Release Notes for Cisco IPICS Release 2.0(1)

March 9, 2007

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (hereafter referred to as Cisco IPICS) and the Push-to-Talk Management Center (hereafter referred to as PMC) release 2.0(1).

Note To view all of the release notes for Cisco IPICS, go to:
http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Before you install Cisco IPICS, Cisco recommends that you review the "Important Notes" section on page 79 for information about issues that may affect your system.

For a list of the open and resolved caveats for Cisco IPICS release 2.0(1), see the "Resolved Caveats for Cisco IPICS - Release 2.0(1)" section on page 99 and the "Open Caveats for Cisco IPICS - Release 2.0(1)" section on page 103. Updates for these release notes occur with every maintenance release and major release.

To access the documentation suite for interoperability systems products, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/index.htm

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

You can access some of the Cisco IPICS software upgrades on Cisco Connection Online (CCO) at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/ipics

Contents

These release notes contain the following topics:

Introduction

This section provides an introduction to the Cisco IPICS product. It includes the following topics:

Overview

Cisco IPICS provides a high-quality IP standards-based solution that enables voice interoperability among disparate systems. The Cisco IPICS solution interconnects voice channels, talk groups, and virtual talk groups (VTGs) to bridge communications from radio networks to IP networks and devices, such as the Cisco IPICS Push-to-Talk Management Center (PMC) PC application, and supported models of Cisco Unified IP Phones.

To provide this functionality, Cisco IPICS uses new components, such as the Cisco IPICS server and the PMC, and existing technologies, such as Land Mobile Radio (LMR), Cisco gateways, and Voice over IP (VoIP) technology, along with new applications of existing technologies, such as the use of the router media services (RMS) functionality for channel mixing.

As part of the Cisco IPICS solution, the server includes the Administration Console, which is an integrated web-based system management software that provides the incident management framework graphical user interface (GUI). The Administration Console facilitates the tasks that are associated with operations and command and control to extend the reach of push-to-talk (PTT) voice technology from the LMR environment to the IP network and enable rapid deployment and management of disparate audio communications systems.

In addition, the server includes the Cisco IPICS policy engine (hereafter referred to as *policy engine*), which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

The PMC application provides the interface for users to host push-to-talk audio communications. By using a simplified GUI, the PMC allows simultaneous monitoring and participation in one or more talk groups or VTGs at the same time.

Because the Cisco IPICS server controls the configuration of the PMC application, PMC users have limited access to the configuration parameters; however, Cisco IPICS includes the ability for PMC users to configure the PMC GUI skins for mouse-based or touch screen-based display.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

Cisco IPICS Components

The Cisco IPICS solution comprises the following major components, as described in Table 1:

Table 1 Cisco IPICS System Components

Component	Description
Cisco IPICS Server	This component provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Cisco Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. (Refer to the *Cisco IPICS Compatibility Matrix* for information about the servers that Cisco IPICS supports.) The Cisco IPICS server software includes the Cisco IPICS Administration Console, which is an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. (In Cisco IPICS, VTGs combine one or more channels and/or users.) By using this GUI, authorized Cisco IPICS users can manage the system configuration and authentication and security services, policies and privileges, and database information. The server also enables control of the configuration of the media resources that are installed in the router and which are used for audio mixing capabilities. In addition, the server includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications. Cisco IPICS supports several different user roles. For more information, see the "User Roles" section on page 6. Cisco IPICS supports several different system user roles and groups. For more information, see the "System User Roles and Groups" section on page 8.

Table 1 Cisco IPICS System Components (Continued)

Component	Description
Push-to-Talk Management Center (PMC)	The PMC is a PC-based software application that comprises a stand-alone PTT audio application that connects end-users, dispatch personnel, and administrators via an IP network. By using a simplified GUI, the PMC allows simultaneous monitoring and participation in one or more talk groups or VTGs at the same time. (VTGs are the voice channels that users connect to based on specific incidents.) PMC users may change the appearance of the PMC user interface by choosing another Cisco-provided or custom skin. The PMC runs on the Microsoft Windows 2000 and Windows XP operating system. For more information about hardware and software requirements, see the "System Requirements" section on page 11.
Gateways	This component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams. Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

Table 1 Cisco IPICS System Components (Continued)

Component	Description
Router Media Service	The Router Media Service (RMS) component enables the PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality. The RMS provides support for mixing multicast channels in support of VTGs and for mixing remote PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway. For a list of Cisco IOS versions that Cisco IPICS supports for use as an RMS, refer to the *Cisco IPICS Compatibility Matrix*. (Each supported Cisco IOS version includes the Cisco Hoot ‘n’ Holler feature.)
Networking Components	The Cisco IPICS solution may include some or all of the following network components, depending on the functionality that you require: routers, switches, firewalls, mobile access routers, wireless access points, and bridges.
Cisco Unified CallManager and VoIP Services	Cisco IPICS provides support for SIP-based interoperability with supported versions of Cisco Unified CallManager and Cisco IOS, with optional Cisco Unified CallManager Express, and VoIP services, such as the Cisco Unified IP Phone services, to help extend the reach of PTT technology to the IP network. These services allow participation in channels and/or VTGs through the use of supported models of Cisco Unified IP Phones by enabling these phones to work with Cisco IPICS as IP phone multicast client devices.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

User Roles

The Cisco IPICS solution authorizes access to different features based on the role that is assigned to each user. Cisco IPICS users may have one or more roles, including system administrator, operator, dispatcher, and user.

Table 2 describes the user roles that Cisco IPICS supports.

Table 2 Cisco IPICS User Roles

User Role	Description
System Administrator	The system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and PMC versions, and monitors the status of the system and its users via the activity log files. The system administrator has the ability to administer all resources in the Cisco IPICS system. For more information, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1)* and the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*.
Ops View Administrator	The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (**Administration** > **Activity Log Management**) window. For more information, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1).*
Operator	The operator is responsible for setting up and managing users and policies, configuring access privileges, and assigning user roles, and ops views. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges. For more information, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Table 2 Cisco IPICS User Roles (Continued)

User Role	Description
Dispatcher	The dispatcher is responsible for setting up the VTG templates, activating the VTGs to begin conferences, and adding and/or removing participants in VTG templates and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges. For more information, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
User	The Cisco IPICS user may set up personal login information, download the PMC application, configure the PMC skin, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the policy engine. For more information, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1)* and the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

System User Roles and Groups

This release of Cisco IPICS supports the system user roles and system groups, as described in Table 3.

Table 3 Cisco IPICS System User Roles and System Groups

System User Roles and System Groups	Description
ipics linux group	Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.
informix linux group	Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.
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.
ipics user	The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.
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.

Table 3 Cisco IPICS System User Roles and System Groups (Continued)

System User Roles and System Groups	Description
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).

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

Cisco IPICS Support Team Communications

The Cisco IPICS Support Team provides an external mailing list that you can use to obtain additional support directly from the Cisco IPICS engineering team. To subscribe to this mailing list, create an email that includes "subscribe" in the subject line; then, send the email to the following address:

ask-ipics-support@external.cisco.com

Whenever you need additional support, or if you have questions about Cisco IPICS, send your request to ask-ipics-support@external.cisco.com.

A Cisco IPICS engineer will respond to your email to provide you with the assistance that you need.

System Requirements

This section contains information about systems requirements for the Cisco IPICS server and PMC components; it includes the following sections:

- Server Requirements, page 11
- PMC Requirements, page 12

Server Requirements

The Cisco IPICS server requires the following minimum versions of hardware and software:

Hardware

For a list of supported hardware platforms, including Cisco Media Convergence Servers (MCS), Cisco IPICS-Mobile Platforms, and Cisco routers that you can use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Note Make sure that you install and configure Cisco IPICS release 2.0(1) only on a supported Cisco platform.

