Introducing Cisco IPICS

The Cisco IP Interoperability and Collaboration System (Cisco IPICS) provides voice interoperability among disparate systems. It offers an IP standards-based solution that interconnects voice channels, talk groups, and virtual talk groups (VTGs). It also provides powerful and flexible management of personnel and media resources.

This chapter provides an overview of Cisco IPICS. It also introduces the Cisco IPICS Administration Console, which gives you complete control over Cisco IPICS operation and administration. Read this chapter if you are setting up Cisco IPICS for the first time or if you want to learn about the basic components and concepts of Cisco IPICS.

Tip If you use Cisco IPICS only for communicating with other users and you do not require any introductory material, go to Chapter 4, "Performing Cisco IPICS User Tasks." That chapter describes how to log in to Cisco IPICS, download your Cisco IPICS Dispatch Console (IDC), set up push-to-talk (PTT) channels for the IDC and Cisco IP Phone, and complete your user profile.

This chapter includes the following sections:

Getting Started

After you install Cisco IPICS, you perform a series of procedures to set up and configure Cisco IPICS for use. The following table lists these procedures and provides references to more information about each one.

Use this information as a guide when you set up Cisco IPICS for the first time. Depending on your deployment, you may not need to perform each of these procedures.

	Procedure	Reference	Checkoff
	Become familiar with Cisco IPICS		
Step 1	Learn about the hardware and software components that are part of Cisco IPICS	See the "Cisco IPICS Overview" section on page 1-3	❏
Step 2	Learn about the roles that Cisco IPICS users can have	See the "Cisco IPICS Roles" section on page 1-6	❏
Step 3	Learn about the Cisco IPICS Administration Console, including how to access this application	See the "Cisco IPICS Administration Console" section on page 1-8	❏
	Set Up and Configure Cisco IPICS		
Step 1	Configure RMS components, if needed	See Appendix A, "Configuring the Cisco IPICS RMS Component"	❏
Step 2	Configure UMS components, if needed	See the "Managing the UMS" section on page 2-48	❏
Step 3	Configure the ISSI gateway, if needed	See the "ISSI Gateway Overview" section on page 9-3	❏
Step 4	Configure the DFSI gateway, if needed	See the "DFSI Gateway Overview" section on page 9-4	❏
Step 5	Configure locations	See the "Managing Locations" section on page 2-25	❏
Step 6	Configure the multicast pool	See the "Managing the Multicast Pool" section on page 2-31	❏
Step 7	Configure radios and radio descriptors	See Chapter 9, "Managing Radios and Radio Descriptors"	❏
Step 8	Create push-to-talk channels	See the "Managing PTT Channels and Channel Groups" section on page 2-2	❏
Step 9	Determine user roles and add users	See the "Managing Roles for a User" section on page 3-8	❏
Step 10	Create VTG templates	See the "Managing Inactive VTGs" section on page 5-4	❏
Step 11	Ensure that the server is hosting the current version of the IDC	See the "Managing IDC Versions" section on page 2-102	❏
Step 12	Configure the Cisco IPICS policy engine, if needed	See Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"	❏
Step 13	Create operational views, if needed	See Chapter 7, "Configuring and Managing Cisco IPICS Operational Views"	❏
Step 14	Set up Cisco Unified IP Phones, if needed	See Appendix C, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device"	❏
Step 15	Configure keystores and keys, if needed	See the "Managing P25 Keys" section on page 2-56	❏
Step 16	Configure high availability, if needed	See Chapter 10, "Configuring and Managing Cisco IPICS High Availability"	❏
Step 17	Generate SSL certificates, if needed	See Appendix D, "Generating SSL Certificates"	❏

Cisco IPICS Terminology

This document uses a variety of terms to describe Cisco IPICS features and functions. Table 1-1 describes some of the common terms that you may see throughout this document.

Table 1-1   Cisco IPICS Terms

Term	Description
Channel	Consists of a single unidirectional or bidirectional path for sending and receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency channel.
Talk Group	Comprises a subgroup of radio users who, under normal circumstances, only coordinate actions among users who are in the same talk group. Radio interface with other subgroups is not required. In Cisco IPICS, a channel maps to a logical talk group; that is, all the participants who talk on the same radio frequency belong to a talk group
Virtual Talk Group	Represents interoperability of a group of channels and maps to a voice channel that users attach to based on a specific incident. And end device (IDC, Cisco Unified IP Phone, dial-in phone) joins the VTG based on the location configuration that is configured in the server.
Group	When you use the Cisco IPICS policy engine telephony user interface (TUI), you may hear channels and VTGs referred to as groups.
Incident	An event that you identify in Cisco IPICS and for which various users can coordinate responses by using the IDC.

