more information about how resources are assigned to ops views.

To view resources that either belong to, or are accessible to ops views, perform the following procedure:

### Procedure

- 
- Step 1** From the Configuration drawer in the Cisco IPICS Administration Console, click **Ops Views**.
- Step 2** To view ops view resources, take either of these actions:
- In the Name column, click the link of the ops view for which you want to view resources; then, click the **Resources** button at the bottom of the window.
  - Check the check box to the left of the ops view for which you want to view resources; then, click the **Resources** button at the bottom of the window.

The Resources window displays.

- Step 3** Take either of the following actions:
- To view resources that belong to this ops view, choose **Resources That Belong To This Ops View** from the View drop-down list.
    - Proceed to [Step 4](#).
  - To view resources that are accessible to this ops view, and that could be assigned to it, choose **Resources That Are Accessible To This Ops View** from the View drop-down list.
    - Proceed to [Step 4](#).

The resource window that you choose displays, showing information tabs for each resource.

- Step 4** To view the specific resources that either belong to or are accessible to this ops view, take any of the following actions:
- To view channels that belong to or are accessible to this ops view, click the **Channels** tab.




---

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

---

The channels display, showing the channel name and status for each channel.

- To view channel groups that belong to or are accessible to this ops view, click the **Channel Groups** tab.

The channel groups display, showing the channel group name, ops view, and channel count for each channel group.

- To view users who belong to or are accessible to this ops view, click the **Users** tab.




---

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

---

The users displays, showing the user name, last name, first name, and status of each user.

- To view the user groups that belong to or are accessible to this ops view, click the **User Groups** tab.

The user groups display, showing the user group name and ops view for each user group.

- To view the VTGs that belong to or are accessible to this ops view, click the **VTGs** tab.



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

The list of VTGs display, showing the VTG name and status of each VTG.

- To view the policies that belong to or are accessible to this ops view, click the **Policies** tab.

The policies display, showing the policy name of each policy.

## Viewing Ops Views License 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:

- [Managing Ops Views License Usage and Limits, page 7-16](#)
- [Configuring Licenses for Ops Views Usage, page 7-18](#)

To access the detailed information for each ops view, from the Configuration drawer of the Cisco IPICS Administration Console click the **Ops Views** link. In ops view configuration window, click the name of an ops view to highlight it. The system displays the details for the specific ops view.

The ops view window includes information about the number of available license limits for licensable features, which includes LMR ports, multicast ports, IDC users, IP phones, and dial ports, as well as dial information. This information displays in the **General** tab of the window.

The numbers in the License Allocation pane represent 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.

For more information about the ops view configuration window, see the [“Performing Ops Views Tasks” section on page 7-11](#).

## Managing Ops Views License Usage and Limits

Cisco IPICS displays detailed license information for current usage and license limits for licensable features. To view this information, navigate to the Configuration > Ops Views window; then click the name of the ops view.



### 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 LMR ports, multicast ports, IDC usage, IP phones, and dial ports usage:

- **LMR Ports Usage**—LMR ports determine the number of enabled channels that the system can use. After the channel is deleted or disabled or the VTG is deactivated, the server releases the license and makes it available for use. An ops view is only charged for active channels to which it belongs.
- **Multicast Ports Usage**—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. An ops view is only charged for VTGs that have been activated by dispatchers who belong to the ops view. A VTG can belong to only one ops view but be activated by a different ops view to which another dispatcher belongs; however, the activating ops view is charged with the license.



**Note** Be aware that VTGs can be automatically activated by an enabled policy and, therefore, use a license. The ops view that a policy belongs to is charged the license usage for activation of that VTG. If the number of licenses has been exceeded, the policy is not able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.

- **Cisco IPICS IDC User Usage**—An IDC silver, platinum, or mobile user uses a license each time that the user logs in to an IDC. This license is used against the ops view to which the user belongs.



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

- **IP Phones Usage**—An IP phone user uses a license each time that the user dials in to a VTG or channel via an IP phone. This license is used against the ops view to which the user belongs.
- **Dial Ports Usage**—Cisco IPICS uses these licenses for dial-in, dial-out, or notification connections. For dial ports that are allocated among the ops view, dial ports are used by dial-in according to the phone number that is dialed. Each ops view has a preassigned dial-in phone number for this purpose. For dial-out, the dial ports are used from the ops view to which the user, to be dialed, belongs.



**Note** The policy engine requires that a dial connection make use of two multicast addresses, one for receive and one for transmit. The two multicast addresses are used only if the dial connection is used to join a VTG or channel. If the dial connection is used for notification purposes, then no multicast addresses are used.

See the [“Configuring Licenses for Ops Views Usage”](#) section on page 7-18 for more information about allocating dial ports.

For more detailed information about the dial-in/invite and notification features, see [Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine,”](#) and [Chapter 6, “Using the Cisco IPICS Policy Engine.”](#)

## Configuring Licenses for Ops Views Usage

You can configure the number of licenses that should be allocated to ports, IDC users, and IP phone users, and dial users on a per ops view basis by entering the values in the License Allocation Limit field in the Ops View Configuration window.

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.

Ports are allocated in proportion to the number of ports that are requested by an ops view, relative to the other ops views.

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.