Software

For a list of the software that is supported for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Note You must use only the Cisco-supported operating system for use with Cisco IPICS. No other operating system versions are supported.

Where to Find More Information

- *Cisco IPICS Compatibility Matrix*

PMC Requirements

The following sections detail the minimum hardware and software requirements that Cisco IPICS supports for use with the PMC:

- PMC Hardware, page 12
- PMC Software, page 13

PMC Hardware

Table 4 shows the PMC minimum hardware requirements that Cisco IPICS supports. These requirements are dependent on the number of active PMC channels that you use.

Table 4 PMC Minimum Hardware Requirements

Number of PMC Channels	PMC Hardware Requirements
Supports up to 4 active channels	• 800 MHz Pentium III class, including Mobile Pentium • 512 MB RAM • 1 GB free space • Network interface card

Table 4 PMC Minimum Hardware Requirements (Continued)

Number of PMC Channels	PMC Hardware Requirements
Supports up to 6 active channels	• 1.5 GHz Pentium IV class, including Mobile Pentium • 512 MB RAM • 1 GB free space • Network interface card
Supports up to 18 active channels	• 3.2 GHz Pentium IV class, including Mobile Pentium • 2 GB RAM • 1 GB free space • Network interface card

Note The Cisco IPICS system allows you to turn on or turn off logging for individual PMC log files and set the debug log levels. To use the logging functionality, Cisco IPICS requires sufficient free disk space on the PMC client machine; that is, when the PMC detects that only 100 MB of disk space is available on the PMC client machine, it displays a warning message to alert you, and when the PMC detects only 50 MB of free disk space, it stops logging data to the log files.

Caution Because of the large amount of information that the system collects and generates when you set all of the debug options, Cisco recommends that you use debug logging only to isolate specific problems. When your debugging tasks have been completed, be sure to turn off debug logging by clearing the debug log. For more information, refer to the “Using the PMC Application Logs” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

PMC Software

Cisco IPICS supports the following operating system software for use with the PMC:

- Windows 2000 Professional SP4

- Windows XP Professional SP2

Note Make sure that you install the PMC application on a PC that has the required Windows operating system installed.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*
- *Cisco IPICS Compatibility Matrix*

Determining the Software Version

The current version of the Cisco IPICS server software displays in the upper left corner of the Administration Console. You can also locate the server version information by clicking the **About** link that is located in the upper right corner of the Administration Console.

To see the version information for the PMC application, click the **Menu** button or right-click in the PMC interface to see a list of options; then, click **About**. The version information for your PMC application displays. Alternatively, you can access the **Settings** > **Status** menu to see version information for the PMC.

Compatibility Matrix

You can find the list of the hardware and software versions that are compatible with this release of Cisco IPICS by referring to the *Cisco IPICS Compatibility Matrix* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Note Make sure that you check the *Cisco IPICS Compatibility Matrix* for the most current versions of compatible hardware components and software versions for use with Cisco IPICS.

Related Documentation

For more information about this release of Cisco IPICS, refer to the following documentation:

- *Cisco IPICS PMC Quick Start Reference Card, Release 2.0(1)*—This document provides tips and quick references for the most frequently used procedures that a user can perform on the Cisco IPICS PMC.
- *Cisco IPICS PMC Debug Reference Quick Start Card, Release 2.0(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPICS Server Quick Start Guide, Release 2.0(1)*—This document is a condensed version of the *Cisco IPICS Server Administration Guide* to help the administrator to quickly get started with Cisco IPICS.
- *Cisco IPICS Server Quick Start Reference Card, Release 2.0(1)*—This document provides tips, quick references, and usage guidelines for the Cisco IPICS server.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*—This document describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system.
- *Cisco IPICS Server Quick Start Installation Reference Card, Release 2.0(1)*—This document provides tips and quick references for installing and upgrading the Cisco IPICS server.
- *Cisco IPICS Troubleshooting Guide, Release 2.0(1)*—This document contains reference material about how to maintain and troubleshoot the Cisco IPICS system.
- *Cisco IPICS PMC Command Line Interface, Release 2.0(1)*—This document describes the commands that you can use from the command line interface (CLI) to obtain information or to change settings for the Cisco IPICS PMC.
- *Release Notes for Cisco IPICS Release 2.0(1)*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.

- *Cisco IPICS 2.0(1) Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.
- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*— This document provides information about design considerations and guidelines for deploying the Cisco IPICS solution.
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.

To access the documentation suite for Cisco IPICS, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

New and Changed Information

The following sections describe the new features that are available and pertinent to this release of Cisco IPICS. These sections may include configuration tips for the administrator, information about users, and where to find more information.

- Server Installation Guidelines, page 17
- Server Upgrade Guidelines, page 20
- Backup and Restore Guidelines, page 21
- PMC Installation and Upgrade Guidelines, page 23
- Cisco IPICS Security Enhancements, page 25
- Introducing the Cisco IPICS Policy Engine, page 32
- Cisco IPICS Server Enhancements, page 34
- Support for High Latency Low Bandwidth Links, page 51
- Cisco IPICS PMC Enhancements, page 63
- Upgrading to Cisco IPICS Release 2.0(1), page 76
- Support for Additional Cisco Unified IP Phone Models, page 77
- Support for Additional Cisco IPICS Hardware Platforms, page 78
- Revision to the Cisco IPICS PMC CLI Commands, page 78

Server Installation Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.0(1) server installation procedures.

As a best practice, make sure that you adhere to the following guidelines when you perform Cisco IPICS server installation procedures:

- If your server includes more than one network interface card (NIC), make sure that you configure the eth0 network interface, as documented in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1).* Cisco IPICS requires that you configure the eth0 interface, even if it is disabled, because the Cisco IPICS licensing mechanism performs its validation by using this NIC. Therefore, to ensure proper system operation, always configure the eth0 interface.
- Use the MAC address of the eth0 interface to obtain your license. To obtain the MAC address of the eth0 interface, enter the **ifconfig eth0** command.
- To obtain a license for your server, navigate to the following URL: http://www.cisco.com/go/license. (You need the Product Authorization Key (PAK) that shipped with your Cisco IPICS product package.)
  - You must purchase and install valid Cisco IPICS release 2.0(1) license(s) for use with this release. For more information about licenses, see the "License Structure and Feature Enhancements" section on page 43.
- Always log in to the Cisco IPICS server with root user privileges before you begin the server installation or uninstallation process.
- Make sure that you do not press the SysRq key when you are about to start the Cisco IPICS operating system installation or at any time during this installation process. If you press the SysRq key while you are installing the operating system, a kernel panic error occurs. To resolve this problem, you must restart the system with a hard reboot.
- Cisco recommends that you perform server installation tasks during a maintenance window or other off-peak hours to minimize service interruptions to users.
- The server installation process requires that you use the applicable Cisco IPICS operating system that is compatible with the version of server software that you are installing.

Note You must use only the Cisco-supported operating system for use with Cisco IPICS. No other operating system versions are supported.

- The Cisco IPICS installation requires a minimum of 2 GB of memory on the Cisco IPICS server. You can check the amount of memory that is installed on your server by entering the following command from the root user account:

  [root] #**top**

  The amount of memory that is installed on the server displays as shown in the example below:

  ```
  Mem:  2055448k av, 1490160k used,  565288k free, 0k shrd,  142344k
  buff
  ```
  To exit, press **Ctrl-C**.