Cisco IPICS Overview

Cisco IPICS can be deployed in a variety of configurations. Your configuration depends on the types of communications devices that users employ, the media types that are used, your interoperability requirements, and so on. A Cisco IPICS deployment includes various hardware and software components to provide the functionality that you require, including some or all of the following:

- Cisco IPICS server—Provides the core functionality of the Cisco IPICS system. For more information, see the "Cisco IPICS Server" section on page 1-4.

- IPICS Dispatch Console (IDC)—Standalone PC-based software application that provides PTT functionality so that users with a variety of communication devices can participate in the event. For more information, see the "IPICS Dispatch Console" section on page 1-4.

- LMR gateways—Provides radio network interoperability and application integration. For more information, see the "LMR Gateways" section on page 1-5.

- RMS—Enables a Cisco Dispatch Console to remotely attach to a VTG or channel, enables channels to be joined in VTGs, and performs other mixing functions. For more information, see the "RMS" section on page 1-5.

- UMS—An alternative to the RMS. For more information, see the "UMS" section on page 1-5.

- Networking components—Include switches, routers, firewalls, mobile access routers, and wireless access points and bridges. For more information, see the "Networking Components" section on page 1-6.

- Cisco Unified Communications Manager functionality—Provide voice interoperability between radio and non-radio networks. For more information, see the "Cisco Unified Communications Manager Functionality" section on page 1-6.

- Audio clients—Devices such as land mobile radios (LMRs) and Cisco Unified IP Phones that let users participate in VTGs. For more information, see the "Audio Clients" section on page 1-6.

- Cisco Instant Connect—Standalone applications that run on Android devices or supported Cisco Unified Wireless IP Phone models. Cisco Instant Connect for Android devices allows you to use an Android device to participate in Cisco IPICS incidents, channels, VTG, and radios. The Cisco Instant Connect MIDlet lets you use a Cisco Unified Wireless IP Phone to communicate with other Cisco IPICS users via a point-to-point or standard telephone call, and communicate via channels, VTGs, and incidents by using your phone as a push-to-talk device. For more information, see *Cisco Instant Connect for Android Devices Reference Guide* or *Cisco Instant Connect MIDlet Reference Guide*.

Cisco IPICS Server

Every Cisco IPICS deployment includes a Cisco IPICS server, which is the center of all Cisco IPICS activity. The Cisco IPICS server software runs on the Cisco Linux operating system. It performs the following functions:

- Hosts the Administration Console, which gives you control over operation and administration of Cisco IPICS

- Hosts the Cisco IPICS policy engine

- Provides Cisco IPICS authentication and security services

- Stores data that is required for operation

- Enables integration with various media resources, such as RMS components, Cisco Dispatch Console, and Cisco Unified IP Phones

IPICS Dispatch Console

The IDC is a PC-based software application that enables end-users, dispatch personnel, and administrators with a variety of communication devices can participate in and event. The IDC integrates with virtually any analog or digital radio system to provide dynamic PTT communications. It also provides rich media IPICS incident support, enabling the sharing of multimedia data such as video, photographs, and data.

You install the IDC on your PC after downloading the software from the Cisco IPICS server. For more information, see the "Downloading the IDC" section on page 4-17. After you install the application for the first time, Cisco IPICS automatically alerts you when new versions become available.

The Cisco IPICS operator sets up user access to the IDC. The operator also assigns specific PTT channels that IDC users can monitor and use to participate in conferences with other Cisco IPICS users.

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

LMR Gateways

LMR gateways provide radio network interoperability by using the Cisco IOS Hoot 'n' Holler feature. They provide a bridge between radio frequencies and IP multicast streams. They also provide keying signals to key radio transmissions. The LMR gateway functionality is often installed as an additional feature in a router.