### 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.

## Allocating Dial Ports for the Dial-In/Invite and Notification Features

You must allocate dial ports for users to be able to dial in to Cisco IPICS, dial out to other users, or for the system to notify users. These dial ports are configured in the Dial Information and Dial Port Resources Allocation pane in the Ops View window, and are allocated per ops view. When you allocate the dial ports, be aware of the considerations in the following sections:

- [Understanding Dial Port Pools, page 7-18](#)
- [Determining How Many Dial Ports to Allocate, page 7-19](#)

### Understanding Dial Port Pools

Dial port containers (also referred to as *dial pools*) allow you to configure reserve dial ports that are only used for specific dial functions (such as dial-in/invite and notification).

These reserved dial ports ensure that you always have ports configured specifically for this use and that they cannot be used for any other purpose. The following dial pools are used for reserving ports for dial-in/invite and notification:

- Dial ports reserved for dial-in/invite—This dial pool contains dial ports that can only be used for the dial-in and invite features.

- Dial ports reserved for notification—This dial pool contains dial ports that can only be used for notification.

**Note**

When you create a new ops view, dial port licenses are reallocated from the SYSTEM ops view to the new ops view, but there is no adjustment to the dial port numbers that were configured in the Dial ports reserved for dial-in/invite and Dial ports reserved for notification dial pools for the SYSTEM ops view. For the new ops view, if the dial port numbers that you configure in the reserved dial pools exceed the number of ports in the Dial Ports field, Cisco IPICS displays an error message to alert you. To resolve this issue, reduce the number of reserved ports in the SYSTEM ops view to an appropriate number and try again.

The following list provides detailed information about the dial port fields in the Dial Information and Dial Port Resource Allocation pane:

- The Dial ports reserved for dial-in/invite or notifications field is the dial pool that contains ports that Cisco IPICS uses for both dial-in/invite and for notification. This field is a read-only field that displays as dimmed.

The ports that display in this field are the ports that remain after you have reserved dial ports for dial-in, invite, and notification actions. The remaining number are the dial ports that are reallocated from the total number of dial ports in the Dial Ports dial pool.

For example if there are 20 dial ports total (in the Dial Ports pool) and you have configured 5 of those dial ports in the Dial ports reserved for dial-in/invite field, and 2 dial ports in the Dial ports reserved for notification field, the Dial ports reserved for dial-in/invite or notification field display 13 dial ports.

This total equals the number of ports remaining after subtracting 5 ports for dial-in/invite and 2 for notification. The Dial Ports field still displays 20, the total number of dial ports.

- When a dial-in or invite action executes, Cisco IPICS first checks the Dial ports reserve for dial-in/invite or notification dial pool for an available dial port that can be used for dial-in/invite. If there are not enough available dial ports in that dial pool, Cisco IPICS checks the Dial ports reserved for dial-in/invite dial pool.
- In the same way, when a notification action executes and there are no available dial ports in the Dial ports reserved for dial-in/invite or notification dial pool, Cisco IPICS checks the Dial ports reserved for notification dial pool to obtain the dial ports.
- Ports from the available dial pool are used by the currently executing policy actions. If there are fewer dial ports available than what is needed, the other individual policy actions are held in a waiting state until ports become available.

### Determining How Many Dial Ports to Allocate

When you need to determine how many dial ports to allocate for a particular function, you should consider that some actions, such as notification, are usually needed on a short-term basis. Other actions, such as dialing in to a VTG, usually require dial ports for longer periods of time.

For example, when notifications are sent out, the dial ports are used only briefly because once the notification has been sent the dial port is no longer needed and becomes available again. Therefore, when you allocate ports for dial-in/invite and notification, you may want to allocate a greater number of ports for dial-in and a smaller number for notification.

**Note**

Be aware that when you allocate the number of ports in your dial pool, this number should match the number of outbound/inbound ports that are available on the gateway. The available physical ports should match the total number of outbound and inbound calls.

To allocate dial ports in the Ops View window, see the [“Adding Ops Views” section on page 7-11](#).

For license allocation and dial information field descriptions, see the [“Adding Ops Views” section on page 7-11](#).

For more detailed information about the way that dial-in/invite (also referred to as *dial-out*) and notification features work, see [Chapter 8, “Configuring and Managing the Cisco IPICS Policy Engine,”](#) and [Chapter 6, “Using the Cisco IPICS Policy Engine.”](#)

## Associating a User or User Group to an Ops View

After you create the ops view, an operator must be defined as belonging to the specific ops view.

**Tip**

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.

**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 system administrator or all role user to belong to or be accessible to an ops view.

For detailed information about how to associate a user to an ops view, see the [“Managing Ops Views for a User” section on page 3-24](#), and the [“Managing Ops Views for a User Group” section on page 3-32](#).

## 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 Views pane.

**Note**

To associate a channel or channel group to an ops view, you must be assigned the system administrator role and belong to the SYSTEM ops view.

For detailed information about how to associate a channel or channel group to an ops view, see the [“Associating Users to PTT Channels” section on page 2-17](#) and the [“Associating a Channel or Channel Group to an Ops View” section on page 7-20](#).

## Deleting Ops Views

To delete ops views from Cisco IPICS, perform the following procedure:

### Procedure

---

**Step 1** From the Configuration drawer in the Cisco IPICS Administration Console, click **Ops Views**.

**Step 2** Check the check box next to the ops view that you want to delete.



---

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

---

**Step 3** Click **Delete**.

**Step 4** To confirm the delete operation, click **OK** when prompted.

**Step 5** From the list of provided ops views, choose the ops view to which all resources (users, user groups, channels, channel groups, and VTGs) and licenses should be transferred. All transferred resources are reallocated to belong to the selected ops view.

**Step 6** To finalize the resource update and to delete the ops view, click **OK**.

---