- The Cisco IPICS operating system software installation is GUI-based and must be run from a directly-connected console terminal.
  - During this installation, the installer prompts you for the root user password.
  - Cisco IPICS enforces password aging for the root user (180-day password expiration) and strong passwords that must adhere to the following rules:

    Strong passwords must be at least eight characters long and include the following elements: at least one lower case letter, at least one upper case letter, at least one number, and at least one of the following special characters:

    @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

- In Cisco IPICS release 2.0(1), the server software installation program has been modified to use a text-based interface; you can install this software from a directly-connected console terminal or by remotely accessing the system via SSH Secure Shell client software (or similar software).
  - During this installation, the installer prompts you for the ipics and ipicsadmin user passwords.
  - Cisco IPICS enforces strong passwords that must adhere to the following rules:

Strong passwords must be at least eight characters long and include the following elements: at least one lower case letter, at least one upper case letter, at least one number, and at least one of the following special characters:

@ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

- Make sure that you follow the exact instructions in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)* to mount and copy the contents of the Cisco IPICS server software CD on to the server.
- To start the server software installation, enter the following command:

  [root]# **bash** <*installerfilename*>**.run**

  where:

  <*installerfilename*>**.run** specifies the name of the installer file.
- Cisco IPICS does not support a Redundant Array of Disks (RAID) on Cisco MCS 7825 servers. When you install the Cisco IPICS operating system on Cisco MCS 7825 servers, you must disable both the Serial ATA (SATA) controller option and the virtual install disk option to disable RAID.
- To complete the server software installation, log in by using the ipics user ID and password. Then, upload and apply the license file(s) to the server by navigating to the **Administration > License Management** window. (You must upload the license file to use the Administration Console features.)
- In this release, the default run level has been changed from run level 5 (GUI mode) to run level 3 (console mode).
- The Cisco IPICS server supports the following installation and/or upgrade options:
  - Typical—This option installs the Cisco IPICS server software and the Cisco Security Agent (CSA) software.
  - Upgrade—This option allows you to upgrade your server software.
- After you install the server software, make sure that you generate the PMC installer so that the installation file is associated with the correct server IP address. To generate the PMC installer, log in to the Administration Console. From the Server tab, navigate to **PMC Management > PMC Installer** to access the PMC Installer window. From this window, you can generate a new PMC installation file.

Note The Cisco IPICS server software includes the PMC application. You need to generate the PMC installer after the first time that you install the server software and after subsequent PMC application updates that include software fixes.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*

Server Upgrade Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.0(1) server upgrade procedures.

As a best practice, make sure that you adhere to the following guidelines when you perform Cisco IPICS server installation procedures:

- Verify the versions of Cisco IPICS that are compatible for upgrade before you upgrade your system. For the most recent version information, refer to the *Cisco IPICS Compatibility Matrix*.
- The Cisco IPICS operating system was modified, as part of this release, to accommodate support for additional hardware drivers and to provide hardware detection logic. Before you upgrade your server, make sure that you follow the sequence of steps to upgrade the operating system and server software, as documented in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*.
- Before you back up your data, make sure that you have available another Linux-based server or a Windows-based PC or server. Choose the remote host option only if the remote host supports the Linux Secure Copy (scp) command. To back up your data to a remote host that does not support scp, such as a Windows-based PC or server, choose the local directory option.
  - To back up your files to a Linux-based server, use the remote host option before you install the new Cisco IPICS operating system.
  - To back up your files to a Windows-based machine, use the local directory option; then, use the SSH Secure Shell Client software, or similar software, to perform a secure copy (scp) to the Windows-based machine.

- To upgrade to Cisco IPICS release 2.0(1), you must have valid release 2.0(1) license(s). For more information, see the "License Structure and Feature Enhancements" section on page 43.
- Before you begin, make sure that you have the installation CDs that pertain to both Cisco IPICS release 2.0(1) and the CDs that pertain to the Cisco IPICS release 1.0(2) server software.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*
- *Cisco IPICS Compatibility Matrix*

Backup and Restore Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.0(1) backup and restore procedures. It also includes information about guidelines to follow for choosing the database backup destination in the "Guidelines for Choosing a Destination for Database Backups" section on page 22.

Cisco IPICS includes the following options for database backups:

- Manual backups—At any time, you can perform a manual database backup to capture the current state of the Cisco IPICS database. To perform a manual backup, navigate to the **Administration** > **Database Management** > **Database Backup** window and click the **Backup Now** button.
- Scheduled backups—By default, Cisco IPICS backs up the database daily. This backup runs at a predefined time and Cisco IPICS stores the backup in a predefined location. You can change the time, frequency, and/or location of the scheduled backup.

As a best practice, make sure that you adhere to the following guidelines when you perform Cisco IPICS backup and restore procedures:

- To ensure data integrity in the event of system failure, Cisco recommends that you back up your files to a remote host location.
- Cisco recommends that you regularly check the database logs for status messages and/or error information that may be pertinent to recent backup and recovery activity.

  - To view the backup log, navigate to the **Administration > Database Management > Database Backup** window. Log entries display in the Backup Log pane.
  - To view and/or download the database logs, navigate to the **Administration > Database Management > Log** window.

- To help ensure the security of your data, Cisco IPICS does not support the use of different user IDs for remote backup and restore operations that you perform on the same data set. Therefore, when you restore your data, make sure that you specify the same user ID as the one that you used to back up your data. If you specify a different user ID, the restore procedure does not succeed because of file accessibility issues; in this situation, Cisco IPICS displays “permission denied” error messages in the db-maintenance.log. As a best practice, Cisco recommends that you designate a specific user ID that you can use for all of your remote backup and restore activities.

Guidelines for Choosing a Destination for Database Backups

Be aware of the following guidelines when you choose a destination for your Cisco IPICS backups:

- Cisco recommends that you choose the remote host option when you back up your database. Using the remote host option ensures that you have a location for your database backups that will not be affected by Cisco IPICS server hardware or software failures.
- As an extra safeguard, you can also copy or move a database backup from one remote host to another for redundancy purposes.
- Manually perform a database backup to a remote host destination before you uninstall, reinstall, or upgrade the Cisco IPICS server software to preserve your most recent data.
- When you reinstall the Cisco IPICS operating system software on your server, the installation process formats the hard drive and removes all data from your server. To prevent the loss of your backup data, make sure that you have available another Linux-based server or a Windows-based PC or server to back up your database.
  - For this backup, choose the remote host option only if the remote host supports the Linux Secure Copy (scp) command, such as a Linux server. To back up your data to a remote host that does not support scp, such as a Windows-based PC or server, choose the local directory option.

To back up your files to a Linux-based server, use the remote host option before you install the new Cisco IPICS operating system.

To back up your files to a Windows-based machine, use the local directory option; then, use the SSH Secure Shell Client software, or similar software, to perform a secure copy (scp) to the Windows-based machine.

For information about enhancements to the backup and restore processes in Cisco IPICS release 2.0(1), see the "Updates to the Backup and Restore Functionality" section on page 40.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.0(1)*

PMC Installation and Upgrade Guidelines

Note Cisco IPICS does not support the use of previous PMC releases with a Cisco IPICS release 2.0(1) server. That is, you must use PMC release 2.0(1) with a Cisco IPICS server that also has release 2.0(1) installed. If you try to use a pre-2.0(1) version of the PMC with a server that has release 2.0(1) installed, the PMC pops up a message to alert you of the version mismatch. In this situation, you must access the Cisco IPICS server via your browser to download and then install the 2.0(1) version of the PMC. Be aware that you will not be able to connect to your server by using the PMC until you upgrade your PMC.