RMS

A router media service (RMS) provides a variety of functions for Cisco IPICS, including the following:

- Support through its loopback functionality for combining two or more VTGs
- Mixing of multicast channels to support VTGs
- Mixing of remote IDC unicast connections to a multicast channel or a VTG
- Support for unicast M1:U12:M2 connection trunks

Table 1-2 lists which IPICS features are supported by RMS, UMS, or both.

Table 1-2   RMS and UMS Feature Support

Feature	RMS	UMS
IPICS Channel	Yes	Yes
IPICS VTG	Yes	Yes
IPICS Radio	Yes	Yes
SIP	Yes	Yes
Multicast	Yes	Yes
G.711	Yes	Yes
G.729	Yes	Yes
Talker ID	Partial (multicast only)	Yes
Direct Dial	Yes	No
LMRG	Yes	No
CUCM	Yes (CME)	No
MUM Trunks	Yes	No
ILBC	Yes	No

UMS

A unified media service (UMS) performs functions similar to those performed by the RMS. Controlled by the Cisco IPICS server, a UMS provides for:

- Mixing audio from multicast and SIP streams and broadcasting the mixed audio to other multicast and SIP streams
- Talker ID between multicast and SIP endpoints
- Radio control from SIP endpoints

- Improved multicast voice quality

- Creation of VTGs that are composed of diverse end points

- Bridges multicast and unicast users

- Proxy mixing for resource-constrained end points

- G.711 and G.729 transcoding services so that local IDCs, remote IDCs, and IP phones can participate in the same VTG

See Table 1-2 for a list of IPICS features that are supported or not supported by UMS.

Networking Components

Networking components include switches, routers, firewalls, mobile access routers, and wireless access points and bridges.

Cisco Unified Communications Manager Functionality

Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS enable selected Cisco Unified IP Phone models to participate in channels and VTGs. These applications also serve as the SIP provider for the Cisco IPICS policy engine. The SIP provider provides SIP telephony support for calls to and from the dial engine.

Audio Clients

Audio clients are devices through which users communicate with Cisco IPICS. They include IDC clients, LMR gateways, various models of the Cisco Unified IP Phone, mobile clients, and Cisco Instant Connect.

Cisco IPICS Roles

Every Cisco IPICS user is assigned one or more roles. Roles define the Cisco IPICS features that a user can access and the functions that a user can perform. In this way, roles help to provide system security.

Table 1-3 describes the Cisco IPICS roles.

Table 1-3   ***Cisco IPICS Roles***

Role	Description	Reference
User	Has the ability to maintain personal information, download the IDC client application, specify communication preferences that are used to configure audio devices, activate a policy, and view associated policies. Each Cisco IPICS user is assigned the user role. The user may have additional roles.	See Chapter 4, "Performing Cisco IPICS User Tasks."
System administrator	Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. Also creates, edits, or deletes ops views, manages Cisco IPICS licenses and IDC versions, performs activities relating to the dial engine, activates policies, views certain policies, and monitors the status of the system and its users via the activity log files and the Dashboard.	See Chapter 2, "Performing Cisco IPICS System Administrator Tasks."
Ops view administrator	Has the ability to manage and monitor the activity logs that are filtered by ops views and accessible in the Administration Console (Administration > Activity Log Management) window.	See Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Operator	Responsible for setting up and managing users and user groups, granting access to Cisco IPICS and the IDC, assigning user channels, roles and ops views, and creating and managing policies.	See Chapter 3, "Performing Cisco IPICS Operator Tasks."
Dispatcher	Responsible for setting up inactive VTG, activating VTGs to begin conferences, and adding or removing participants in VTG templates and active VTGs. Creates and manages policies. Also monitors active VTGs and events and can mute and unmute users, as necessary.	See Chapter 5, "Performing Cisco IPICS Dispatcher Tasks."
All	Equivalent to being assigned each of the other Cisco IPICS roles.	—

Linux User Roles

Cisco IPICS supports the Linux user roles that Table 1-4 describes.

Table 1-4   Linux User Roles

System User Roles and System Groups	Description
root user	The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.
ipicsadmin user	The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.
ipicsdba user	The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires. To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - ipicsdba** (substitute user from root).
informix user	The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires. To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - informix** (substitute user from root).

Cisco IPICS Administration Console

The Cisco IPICS server includes the Administration Console, which is a web-based application. You use the Administration Console to perform and manage Cisco IPICS activities, depending on your Cisco IPICS role.

