Cisco IPICS Server Administration

This chapter describes the various administration tasks and concepts that are important to understand when you use Cisco IPICS and includes the following sections:

You install the Cisco IPICS software on supported Cisco Media Convergence Servers (MCS). Before you can perform administration tasks in Cisco IPICS, you must first install the Cisco IPICS operating system and the Cisco IPICS server software.

For detailed information about installing Cisco IPICS, refer to the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1).*

Managing Cisco IPICS Licenses

You must first purchase and upload the applicable license file(s) on to the Cisco IPICS server to use any of the features that are available in Cisco IPICS or to use the Cisco IPICS Administration Console.

After you complete the Cisco IPICS installation, you use the Product Authorization Key (PAK) that was included in your Cisco IPICS product package to obtain the license file.

The license that you purchase is based on the total number of the following licensable features:

- The concurrent number of land mobile radio (LMR) ports
- The concurrent number of multicast ports
- The concurrent number of PMC users
- The concurrent number of IP phone users
- The concurrent number of dial users (this feature is dependent on the policy engine, which must be specifically enabled for use)
- The concurrent number of ops views

Tip The total number of licensable features cannot exceed the number that is specified in the license or licenses that you purchased. If you require additional licenses, contact your Cisco representative.

Note Cisco IPICS does not support the use of release 1.x licenses when you use release 2.0(1). You must purchase and install new license(s) that are compatible with release 2.0(1). To obtain new licenses for this release, contact your authorized Cisco representative.

To purchase your Cisco IPICS license file(s), access the following URL:

http://www.cisco.com/go/license

Tip Be sure to register with Cisco.com before trying to process a license order.

After you have purchased your license file, you can upload the file(s) by accessing the **Administration > License Management** window in the Administration Console. Refer to the *Cisco IPICS Server Administration Guide* for information about how to upload and apply your Cisco IPICS licenses.

Logging In to and Out of Cisco IPICS

You must log in to the Cisco IPICS Administration Console to perform any administration functions. When you have finished using Cisco IPICS, you log out of the Administration Console.

Note Because the Cisco IPICS Administration Console times out after 30 minutes of no use. When this timeout occurs, you are not able to perform any functions in the Administration Console until you log back in.

You must install the Cisco IPICS operating system and server software, and upload one or more license files before you can log in to Cisco IPICS. For detailed information about obtaining license file(s), refer to the *Cisco IPICS Server Administration Guide*.

To log in to and out of Cisco IPICS, complete the following steps:

Step 1 To log in to Cisco IPICS, follow these steps:

a. Launch your browser and enter the IP address or host name of the Cisco IPICS server in the Address field.

b. Enter your user name and password.

Note Be aware that passwords are case-sensitive and must be entered exactly as they were configured by the Cisco IPICS operator.

c. Click **Log In**.

The Cisco IPICS Administration Console displays the My Profile window. You see only the information that relates to your user ID and the user role that was assigned to you.

Step 2 To log out of Cisco IPICS, click the **Logout** button that displays in the menu at the top of the Administration Console window.

The Cisco IPICS window closes and you return to the Cisco IPICS login window.

Accessing Online Help in the Administration Console

You can access the Cisco IPICS help system from any window in the Administration Console by clicking **Help** in the menu at the top of the window. The help system provides online access to the information that is contained in the *Cisco IPICS Server Administration Guide*. This help system is whenever you use the Administration Console.

Important Cisco IPICS Concepts

You should be aware of some important concepts when you use Cisco IPICS. The following sections describe some of these concepts:

- Understanding Locations, page 2-4
- Understanding VTGs, page 2-6
- Understanding Ops Views, page 2-7
- Understanding Associations, page 2-12

Understanding Locations

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

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

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

Note The ALL location defines the scope or reachability or a multicast address. For this reason, the ALL location is applicable to channels and VTGs, which are associated with multicast addresses, but not applicable to IP phones and RMS components, which are not associated with multicast addresses.

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

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

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

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

Note Each RMS component that you configure for use with Cisco IPICS must be associated with a location. An RMS can host only those channel resources that are assigned to the same location as the RMS or to the ALL location. If the RMS is associated with the ALL location, it can host only those channels that are also assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location to an RMS.