This section includes information about the guidelines that apply to Cisco IPICS release 2.0(1) PMC installation and upgrade procedures:

- Install the PMC application on your local PC by downloading the software from the Cisco IPICS server.
- Be sure to install the PMC application on a client machine on which the required Windows operating system is already installed and be aware of the hardware requirements for your PMC client machine. For more information about software and hardware requirements, see the "PMC Requirements" section on page 12.

- The PMC installation involves downloading the self-extracting PMC installation program, which includes the PMC installation and configuration files along with the PMC skins, from the Cisco IPICS server. If you are authorized to use alert tones, the PMC installation program may also include alert tones (or they may be downloaded separately).
- The PMC installation program automatically installs the PMC software on your client machine.
- The PMC installation does not require connectivity to the server.
- The installation automatically adds an entry to the Windows Start menu for "Cisco IPICS PMC" along with a desktop shortcut. You can access the Start menu shortcut by navigating to **Start** > **Programs** > **Cisco IPICS** > **PMC**.
- Make sure that you close the PMC application before you install a new version of the PMC software.
- Upon login, the Cisco IPICS server provides information to the PMC about available versions; the PMC then performs a check for version compatibility and determines whether the PMC must be upgraded. See the "Managing PMC Version Numbers" section on page 71 for more information about version management.
- In this release, you do not need the fully executable file to completely update the PMC. The PMC automatic upgrade feature can update the PMC.dll file, PMC skins (if necessary), alert tones (optional), and/or online help depending on the contents of the update package. For more information about the automatic update process, see the "Managing PMC Version Numbers" section on page 71 and the "Support for Automatic Upgrades" section on page 73.
- In this release, Cisco IPICS provides the capability for the PMC to log in to the default, or primary, server or an alternate server if the primary becomes unavailable. To log in to the PMC, enter or choose the server IP address or host name, followed by your user ID and password.

Note Be aware that login user names and server host names are case-insensitive; that is, you can enter either upper case or lower case characters for these names. However, passwords are case-sensitive.

- The PMC can maintain multiple versions, current and previous, of the PMC application to enable quick reversion to an earlier compatible version, if necessary.

- When you have Cisco Security Agent (CSA) installed on the PMC client machine, be aware that you may be prompted with CSA access permission dialog boxes for various operations that you are trying to perform. Whenever CSA prompts you for permission, while you are performing any operation on the PMC, be sure to always click **Yes** to grant permission and continue with that operation. For more information about using CSA, refer to the Cisco Security Agent documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/index.htm

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

Cisco IPICS Security Enhancements

This release of Cisco IPICS includes many new security features and enhancements. The following sections describe the enhanced security features that are included in this release:

- Cisco IPICS Operating System Security Enhancements, page 25
- Cisco IPICS Server Security Enhancements, page 29

Cisco IPICS Operating System Security Enhancements

The following security and feature enhancements are available with this release of the Cisco IPICS operating system (OS). This section includes the following topics:

- Enhancements to the Cisco IPICS Operating System First Boot Window, page 26
- Changes to the Default Run Level, page 26
- Modifications to the File System Partition, page 26
- Additional Support for Cisco Media Convergence Server (MCS) Models, page 27
- Support for VMware Systems on the Cisco IPICS-Mobile Platform, page 27
- Enhanced System Cleanup for Additional Security, page 27

- Linux OS Password Complexity and Aging, page 28
- Support for Extended Daylight Saving Time, page 28
- SNMP Hardware and OS Support, page 28

Enhancements to the Cisco IPICS Operating System First Boot Window

The Cisco IPICS operating system first boot window has been modified to include the following enhancements:

- The Cisco IPICS OS installation now consists of five first boot windows. The first boot window has been enhanced to include a network configuration utility, which prompts you to configure the eth0 network interface.
- Removed from this release are the windows that prompted you to create a non-system user and an extra CD.
- This release also eliminates the "cisco" default password and adds a window that prompts you to change the root user ID password. The root password must adhere to password complexity and hardening rules. For more information, see the "Linux OS Password Complexity and Aging" section on page 28.
- The Cisco logo has been updated with the newly-introduced Cisco Corporate logo.

Changes to the Default Run Level

The following changes to the default run level, which is used when you install the Cisco IPICS operating system, have been implemented:

- In this release, the default run level has been changed from run level 5 (GUI mode) to run level 3 (console mode).

Modifications to the File System Partition

In this operating system release, the file system partition has been changed as described below:

- The amount of space that is allocated to the /opt file system has been increased.
- The /ipics file system has been omitted. Instead two file systems, "/idspri" and "/idssec" are created for a multidisk system and "/idspri" is created for a single disk system.

Additional Support for Cisco Media Convergence Server (MCS) Models

The addition of hardware drivers and hardware detection logic for supported Cisco IPICS platforms are included in this release:

- Hardware detection logic for the Cisco MCS servers has been added in this release.
- The OS can now detect Cisco MCS servers that use the hwdetect utility and install the necessary Ethernet drivers.
- This release adds support for additional Cisco MCS servers. For a complete list of hardware that is supported for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix*.

Support for VMware Systems on the Cisco IPICS-Mobile Platform

This release has been enhanced to provide support for systems that run the VMware operating system on the Cisco IPICS-Mobile Platform (Cisco IPICS-MP).

- The hardware detection logic in this updated OS can now detect an underlying VMware platform.
- This platform is supported only through a Cisco certified systems integrator. For additional details, please contact your Cisco sales representative.

Enhanced System Cleanup for Additional Security

To provide for enhanced security in Cisco IPICS, the following services have been removed:

- The Ethereal network sniffer has been removed from the operating system.
- The sendmail, mdmpd, mdmonitor, and netdump-server services have been removed.

To provide for enhanced security in this release of Cisco IPICS, the following Linux OS users have been removed or modified:

- The Tomcat, drf, enotify, and servmgr users have been removed.
- The sudoers file was cleaned to remove any entries that pertain to the Tomcat user so that there are no unnecessary Tomcat user associations in the sudoers file.

Linux OS Password Complexity and Aging

The following password security features have been implemented to provide enhanced levels of security in the Cisco IPICS operating system:

- The enforcement of password complexity, or strong passwords, that must adhere to certain rules for password creation for both the Linux root and ipicsadmin users.

  Strong passwords must be at least eight characters long, and include the following elements:

  - At least one lower case letter
  - At least one upper case letter
  - At least one number
  - At least one of the following special characters:

    @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

- The introduction of a password expiration setting that supports password aging for the Linux root user. By default, the password for this user is set to expire in 180 days.

Support for Extended Daylight Saving Time

The Cisco IPICS operating system has been updated to ensure compatibility with the planned change to extend Daylight Saving Time (DST) in the United States.

In August, 2005, Congress passed the Energy Policy Act of 2005 that includes the extension of DST to start on the second Sunday in March and end on the first Sunday in November. Beginning in 2007, DST starts on March 11 and ends on November 4. These dates differ from the previous DST start and stop dates that began on the first Sunday in April and ended on the last Sunday in October.

You do not need to take any action to ensure that these date changes occur accurately on your Cisco IPICS hardware.

SNMP Hardware and OS Support

For improved resource management, this feature enables a Simple Network Management Protocol (SNMP) agent to provide information and report on Cisco IPICS hardware and Linux operating system metrics.