This section includes the following topics:

Cisco IPICS Server Usage Guidelines

Be aware of the following tips and guidelines when you use the Cisco IPICS server:

- The Cisco IPICS Administration Console contains the following tabs:
  - Server tab—Provides access to drawers and windows in which you perform Cisco IPICS administration and management activities. These activities include configuring and managing Cisco IPICS components, uploading licenses, managing the database, monitoring activity logs, setting system performance options, and monitoring system performance. You can also perform VTG, user, and IDC management operations.
  - Policy Engine tab—Provides access to drawers and windows in which you perform policy engine and dial engine administration and management activities. These activities include creating and managing policies, configuring SIP and dial engine parameters, managing prompts, and monitoring policy engine services, and managing tracing for the dial engine.

- Many of the Administration Console windows let you enter a variety of information. You might enter information by typing in fields, choosing from drop-down lists, or checking check boxes, depending on the window. An asterisk (*) next to a field, drop-down list, or check box indicates required information. You must provide this information before you can save your changes and exit the window.

- Most windows contain a **Save** button and a **Cancel** button. The **Save** button saves any changes that you make in a window and often closes the window. The **Cancel** button discards any changes that you have made and often closes the window.

- Many Cisco IPICS resources, such as channels, users, and VTGs, display in lists in the Administration Console. These lists include check boxes that you can check to select resources for which to perform certain functions. Most resource lists include a check box at the top of the list that allows you to select all resources at one time.

- Many of the Administration Console windows include drop-down lists. Some of these lists become available only after you perform certain functions. If you do not perform the required function, the drop-down list is dimmed to indicate that it is not available.

- For some resources, separate windows display in which you can take the following actions:
  - To move an item from one list to another list, click the item to highlight it and then click **>** or **<**, or double-click the item.
  - To move several items from one list to another list at one time, Shift+click or Ctrl+click to select the items and then click **>** or **<**.
  - To move all items from one list to another list at one time, click **>>** or **<<**.

- Cisco IPICS provides connection support for both multicast and unicast communications. Make sure that users are aware of the appropriate location information to use when they log in to Cisco IPICS.

- When configuring IP multicast addresses, Cisco strongly recommends that you configure IP multicast addresses that are only in the 239.192.0.0 to 239.251.255.255 range. This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in

a local domain. This address range is less likely to cause an addressing conflict in an existing multicast domain. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-34.

- When adding users, channels, user groups, channel groups, or VTGs, be aware that names within each category must be unique. For example, no two user names can be the same, and no two channel names can be the same, but a user name and a channel name can be the same.

- Users who are in the same multicast domain are also in the same Cisco IPICS location.

- To ensure that each Cisco IPICS server has use of resources on a dedicated RMS component, Cisco IPICS does not support the use of the same RMS component with use multiple Cisco IPICS servers. (In a high availability deployment, the primary and secondary Cisco IPICS server use the same RMS component because only one server is active at a time.)

- Cisco IPICS supports more than one RMS component or UMS component in the same location.

- When you configure an RMS component, make sure that you perform all of the configuration procedures that are described in Appendix A, "Configuring the Cisco IPICS RMS Component."

- If a VTG becomes active or inactive unexpectedly, a policy may have activated or deactivated the VTG. For more information about policies, see Chapter 6, "Using the Cisco IPICS Policy Engine."

- All all time stamps that appear in the Cisco IPICS server Administration Console web interface in Greenwich Mean Time (GMT).

Browser Guidelines

When you access the Cisco IPICS Administration Console by using a supported browser, follow the guidelines that this section describes.

Note By default, the Administration Console times out after a period of no use. For more information, see the "Administration Console Timeout" section on page 1-14.

- Windows in the Administration Console do not refresh automatically. As a best practice, update your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update in a window that does not display the most current data, the update may not succeed and Cisco IPICS displays an error. If this situation occurs, update your browser window and retry the operation.

- To ensure that a current window displays the most up-to-date information, refresh it by clicking the button or tab that you used to display it. Some windows in the Administration Console provide a **Refresh** button, which you can use to refresh the window. or click Refresh on the. Cisco IPICS does not support the use of the browser **Refresh** button to refresh a window in the Administration Console.

- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.

- Cisco IPICS does not support accessing the Administration Console in more than one browser session at the same time on the same machine. If you use multiple browser sessions to access the Administration Console, you may experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.

- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.

Accessing the Administration Console

After you install Cisco IPICS, you can access the Administration Console from any computer that has IP connectivity to the Cisco IPICS server and meets the requirements that *Cisco IPICS Compatibility Matrix* specifies.

To access the Cisco IPICS Administration Console, perform the following procedure:

Procedure

Step 1   Start Internet Explorer, and in the Address field, enter the fully qualified hostname (for example, ipics1.cisco.com) or the IP address of the server on which Cisco IPICS is running.

A fully qualified hostname is preferred. If you enter an IP address and the PC that you are using does not have a valid trust certificate from the server, a pop-up window prompts you to download a certificate. Follow the prompts to do so.

The Authentication window displays.

Step 2   In the Authentication window, enter your user name and password in the User Name and Password fields.

Passwords are case-sensitive, so make sure to enter a password exactly as it is configured.

User names and server hostnames are not case-sensitive.

Step 3   Click **Log In**.

The Cisco IPICS Administration Console displays. The My Profile window appears on the right. The left pane in this example shows all of the available drawers in the Administration Console. The drawers that appear for you correspond to your roles, so you may not see all drawers in your window. The Policy Engine tab appears only if you have licensed the Cisco IPICS policy engine.

You can perform a variety of activities in the User Details window. Table 1-5 describes these activities.

Table 1-5   User Details Window Activities

Activity	Reference
Update your user information	See the "Managing Your User Profile" section on page 4-2
Choose a tab and drawer to access additional windows	See the appropriate chapter: • Chapter 2, "Performing Cisco IPICS System Administrator Tasks" • Chapter 3, "Performing Cisco IPICS Operator Tasks" • Chapter 5, "Performing Cisco IPICS Dispatcher Tasks" • Chapter 4, "Performing Cisco IPICS User Tasks" • Chapter 6, "Using the Cisco IPICS Policy Engine" • Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"
Obtain online help	See the "Getting Help in the Administration Console" section on page 1-14
Obtain information about Cisco IPICS	See the "Viewing Information about Cisco IPICS" section on page 1-14
Log out and exit from the Administration Console	See the "Exiting the Administration Console" section on page 1-12

Exiting the Administration Console

You can exit the Administration Console from any window within the application. To do so, click **Logout** in any Administration Console window.

Entering Required Information in Administration Console Windows

Many of the Administration Console windows let you enter a variety of information. You might enter information by typing in fields, choosing from drop-down lists, or checking check boxes, depending on the window.

An asterisk (*) next to a field, drop-down list, or check box indicates required information. You must provide this information before you can save your changes and exit the window.

Using Search Windows

Several activities that you perform in the Administration Console require you to locate or to identify items that the activities affect. For example, when you associate channels with a user, you must identify the channels that you want to associate.

To let you locate the items that you need, Cisco IPICS provides a Search or a Search Results window. This window pops-up automatically when needed. It provides one or more fields that let you search for the item or items that you want based on a variety of criteria.

The following guidelines apply to Search or Search Results windows:

- These windows may contain one of more filter fields in which you can type characters. The names of these fields depend on the activity that you are performing and the information that you need to find.

  In a filter field, you can enter a character string that includes the first few characters of the name that you want to find. Characters are not case-sensitive.

- The windows may contain one or more filter drop-down lists. These lists depend on the activity that you are performing and the information that you need to find.

  From a filter drop-down list, you can choose the option that matches the item that you want to find. For example, if you are searching for a user and choose **Dispatcher** from a Roles drop-down list, Cisco IPICS will find users who are assigned the Dispatcher role.

- If you enter information in more than one filter field, Cisco IPICS finds only items that match all search criteria that you specify.

- To perform a search based on filters that you specify, click **Go** in the Filter area of a Search or a Search Results window. If you click **Go** without specifying any filters, Cisco IPICS locates all items of the type that you are searching for.

- To clear fields and reset drop-down lists to their default values, click **Clear Filter** in the Filter area of a Search or a Search Results window.

- The results of a search, except a search for locations, depend on the ops view to which you belong. Search for results for locations include all locations that match the search criteria, regardless of your ops view.