Tip Whenever possible, user access via multicast communications is preferable over SIP to minimize the use of RMS resources.

For more detailed information about configuring locations, refer to the *Cisco IPICS Server Administration Guide* and the *Cisco IPICS PMC Installation and User Guide.*

Understanding VTGs

A VTG enables multiple participants on various channels to communicate by using a single multicast address. Participants in a VTG can include users, user groups, channels, channel groups, and other VTGs. An active VTG is a VTG in which all the participants have live connections with each other.

Cisco IPICS dispatchers can stage a VTG by creating a VTG template, which is an inactive VTG. The dispatcher uses a VTG template to arrange participants who can communicate when the VTG template is activated.

A VTG template allows the dispatcher to create various arrangements of members without committing network resources or affecting other VTGs that are in progress.

After the VTG is activated, the dispatcher can add and remove users, channels, and other VTGs, notify and dial out to VTG participants, and mute and unmute PMC users at any time; however, when the dispatcher makes changes to an active VTG, the original VTG template remains unchanged.

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

For more detailed information about VTGs, refer to the *Cisco IPICS Server Administration Guide*.

Understanding Ops Views

Cisco IPICS ops views provide the ability to organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other, providing increased security by limiting operator and dispatcher access. While these views are maintained separately by the 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. In other words, resources in separate ops views are not accessible to users in other ops views unless the users are granted permission to access them.

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 Unified IP Phone.

Ops View Port Allocation

When you purchase Cisco IPICS license(s), the license includes a specified number of ops views that you can configure. By default, Cisco IPICS includes the SYSTEM ops view with every installation. Cisco IPICS users who belong to the SYSTEM ops view can view all ops views, and their resources, that are configured on the system.

Each time the system administrator adds a new ops view, ports are reallocated from the SYSTEM ops view and distributed to the newly created ops view. The system administrator determines the number and types of ports, such as PMC ports, LMR ports, and dial ports that are needed for a particular ops view.

Note If the Cisco IPICS license contains the policy engine, the system administrator can configure dial information per ops view.

When you add dial numbers (DNs) for ops views in a Cisco IPICS deployment that includes the policy engine, and if the new DNs fall outside of existing route patterns that are assigned to a SIP trunk (in Cisco Unified CallManager) or outside of existing destination patterns that are assigned to a dial peer (in Cisco IOS), you must update the SIP provider configuration to include the new DNs. For detailed information, refer to the *Cisco IPICS Server Administration Guide*.

When an ops view gets deleted, the system administrator has the option to reallocate the resources that were in the deleted ops view to other existing ops views in the system.

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 **Configuration > Ops Views** window.

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 which 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 Dial ports reserved for dial-in/invite or notifications field is a read-only field that displays ports that Cisco IPICS allocates for both dial-in/invite and notification actions. The ports that display in this field are the ports that remain after you have reserved dial ports for dial-in, invite, and notification. The remaining number are the dial ports that are reallocated from the total number of dial ports in the Dial Ports dial pool.

For more detailed information about dial port allocation, refer to the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section in the *Cisco IPICS Server Administration Guide*.

Ops View Attributes

Cisco IPICS ops views support the following attributes:

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, refer to the *Cisco IPICS Server Administration Guide*.

- When a user logs in to a PMC or a Cisco Unified IP Phone, that user uses a PMC or Cisco Unified 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 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.

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 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 View Considerations

When using ops views, considering the following caveats:

- 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 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 windows.
- 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 VTG windows, 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.
- 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.

- As a general rule, VTGs inherit accessibility from the resource that it contains.

For detailed configuration information about Cisco IPICS ops views, refer to the *Cisco IPICS Server Administration Guide*.

Understanding Associations

In Cisco IPICS, you can assign attributes to users, that control their behavior. In some cases, attributes may have the same attribute behaviors, so when users are associated to channels or VTGs, the system determines the resulting PMC behaviors based on the configured attributes for each associated resource. For example, a user may be allowed to perform a particular function, such as the use of the PMC latch feature, but when the same user is associated to a channel that does not allow the latch feature, the user will not be allowed to latch on that channel as long as the user is a part of that association. After the user is no longer associated to that channel, then the attributes that were originally configured for the user will apply (the user will be allowed to latch on channels again).