- This release of Cisco IPICS provides read-only support for SNMP version 3 (SNMPv3). Read-only support includes the ability to monitor system status and performance; it does not include the ability to configure tasks by using SNMP.
- SNMPv3 is a protocol that facilitates the exchange of management information between network devices and includes security features for message integrity, authentication, and encryption.
- Cisco IPICS supports hardware status Management Information Base (MIBs) network objects and a set of network status MIBs that can be managed by using SNMP to provide information about the Cisco IPICS hardware and the Linux operating system.
  - Support is provided for a standard MIB browser that supports SNMPv3; the MIB browser includes the monitoring software that can be used to query the server for status and statistics and enable viewing of these MIB values.
  - To access the hardware MIBs, navigate to the Hewlett-Packard web site at http://www.hp.com. You can search for the MIBs by using the MIB name or the object ID (OID) and download the MIBs to your SNMP machine, if they are not already integrated.
  - The Cisco IPICS server stores the standard MIBs that are installed with the Linux operating system Net-SNMP package in the **/usr/share/snmp/mibs** directory; you can choose to download the MIBs from this directory to your MIB browser or management console, if these MIBs are not already installed.

Cisco IPICS Server Security Enhancements

The following information describes the security enhancements that have been implemented in the server, as part of this release. This section includes the following topics:

- Application Hardening, page 30
- File Permissions Hardening, page 30
- Tomcat Port Translation and Hardening, page 30
- Informix and Database User Hardening, page 31
- Application Password Hardening, page 31

Application Hardening

This release has been enhanced with the following application hardening security features:

- As part of the Cisco IPICS application hardening efforts, the ipicsadmin user has been created and enabled to perform Tomcat administration activities and connect to the Informix Dynamic Server. (The ipicsadmin user replaces the root user for this functionality.)
- The password of the ipicsadmin user is encrypted by using the Triple Data Encryption Standard (3DES) algorithm.
- With the Tomcat process running as the ipicsadmin user, which is a non-root user, it does not have access to files and/or folders that are not accessible by the ipicsadmin user or the ipics linux group.

File Permissions Hardening

File permissions hardening has been implemented in this release to ensure enhanced security when you use Cisco IPICS:

- A new group, ipics linux group, has been created.
- The ipicsadmin user belongs to the ipics linux group.
- The Tomcat directory is readable, writable, and executable by the ipicsadmin user and readable and executable by other members of the ipics linux group. All other users are denied access to this directory.

For more information about these system groups, see the "System User Roles and Groups" section on page 8,

Tomcat Port Translation and Hardening

The following security features have been implemented for the Tomcat server:

- The Tomcat server implements enhanced security by running on port 8080 (incoming HTTP traffic on port 80 is redirected to port 8080) and 8443 (all secure Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) traffic on port 443 is redirected to port 8443.)
- The PMC uses HTTP port 80 to poll the server for changes to download; all other communications are transmitted via secure Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) port 443.

Informix and Database User Hardening

For enhanced security, the following changes to database administration have been implemented:

- The informix user maintains the role of database system administrator.
- A new user, ipicsdba, has been created as a more restrictive user with the ability to execute certain utilities within the database. Cisco IPICS database and database objects are created by the ipicsdba user.
- Both the ipicsdba and informix users belong to the informix linux group; the ipicsdba user also belongs to the ipics linux group.
- Permission to access the database is limited to the ipicsadmin user.

For more information about these system user roles and groups, see the "System User Roles and Groups" section on page 8,

Application Password Hardening

The following password security features are available in this release to provide enhanced levels of security in Cisco IPICS:

- The enforcement of password complexity, or strong passwords, that must adhere to certain rules for password creation.

  Strong passwords must be at least eight characters long and include the following elements:

  – At least one lower case letter

  – At least one upper case letter

  – At least one number

  – At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?
- The introduction of a password expiration setting that allows you to configure when user passwords should be changed.
- A setting for the password history count, which specifies the number of passwords that Cisco IPICS marks as previously used and which the user cannot use again.
- The capability to lock out a user account and disallow new logins when the maximum number of consecutive invalid login attempts has been exceeded.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*

Introducing the Cisco IPICS Policy Engine

This release of Cisco IPICS introduces new functionality with the Cisco IPICS policy engine, which is included as part of the Cisco IPICS server. The policy engine enables telephony dial functionality and provides the capability to manage and execute policies and user notifications.

Note To enable the policy engine, you must install a Cisco IPICS license that includes a license for the policy engine. For more information about licenses, see the "License Structure and Feature Enhancements" section on page 43.

The Cisco IPICS Administration Console Policy Engine tab has been added to include the Policy Management and Dial Engine drawers. Any Cisco IPICS user can access these drawers, but some activities that are available from each drawer are accessible only to the Cisco IPICS operator or the dispatcher role.

The dial engine provides the capability to manage standard and/or custom scripts and prompts that enable the telephony user interface (TUI) interaction with incoming and outgoing calls and audio instructions to users. The control center enables system status monitoring and tracing.

- Policy engine activities can be performed from the Policy Management drawer in the Administration Console. These activities include policy creation, association, modification, activation, and execution status for scheduled policies and executing/executed policies.
- Dial engine activities can be performed form the Dial Engine drawer in the Administration Console. These activities include prompt management, script management, configuring SIP subsystem and provider parameters, setting dial engine parameters, managing the direct dial functionality, and monitoring the system status and configuring tracing via the control center.

The policy engine implements the following new features in this release:

- Policy creation and management have been enabled in this release. A policy includes one or more actions, or discrete functions, that perform when the policy executes. For example, a policy can start VTG and invite designated users to the VTG. Policies can also include one or more triggers, which cause the policy to execute automatically and, optionally, to repeat according to a specified schedule.
- The policy engine includes the dial engine, which integrates and enables the telephony user interface (TUI) and its associated features. The policy engine TUI executes scripts, which use prompts to provide audio instructions and information to users. The policy engine executes scripts that provide instructions to the TUI to play prompts and perform other operations. (A script plays prompts in the language that is designated for the script.)
- The TUI functionality enables dial-in access to VTGs and channels and dial-out and notification capabilities, based on user preferences, from VTGs to users. The TUI interacts with incoming and outgoing calls by using scripts. (An executing script plays prompts, which provide audio instructions to users.)
- The TUI allows users to use the telephone to receive information from, and provide instructions, to the policy engine, such as when users join and participate in associated VTGs or channels.
- The dial engine provides support for standard script prompts, customized script prompts, and spoken name prompts. (Custom prompts files that are uploaded for use must be G.711 u-law encoded. The PSTN gateways must also encode the audio to G.711 u-law for the dial-in PTT functionality.)
- Cisco IPICS stores prompts in a repository (logical storage medium) on the Cisco IPICS server. The server stores these prompts in logical folders that correspond to the languages of the prompts. When the policy engine TUI executes a script, it plays prompts from the language folder that is designated for the script to provide the ability to control the language in which a script executes. A special logical language folder, called default, makes prompts available to any script, regardless of the language that is designated for the script.
- The dial engine control center provides utilities to monitor system status and logs, configure tracing, and enable feature configuration. In addition, it also includes management of system and custom scripts and prompts, including language support. The TUI interacts with incoming and outgoing calls by using scripts. (An executing script plays prompts, which provide audio instructions to users.)

- Support for SIP-based dial functionality is provided via Cisco Unified CallManager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider for use with the policy engine. The policy engine requires that a SIP provider be configured in the customer network. A SIP provider handles calls to and from the policy engine.
- Enables implementation of the direct dial feature, which allows a PMC user to use the PMC push-to-talk (PTT) features to directly dial a phone number that is connected via the PSTN or an IP phone that is reachable via the customer network.
  - A direct dial call is a SIP call that originates from a PMC and routes through the RMS to the SIP provider. (The SIP provider routes the call to the number that the PMC user dials. The destination telephone can be any phone that is reachable by the SIP provider.)