- Some search results depend on items that you can choose from the results list. For example, if you search for channels to associate with a user, the results do not include channels that disallow associations to users. Similarly, if you search for channels to add to a VTG, the results do not include channels that disallow associations to VTGs.

- To view the results in a results list at the bottom of a Search or a Search Results window, see the .

- To choose one or more items that display in the results list in a Search or a Search Results window, check the check box next to each item.

- To exit a Search or a Search Results window, take one of these actions:

  – Click the **OK** button—The window closes and then results that you checked are entered in the window that you return to.

  – Click the **Cancel** button—The window closes and the results that you checked are not in the window that you return to.

Navigating Item Lists

Several windows in the Administration Console may display lists of information. For example, the Users window in the User Management drawer displays a list of Cisco IPICS users.

To view items in these lists, follow these guidelines:

- Lists are divided into *pages* of information. To specify how many rows of items are included in a page, choose the desired value from the Rows per page drop-down list at the top of the window, and then click the **Go** button next that list. You may need to use the scroll bar next to the result list to see all items in a page.

- You can navigate pages of information in a list by using the following navigation controls at the bottom of the list:

  – Page field—To go to a specific page, enter the page number and press **Enter**.

  – |< (First Page button)—Displays the first page in the list. This button is not available when the first page is displayed.

  – < (Previous Page button)—Displays the previous page in the list. This button is not available when the first page is displayed.

  – > (Next Page button)—Displays the next page in the list. This button is not available when the last page is displayed.

  – >| (Last Page button)—Displays the last page in the list. This button is not available when the last page is displayed.

Getting Help in the Administration Console

You can access the Cisco IPICS help system from any window in the Administration Console. The help system provides online access to the information that is in this *Cisco IPICS Server Administration Guide*.

To access Cisco IPICS online help, click **Help** in any Administration Console window.

Viewing Information about Cisco IPICS

To view the following information about Cisco IPICS, click **About** in any Administration Console window:

- Cisco IPICS version that is running

- Ops view to which the logged-in user belongs

- Ops view to which the logged-in user is accessible

- Current server date and time

- Server operating system (this information appears only if you are assigned the Cisco IPICS system administrator role)

- Date and time of the most recent database backup (this information appears only if you are assigned the Cisco IPICS system administrator role)

Administration Console Timeout

For increased system security, the Administration Console times out after 30 minutes of no use. In this situation, the current Administration Console window remains displayed, but Cisco IPICS prompts you to log back in when you attempt to perform a function. To log back in, enter your user name and password, and then click **Log In**. To exit the Administration Console, click **Logout** in any Administration Console window.

To change the timeout period of your Cisco IPICS session or to disable it so that there is no timeout period, navigate to **Administration > Options** in the Administration Console and modify the value of the Cisco IPICS Session Timeout Period option. See the "Managing Cisco IPICS Options" section on page 2-90 for more information.

Cisco IPICS Splash Screen

The Cisco IPICS splash screen is an optional pop-up message that can appear during the login process. It can consist of text, an image, or text and an image. The IPICS server controls the splash screen content and sends it to the client during initial handshake.

When configured, the splash screen is displayed in the following clients:

- IDC
- IPICS Administration Console
- Shell / CLI / SSH

Table 1-6 provides examples of how the splash screen can appear in the different clients:

Table 1-6   *Customized Splash Screen Examples*

Client	Default

SSH	`Using username "root".`
	`Welcome to Cisco IPICS 4.5(1)`
	
	`                          WARNING!!!`
	`              READ THIS BEFORE ATTEMPTING TO LOGON`
	
	`   This System is for the use of authorized users only.  Individuals using`
	`   this computer without authority, or in excess of their authority, are`
	`   subject to having all of their activities on this system monitored and`
	`   recorded by system personnel.  In the course of monitoring individuals`
	`   improperly using this system, or in the course of system maintenance,`
	`   the activities of authorized users may also be monitored. Anyone using`
	`   this system expressly consents to such monitoring and is advised that if`
	`   such monitoring reveals possible criminal activity, system personnel may`
	`   provide the evidence of such monitoring to law enforcement officials.`
	