Cisco IPICS allows values for attributes to be customized or overridden. When attributes of users or channels that are part of an association get modified, the resulting behavior depends on the attribute settings for those users within the association. When you attempt to override a customized value of an attribute in an association, Cisco IPICS prompts you with a message to inform you that the action will override the custom PMC setting for that specific attribute.

Note When you customize the values for attributes a superscript (1) displays next to the value in the appropriate attribute column in the Associations tab, for both the user and the channel. The superscript indicates a customized value.

For more detailed information about attribute association behaviors, refer to the *Cisco IPICS Server Administration Guide*.

Cisco IPICS Roles and Associated Tasks

Each person who uses Cisco IPICS is assigned one or more roles. Roles define the features that a user can access and the functions that the user can perform.

There are specific tasks that are associated with every Cisco IPICS role. Each Cisco IPICS user is assigned a role that determines the scope of user functionality and window accessibility.

The following sections provide brief descriptions of the tasks that are associated with each Cisco IPICS role:

- System Administrator Tasks, page 2-13
- Ops View Administrator Tasks, page 2-17
- Operator Tasks, page 2-18
- Dispatcher Tasks, page 2-18
- User Tasks, page 2-19

System Administrator Tasks

The Cisco IPICS system administrator performs the following tasks, as described in Table 2-1.

Table 2-1 System Administrator Tasks

Task	Description and Reference
Install Cisco IPICS	Before you can perform any system administrator tasks, you must first install and configure the Cisco IPICS server. To install and configure Cisco IPICS, refer to the *Cisco IPICS Server Installation and Upgrade Guide*.
Configure the Cisco IPICS server	
Configure and manage the RMS	You perform RMS management in the RMS window. Access this window from the Configuration drawer in the Administration Console. See the "Managing the RMS" section on page 3-1 for more information about the RMS. For more detailed information about configuring the RMS component, refer to "Configuring the RMS Component" appendix in the *Cisco IPICS Server Administration Guide*.
Manage locations	You add and delete locations in the Locations window. Access this window from the Configuration drawer. For more information about locations, see the "Understanding Locations" section on page 2-4. For detailed information, refer to the *Cisco IPICS Server Administration Guide*.
Set up multicast addresses	You set up multicast IP addresses in the Multicast Pool window. Access this window from the Configuration drawer. For detailed information, refer to the *Cisco IPICS Server Administration Guide*.
Configure PTT channels and channel groups	You perform channel and channel group management in the Channels and Channel Groups windows. Access these windows from the Configuration drawer. For detailed information about channel and channel group management, refer to the *Cisco IPICS Server Administration Guide*.

Table 2-1 System Administrator Tasks (continued)

Task	Description and Reference
Manage PMC versions	You upload PMC version packages to the server and configure the PMC installer, as well as manage PMC alert tones and skins from the PMC Management drawer. For more information about PMC management, see the "Managing the Cisco IPICS PMC" section on page 3-10. For more detailed information, refer to the *Cisco IPICS Server Administration Guide*.
Monitor system status	You monitor system status and diagnostic information, to use for troubleshooting and to monitor user activity, from the Serviceability drawer. For more information about monitoring system status, see the "Cisco IPICS Serviceability" section on page 4-1. For more detailed information, refer to the *Cisco IPICS Server Administration Guide*.
Review log files	You view log file activities that relate to VTGs, such as operational views (ops views) for each channel, user, and VTG, the creator of log entries, and the time that log activities occurred. You can also download archived log entries for historical reporting. Log activities can be performed from the Administration drawer. For more detailed information about log activities, refer to the *Cisco IPICS Server Administration Guide*.
Create and manage Cisco IPICS ops views	Ops views enable the use of resource sharing on one Cisco IPICS server. You perform ops view management in the Ops View window from the Configuration drawer. For more information about ops views, see the "Understanding Ops Views" section on page 2-7. For more detailed information about ops views, refer to the *Cisco IPICS Server Administration Guide*.