For more information about the policy engine functionality, refer to the “Using the Cisco IPICS Policy Engine” and the “Configuring and Managing the Cisco IPICS Policy Engine” chapters in the *Cisco IPICS Server Administration Guide, Release 2.0(1).*

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.0(1)*

Cisco IPICS Server Enhancements

The Cisco IPICS server has been enhanced to include many new features, including the introduction of an improved Cisco IPICS Administration Console and additional functionality. In this release, the server also implements enhanced security features, including application, password, and operating system hardening. For more information about these security enhancements, see the “Cisco IPICS Security Enhancements” section on page 25.

This section describes the server enhancements and includes information about the following topics:

- Updates to the Backup and Restore Functionality, page 40
- Activity Logs and Monitoring Capabilities, page 42
- License Structure and Feature Enhancements, page 43
- Enhancements to the Ops Views Functionality, page 47

The release implements the following new features in the server:

- Support for a redesigned Cisco IPICS Administration Console graphical user interface (GUI) that incorporates GUI standardization, usability enhancements, and performance improvements, such as pagination and filtering for quicker searches.
  - Support for VTG list pagination and search (filter) functionality in the **VTG Management > Virtual Talk Groups** window. The VTG Participants window has been updated to enable view by channels, channel groups, users, user groups, and VTGs and search by channels, users, and VTGs.
  - Support for user groups member list pagination and search functionality, with an option to add a user group member, in the **User Management > User Groups** window. The user groups window includes an Association button that displays associated VTGs for selected user groups and user groups members. The users menu includes an Association button that displays associated VTGs for selected users.
  - Support for ops views details that include a separate resources window that can be accessed for selected resources by clicking the **Resources** button from the **Configuration > Ops Views** list and details windows. Ops views resources includes tabs for each of the resource types (channels, channel groups, users, users groups, VTGS, and policies). The ops views resources list displays in a paginated table.
  - Support for channel list pagination and search capability in the **Configuration > Channels** window. User and VTG associations for channels display by clicking the **Associations** button in the channel list or channel details windows. The channel associations user list displays paginated, with an option to add a user associations.
  - Support for user list pagination, status changes, and permission updates, including account lockout, in the **User Management > Users** window.
  - Support for user list pagination and segmentation by logged-in, PMC, IP phone, and dialed-in users in the **Administration > Active Users** window. This window also includes the ability to log out a PMC user who is currently logged in to Cisco IPICS. This activity releases the PMC resources. If the PMC is connected to the server, the PMC logs out of its session and displays the Login dialog box.
- The enhanced GUI includes the Server tab and the Policy Engine tab, each of which contains several drawers for improved functionality.

  - Server tab—Access the drawers and windows in this tab to perform Cisco IPICS administration and management functions.
  - Policy Engine tab—Access the drawers and windows in this tab to perform policy engine and dial engine functionality.
- The Serviceability drawer has been added to the Server tab in the Administration Console to provide easy access to overall system information, diagnostic details for the Cisco IPICS components, and system logging information.
- Cisco IPICS adds SNMPv3 support in this release. For more information, see the "SNMP Hardware and OS Support" section on page 28.

Table 5 provides a description of the Administration Console tabs and drawers. The functionality that can be performed in each of the drawers may vary depending on the individual user role. For more information, see the "Server Usage Guidelines" section on page 82.

Table 5 Cisco IPICS Administration Console Tabs and Drawers

Tab	Drawer	Description
Server		Contains the drawers that enable server-related administration and management tasks.
	Home	Includes windows that users access to manage profile data, association information, and download the PMC.
	VTG Management	Includes windows that the dispatcher uses to manage VTGs and events.
	User Management	Includes windows that the operator uses to manage users and user groups.
	Configuration	Includes windows that the system administrator uses to configure and manage ops views, channels, channel groups, locations, multicast resources, and RMS components.

Table 5 Cisco IPICS Administration Console Tabs and Drawers

Tab	Drawer	Description
	Administration	Includes windows that the system administrator uses to manage the database for backup and restore activities, upload, apply, and manage licenses, view active users and associated information for each user, manage and download activity log information, specify the activities, by ops view, that Cisco IPICS logs, and adjust system preferences and options in several areas (general, passwords, PMC).
	PMC Management	Includes windows that the system administrator uses to generate the PMC installer, maintain version control, and manage alert tones and skins.
	Serviceability	Includes windows that the system administrator uses to access Cisco IPICS system information via dashboards, view diagnostic information about the server and the components that interact with the server and execute diagnostic scripts and download the results, and view and download available system log information.
Policy Engine		Contains the drawers that enable policy engine and dial engine-related tasks.
	Policy Management	Includes windows that the dispatcher or operator uses to create, delete, and activate policies and manage associations, and manage scheduled and executing/executed policies.
	Dial Engine	Includes windows that can be accessed by different user roles to monitor the system status and set up tracing, manage languages, prompts, and spoken names, manage dial engine scripts, configure SIP and dial engine parameters, and manage direct dial information.

Tip An asterisk (*) that displays next to an input field in any of the drawers indicates required information.

- Includes an integrated RPM Package Manager (RPM) based command line installer for Cisco IPICS (server and the policy engine). RPM is an open package management system that allows source code to be packaged into multiple forms to enable easy installation, tracking, and updating. RPM maintains a database of all packages and their files, which can be used to verify packages and query for information about files and/or packages.
- Enhances the backup and restore processes to optimize usability and include backup and restore functionality for both the server and the policy engine databases. For more information about backup and restore enhancements, see the "Updates to the Backup and Restore Functionality" section on page 40.
- Provides support for high latency, low bandwidth connections. For more information about configuration and deployment models, see the "Support for High Latency Low Bandwidth Links" section on page 51.
- Provides support for policy engine functionality, including "inviting" and "dialing" participants to join VTGs and displaying, to dispatchers, information about the presence of called-in users.
- Supports communications preferences, which specify how the policy engine contacts a user during policy execution or dial-out. Communication preferences can include notification preferences (such as email, short message server (SMS), and pager addresses) and dial preferences (telephone numbers). For more information about the policy engine, see the "Introducing the Cisco IPICS Policy Engine" section on page 32.
- Allows modification of specific configurable attributes that pertain to the channel and user to ensure that entities are properly authorized:
  - The server configuration includes provisions for per-channel features to ensure that the PMC properly authorizes and displays data about the channels that are assigned to each PMC user.
  - The server configuration contains the level of user privileges that are provided to the PMC. These user privileges enable or disable the ability of the user to perform certain activities, such as latching a channel or using alert tones on the PMC.

- Eliminates extra actions that needed to be taken when an entity (user, user group, channel, or channel group) was modified or removed from the system. For instance, in this release the following behaviors apply:
  - When a disabled user is enabled and logs into the system, the user will be able to access and join any enabled channel that the user was associated to and/or any active VTG that the user has been assigned.
  - When a disabled channel is enabled, the channel does not automatically connect to the VTG that it was a participant in. The dispatcher must first reactivate the affected VTG; then, the channel can connect to and join the VTG.

    For more information, refer to the "Performing Cisco IPICS Dispatcher Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1).*
- Provides support for additional PMC functionality, such as automatic upgrades, alerts tones and skin management, the implementation of direct two-way and direct dial channels, the ability to set permissions that relate to latch, audio, and listen-only, and advanced permissions to specify the use of the multiselect, alert tones, DTMF, and All Talk features. The server also implements the use of visual indicators, such as channel coloring, for unique identification. For more information about PMC enhancements, see the "Cisco IPICS PMC Enhancements" section on page 63.
- Adds a new role, ops view administrator, to manage and monitor the activity logs that are filtered by ops views and accessible in the **Administration > Activity Log Management** window.
- Enhances system availability by eliminating the need to reboot the server when licenses or options change.
- Includes updated operating system software to support additional hardware drivers for later models of the Cisco Media Convergence Server (MCS) servers. Adds support for the Cisco IPICS-Mobile Platform, a VMware-based platform that is supported only through a Cisco certified systems integrator. For a list of hardware and software that is compatible for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix*.
- Provides support for Cisco Unified CallManager or a Cisco IOS router as a SIP provider, along with the ability to configure Cisco IPICS as an available phone service for a system that runs Cisco Unified CallManager Express on a Cisco IOS router.