	`root@ipics-example's password:`

Table 1-6   *Customized Splash Screen Examples (continued)*

Client	Default
Administration Console	
IDC	
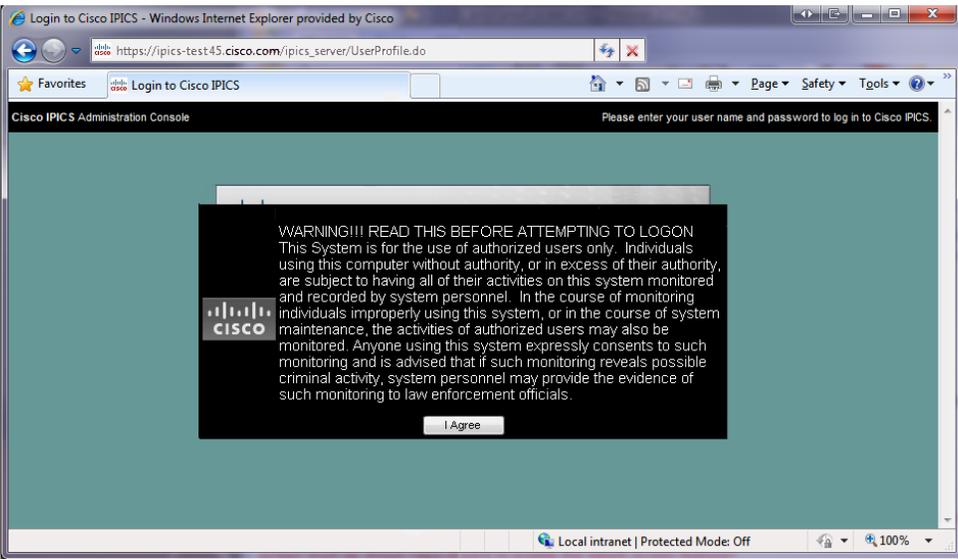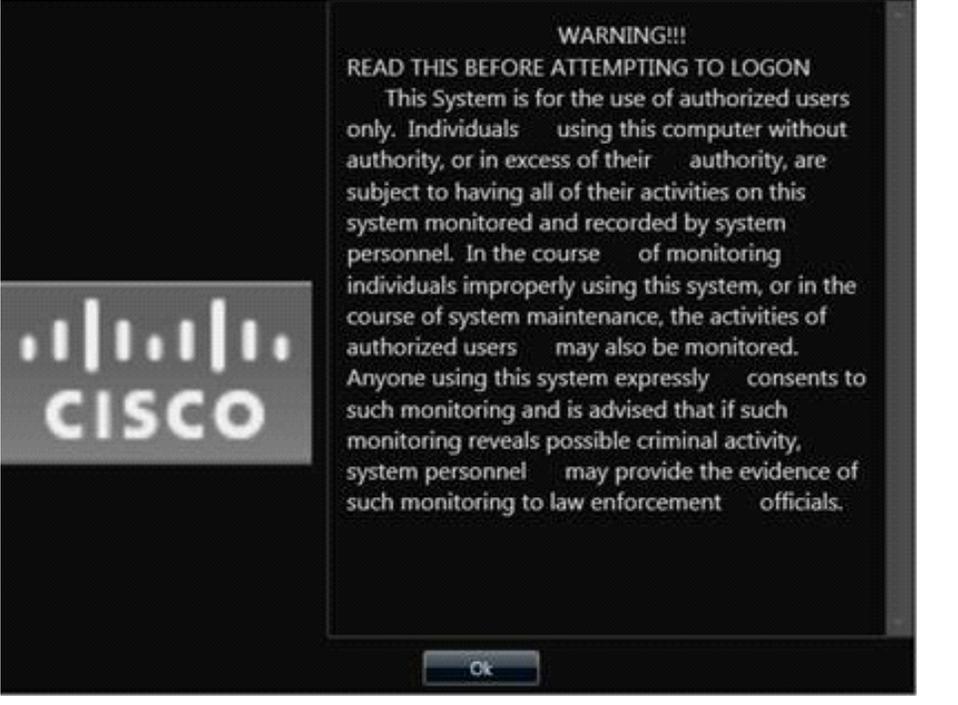
Splash Screen Installation Files

The splash screen feature is not configured from any GUI. Instead, the system administrator invokes a shell script called splash-install to configure it. Table 1-7 describes the files in the /opt/cisco/splash directory that are used to install and configure the splash screen.