Table 2-1 System Administrator Tasks (continued)

Task	Description and Reference
Back up and restore the Cisco IPICS database	You can back up and restore the Cisco IPICS database, as well as download the backup and restore activity log files, in the Database Management window. Access this window from the Administration drawer. For more information, see the "Cisco IPICS Database Management" section on page 4-4. For detailed information, refer to the *Cisco IPICS Server Administration Guide*.
Set up Cisco Unified IP Phones	You configure Cisco Unified IP Phones for phone service in conjuction with the Cisco Unified CallManager or for Cisco Unified CallManager Express. For more information, see the "Using Cisco Unified IP Phones with Cisco IPICS" section on page 3-13. For detailed information, refer to the *Cisco IPICS Server Administration Guide*.

Table 2-1 System Administrator Tasks (continued)

Task	Description and Reference
Create and manage policies	You create and manage policies by using the policy engine. Policies comprise one or more actions, which are discrete functions that perform when the policy executes. You perform policy engine tasks by accessing the Policy Management drawer in the Policy Engine tab. For more information, see the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-3. For detailed information about the policy engine, refer to the *Cisco IPICS Server Administration Guide*.
Manage the dial engine	The Cisco IPICS dial engine enables the TUI and its associated features. You use the dial engine to manage system and custom scripts and prompts that the TUI uses to handle incoming and outgoing calls. You perform dial engine tasks by accessing the Dial Engine drawer in the Policy Engine tab. For more information about the dial engine, see the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-3. For detailed information, refer to the *Cisco IPICS Server Administration Guide*.

Ops View Administrator Tasks

The ops view administrator can download and monitor the Cisco IPICS activity logs for the ops view to which the user belongs. This user can also specify which activity types Cisco IPICS should log, per the ops view of the user.

The tasks that relate to activity logs are performed in the Activity Log Management and Activity Log Options windows. You can access these windows from the Administration drawer in the Administration Console.

Refer to the *Cisco IPICS Server Administration Guide* for more detailed information about the specific tasks that users can perform depending on their Cisco IPICS roles.

Operator Tasks

The operator performs the following tasks:

- Sets up users and user roles—The operator adds users and manages general user information, including user name, login credentials, and the default location of users. Operators can also manage the PMC attributes for users, assign channels, roles, and ops views, associate users with other users, phones, and policies, and perform activities that relate to managing user spoken name prompts.
- Sets up user groups—User groups are logical groupings of users. In addition to creating and deleting user groups, operators can add members to a user group, manage ops views for a user group, and view information about VTGs in which a user group is a participant.

Operator activities can be performed from the User Management drawer in the Administration Console. Users who are assigned the operator role can also access the dial engine windows.

For detailed information about the Cisco IPICS operator tasks, refer to the *Cisco IPICS Server Administration Guide.*

Dispatcher Tasks

The dispatcher performs the following tasks:

- Sets up and activates VTGs—The dispatcher creates VTG templates and activates them to begin conferences, add participants in VTG templates and active VTGs, monitor active VTGs, notify participants about active VTGs, and mute and unmute PMC users. VTG management tasks are performed in the VTG Management window in the Administration Console. See the "Understanding VTGs" section on page 2-6 for more information about VTGs.
- Manages policies—The dispatcher can view policies of users who belong to the same ops view as the dispatcher. Policy management can be performed by accessing the Policy Management windows in the Policy Engine tab. See the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-3 for more information about policies. For more detailed information, refer to the *Cisco IPICS Server Administration Guide*.

User Tasks

A user can perform the following tasks:

- Manages User Profile—Each Cisco IPICS user is assigned the user role. Users can manage personal information by using the My Profile window in Cisco IPICS. The user profile includes information such as user name, password, default location, communication preferences, and other personal information.
- Views Associations—Users view the channels, users, phones, VTGs, and policies with which they are associated in the My Associations window.
- Downloads the PMC—Users download the PMC installer to their client machines and install the most current version of the PMC, as configured in the server, in the Download PMC window.

Users can access the user windows from the Home drawer in the Administration Console. For more information about user tasks, refer to the *Cisco IPICS Server Administration Guide*.