- Supports additional Cisco Unified IP Phone models. For more information, see the "Support for Additional Cisco Unified IP Phone Models" section on page 77. For the most recent list of supported IP phones, refer to the *Cisco IPICS Compatibility Matrix*.
- Enhances license support through the use of more granular license types and improved license management functionality, including detailed license information for current usage and license limits for licensable features. This release also implements the use of time-bound licenses with expiration warnings. For more information about licenses, see the "License Structure and Feature Enhancements" section on page 43.
- Implements enhanced capabilities and flexibility for the Cisco IPICS activity logs and monitoring functionality by enabling filtering by ops view, activity log options, and the addition of the ops view administrator role. For more information about activity log enhancements, see the "Activity Logs and Monitoring Capabilities" section on page 42.
- Introduces the following new tools for enhanced usability:
  - enableuser—This tool can be used to unlock a user account that has been locked out. A user can be locked out when the number of consecutive invalid login attempts exceeds the maximum number, as configured in the server, or when the user ID is locked out from the **User Management > Users** window in the Administration Console. When a user has been locked out, no new logins are allowed.
  - reset_pw—This tool can be used to reset the password for the following users: ipics, ipicsadmin, informix, and root.
  - modify_ip—This tool can be used to facilitate changing the Cisco IPICS server network settings (IP address and/or host name).

Updates to the Backup and Restore Functionality

In this release, Cisco IPICS includes enhancements to the GUI-based backup and restore functionality to optimize usability and include backup and restore functionality for both the server and the policy engine databases.

The Administration Console database management link has been redesigned to include the following tabs in the **Administration > Database Management** window from which you can perform backup and restore operations:

- Database Backup—Click this tab to back up your database and choose one of the following options for your backup destination:
  - Default—Choose this option to store your backup in the Cisco IPICS default directory.
  - Local Directory—Choose this option to specify a directory that is located on the Cisco IPICS server to back up your database.
  - Remote Host—Choose this option to back up your database to a remote location. The remote host must support the Linux Secure Copy (scp) command.

  The log entries that display in the Backup Log pane show the status of your backup activity.
- Restore from Backup—Click this tab to restore the database that you backed up. The following options apply for the restore destination:
  - Default—Choose this option to restore your data from the default location.
  - Local Directory—Choose this option to restore your data from the local directory that you specify. This entry requires the full directory path.
  - Remote Host—Choose this option to restore your data from a remote host, in the directory location that you specify. Be sure to enter the correct user name, password, and remote directory; otherwise, the scp process fails.
- Schedule Backup—Click this tab to configure options for your scheduled database backups. In this window, you can specify the scheduled backup destination, backup retention period, and scheduled backup start time and day(s).
- Log—Click this tab to view the logs entries for backup and restore activity. The Database Logs pane enables a view of the system logs. This window provides visual indication of the types of status messages that display, along with a status summary that indicates the number of error messages, warning messages, and total messages that the log displays.
  - Cisco IPICS stores the backup and restore logs in the db-maintenance.log and the dbm_log_archive.log.gz. To download these log files and save them to your PC as text files, click the **Download** button in the **Administration** > **Database Management** > **Log** window.

The db-maintenance.log file captures the logging information that Cisco IPICS generates for backup or restore operations in a single day. You can view the contents of this log from the **Administration > Database Management > Log** window.

Note The db-maintenance.log file does not appear on the server immediately after a new installation is done. Cisco IPICS generates the db-maintenance.log file after the first time that you complete the backup/restore process

The dbm_log_archive.log.gz file is a compressed file that contains archived data from previous db-maintenance.log daily log files.

Note Cisco IPICS stores these log files in the **/opt/cisco/ipics/database/logs** folder on the server.

Activity Logs and Monitoring Capabilities

This release includes the following enhanced capabilities and flexibility for the Cisco IPICS activity logs and monitoring functionality:

- Expands activity log management by allowing you to choose to view activity logs for any channel, user, or VTG, based on ops views and resource type.
  - By ops view—Specifies the ops views to which the resource belongs
  - By channel—Specifies the users and VTGs that used the channel
  - By user—Specifies the channels and VTGs that the user participated in
  - By VTG—Specifies the users channels that were participants in the VTG
- Enhances your ability to view specific logs by ops view and resource type by searching for particular logs based on a date range. The system administrator and the ops view administrator can apply the date range filter to minimize the log results. After filtering the activity log resource list by ops view and resource type, you can then choose one of the resources from a single list.

- The ops view administrator can monitor only the activity logs of the ops view to which that user belongs. If a particular ops view is removed, then all of the activity logging is done by using the default SYSTEM ops view. The system administrator can monitor all ops views logs.
- Provides the capability to download activity log files that have been archived according to the threshold limits that are configured in the **Administration** > **Options** window in the Administration Console.
- Allows the flexibility of specifying only the activities that you want Cisco IPICS to log, by ops view, in the **Administration** > **Activity Log Options** window.

License Structure and Feature Enhancements

This section contains information about license enhancements in this release of Cisco IPICS. It also includes information about time-bound licenses in the "Support for Time-bound Licenses" section on page 46.

To use the Cisco IPICS solution, you must first upload and install one or more licenses that are specific for release 2.0(1). This release of Cisco IPICS expands the number and types of licenses that you can purchase so that they are more granular.

For instance, the server now differentiates between VTG multicast port licenses and channel multicast port licenses. In earlier Cisco IPICS releases, both VTGs and channels shared the same multicast port license type.

This new licensing structure is based on the following licensable features:

- Base policy engine feature license, which may be in the same or a separate license
- The concurrent number of 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
- Total number of ops views

The total number of LMR and multicast ports, PMC, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased.

Note To enable the Cisco IPICS policy engine, you must install a license that includes the policy engine feature.

See Table 6 for a description of these licenses.

Table 6 Cisco IPICS License Features

Type of License	Description
Concurrent LMR Ports	Cisco IPICS uses a single LMR port license when a channel is enabled. The server releases the license for use after the channel is disabled or deleted. Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location. If a channel has two multicast addresses that are assigned to it, the channel uses two licenses. If one of the multicast addresses is removed, the system releases one of the licenses so that only one license is being used.
Concurrent Multicast Ports	Cisco IPICS uses a single multicast port license when a VTG is activated. The server releases the license for use after the VTG is deactivated.
Concurrent PMC Users	Cisco IPICS uses a single PMC license each time a PMC user logs in to the PMC. If the same PMC user logs in to multiple PMC sessions from different client machines, that user consumes multiple licenses (one for each session). Make sure that you are aware of the current status of PMC licenses. If all of the available PMC licenses have been used, Cisco IPICS interrupts PMC access to the system.
Concurrent IP Phone Users	Cisco IPICS uses a single IP phone license when an IP phone user logs in to Cisco IPICS.

Table 6 Cisco IPICS License Features (Continued)

Type of License	Description
Concurrent Dial Users	Cisco IPICS uses a single dial user license in each of the following situations: • When there is an active inbound call, one license is used • When there is an active outbound call, one license is used
Cisco IPICS Ops View	Cisco IPICS uses one license for each ops view that you configure. The License Summary pane displays the number of ops views that are available for use.
Cisco IPICS Base Server License	This field displays as “licensed” in the License Summary pane to indicate that you have purchased a base license for Cisco IPICS.
Policy Engine Base License	This field displays as “licensed” in the License Summary pane to indicate that you have purchased a license to enable the policy engine functionality.