Table 1-7   Contents of /opt/cisco/splash Directory

File	Purpose		
splash-install	The splash installer		
splash-reverse	The splash uninstaller		
splash-reverse.sql	(Internal file. Do not edit.)		
splash.png	The default splash image is a Cisco logo. Feel free to customize this file. It will get copied to the appropriate place on the IPICS server when the splash-install scripts runs. Keep the filename "splash.png". If you rename it, or need to use a jpg instead, then you will need to also modify "splash_screen_url" found in the splash.sql file, and re-run splash-install. Suggested image dimensions: 300 x 300		
splash.sql	(Internal file. Editing should not be necessary.)		
	Config_name	**Config_value**	**Description**
	splash_screen_message	(splash-install will insert the content of splash.txt here)	Optional customizable splash screen text. If present, IDC and browser will display the splash screen upon startup.
	splash_screen_url	/ipics_server/images/splash.png	Optional customizable splash screen image. If present, IDC and browser will display the splash screen upon startup. A relative URL is recommended (not beginning with http://hostname). If you use an absolute URL, it must be accessible by the IPICS server (e.g. if server is behind a firewall, images on external Internet sites won't work, so you may need to copy the image to the IPICS server.)
	splash_screen_timeout	0	Unused

splash.txt	The customizable splash screen text. The default value is as follows:
	
	``
	                          WARNING!!!
	             READ THIS BEFORE ATTEMPTING TO LOGON
	
	This System is for the use of authorized users only. Individuals using this computer
	without authority, or in excess of their authority, are subject to having all of their
	activities on this system monitored and recorded by system personnel. In the course of
	monitoring individuals improperly using this system, or in the course of system
	maintenance, the activities of authorized users may also be monitored. Anyone using this
	system expressly consents to such monitoring and is advised that if such monitoring
	reveals possible criminal activity, system personnel may provide the evidence of such
	monitoring to law enforcement officials.
	``		

Installing and Configuring the Splash Screen

To install and configure the IPICS splash screen, perform the following procedure:

Procedure

Step 1   Use a secure shell (SSH) client to log in to the primary Cisco IPICS server using the root account and the IP address of the IPICS server.

ssh root@*ipics-server-ip-addr*

Step 2   Change the working directory to /opt/cisco/splash.

cd /opt/cisco/splash

Step 3   Customize as needed:

   a.   Modify splash.txt as needed.

   b.   Replace splash.png with desired image.

   •   Keep the filename as splash.png.

   •   The suggested image dimensions are 300 x 300

Step 4   Run the splash-install file to install the splash screen configuration.

run ./splash-install

Note: While installing the splash screen, you may encounter the following errors that can be safely ignored:

   •   268: Unique constraint (ipicsdba.config_pk) violated.

   •   100: ISAM error: duplicate value for a record with unique key.

Step 5   Either wait 10 minutes for the server to refresh the cached splash screen configuration, or restart the IPICS service.

Step 6   Test by logging into the following clients:

   a.   IPICS Administration Console

   b.   IDC

   c.   SSH

Step 7   If you are not satisfied with the results:

   a.   Run the splash-reverse file to uninstall the splash screen configuration.

   run ./splash-reverse

   b.   Repeat Step 3 through Step 6 until you are satisfied with results.

Step 8   If high availability (HA) is configured, you must repeat Step 1 through Step 4 on the secondary IPICS server.

> **Note**
> - Other endpoints, such as an iPhone, or IP Phone services, do not see the splash screen.
> - You can only install one language at a time. The settings are global for the whole IPICS server.
> - Tectia SSH Client may suppress the SSH splash screen. We recommend that you use PuTTY SSH or similar software instead.

Uninstalling the Splash Screen

To uninstall the IPICS splash screen, perform the following procedure:

Procedure

Step 1   Use a secure shell (SSH) client to log in to the primary Cisco IPICS server using the root account.

ssh root@<ipics-server-address>

Step 2   Change the working directory to /opt/cisco/splash.

cd /opt/cisco/splash

Step 3   Run the splash-reverse file to uninstall the splash screen configuration.

run ./splash-reverse

Step 4   Either wait 10 minutes for the server to remove the splash screen configuration from cache, or restart the IPICS service.