From the **Administration** > **License Management** > **Summary** tab in the Administration Console, you can access the License Summary pane to view the licensed features for your system. The License Summary pane displays the total number of the licensable features.

The License Summary pane also indicates whether the Cisco IPICS base server license and the policy engine base license has each been licensed.

The License Usage Per Ops View pane displays license information per ops view, including types of licenses, the ops view to which they belong, current license usage, and the allocated ports.

For more information about licensable features, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1).*

Support for Time-bound Licenses

This version of Cisco IPICS also includes support for time-bound licenses. Time-bound licenses, such as evaluation or demonstration licenses, differ from purchased (non-time-bound) licenses in that they include a preconfigured license expiration date.

When a time-bound license is about to expire (about 30 days before expiration), Cisco IPICS displays a warning message to alert you of the upcoming expiration.

- When a license feature expires, the relevant functionality of that license becomes disabled.
- After your license expires, it remains valid for a maximum of 24 hours after the expiration date. (The server checks for expired licenses every 24 hours.)

Be aware of the following considerations when you use Cisco IPICS time-bound licenses:

Note The following information does not pertain to purchased (non-time-bound) licenses, which are not affected by system date changes.

- Cisco IPICS invalidates time-bound licenses when you change the system date in the operating system, after the Cisco IPICS server software has been installed, to either a past date or a future date. Invalid licenses cause the Cisco IPICS system to become inoperable.
- Generally, time-bound licenses are valid only when the system date/time is set to the current date. However, an exception occurs when you perform the following actions, which result in time-bound license invalidation:
  - If you change the system date to a past date, the license becomes invalid.
  - If you then change the system date back to the current date, the license remains invalid.
  - If you change the system date to a future date, and then change it to the current date, the license becomes invalid.

  Note You must restart the license manager, or reboot the server, for system date changes to become effective.

To resolve issues that pertain to these system date changes, take the following actions:

1. Restart the license manager by entering the following command:

   [root]# **service ipics_lm restart**

2. Revalidate the license by performing one of the following actions:

   - Navigate to the **Administration > License Management** window; then, click **Apply** to restart the license server.
   - Change the system date to reflect a past date and then reset it to the current date.

For more information about time-bound licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1).*

Enhancements to the Ops Views Functionality

This section includes the following information about the ops view functionality in this release of Cisco IPICS:

- Overview, page 47
- User Roles, page 48
- Ops View Port Allocations, page 49
- Ops View Attributes, page 49
- Ops Views Caveats, page 49

Overview

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. That is, resources in separate ops views are not accessible to users in other ops views unless the users are granted permission to access them.

The use of ops views allows segmentation of resources that authorized Cisco IPICS users may see in the Administration Console. The use of ops views does not affect the channels and/or VTGs that may be assigned and viewable on the PMC or Cisco Unified IP Phone.

Note To create additional ops views, you must purchase and install a Cisco IPICS license that includes a sufficient number of ops views ports to meet your allocation requirements.

When the ops view feature has been enabled, the system displays a Cisco IPICS Ops View entry in the **Administration > License Management > License Summary** pane, along with the total number of ports, current usage, and available ports. For more detailed information about ops views license allocations, navigate to the **Configuration > Ops Views** window.

The Cisco IPICS license contains a specified number of ops views that can be configured.

- By default, Cisco IPICS includes a SYSTEM ops view.
- You cannot delete or edit the SYSTEM ops view.
- Cisco IPICS administrators belong to the SYSTEM ops view and can view all ops views, and their resources, that are configured on the system.

User Roles

Only the system administrator can create new ops views. After a new ops view is created, the system administrator can associate resources, such as channels or users, to the ops view. The operator then can create 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.

Ops view administrators have the ability to monitor resources that are in the ops view to which they belong. An ops view administrator is assigned to each ops view in Cisco IPICS.

Note Cisco recommends that each ops view contain at least one dispatcher and one operator to manage the resources that are visible to these roles.

Ops View Port Allocations

Each time that the system administrator adds a new ops view, ports are taken from the SYSTEM ops view and allocated to the newly created ops view. The system administrator determines the number and types of ports that are needed for a particular ops view.

When an ops view is deleted, the system administrator can reallocate the resources that were allocated to that ops view to existing ops views in the system.

If the Cisco IPICS license contains the policy engine, the system administrator can configure dial information per ops view. For information about adding directory numbers for ops views and updating the SIP provider configuration information to include the new directory numbers, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1).*

Note When the server is upgraded to Cisco IPICS release 2.0(1), the ops view port allocations are adjusted to fit within the new licensing structure. If the number of existing ops views is greater than the newly-allocated port count, Cisco IPICS allows the existing ops views to function but does not allow new ops views to be created. For more information about the license changes in this release, see the "License Structure and Feature Enhancements" section on page 43,

Ops View Attributes

The Cisco IPICS ops views functionality supports the following attributes:

Belongs To— The Belongs To attribute determines the ops view to which the resource belongs, or that the ops view owns. When resources belong to, or are assigned to, an ops view, Cisco IPICS charges the port usage to that ops view.

A resource can belong to only one ops view.

- Accessible To—The Accessible To attribute specifies that the resource is accessible to, or visible to, the ops view(s). Users only have access to the resources that are accessible to the ops view to which they belong.

  A resource can be accessible to an unlimited number of ops views or no ops views at all.

Ops Views Caveats

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

- 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.
- The system allows Cisco IPICS operators to view and modify only those users who either belong to or are accessible to the same ops view as the operator.
- The system allows the Cisco IPICS dispatcher to view and modify only those VTGs that contain resources that either belong to or are accessible to the same ops view as the dispatcher. Any dispatcher who has access to shared resources within a VTG that belongs to a different ops view can fully access that VTG.
- 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.
- 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.
- 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.
- As a general rule, VTGs inherit accessibility from the resource that it contains.

For detailed information about ops views, refer to the “Configuring and Managing Cisco IPICS Operational Views” chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*

Support for High Latency Low Bandwidth Links

This release of Cisco IPICS extends the functionality of release 1.0 by providing support for environments that include high latency and low and/or variable bandwidth links, such as satellite links. In these types of environments, connectivity may become unstable because of the geographical location of the user, weather elements, and other interferences. In this release, Cisco IPICS compensates for these dynamically variable bandwidth scenarios and enhances its support for mobile operations.

This release introduces support for the following deployment scenarios:

- Central site server solution—This solution supports a Cisco IPICS server that is installed at a central site and a distributed router media service (RMS) and end-user client components that are installed at a remote site.
- Remote locations solution—This solution supports deployment of the Cisco IPICS server, RMS, and end-user clients at two remote sites that are connected by M1:U12:M2 tunnels.
- Remote PMC solution—This solution supports a Cisco IPICS server and a distributed RMS at a central site and end-user PMC clients at a remote site.

Note With this deployment scenario, remote PMC clients must be configured to use the "Optimize for low bandwidth" setting in the PMC **Settings > Channels** menu. For information about how to configure the PMC for use in this deployment scenario, refer to the "Configuring the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

The M1:U12:M2 tunneling technology enables these deployment scenarios. For more information about these deployment scenarios, see the "Supported Deployment Solutions" section on page 52,

The following sections describe the new features that are available and pertinent to this release of Cisco IPICS. It includes the following topics:

- Supported Deployment Solutions, page 52
- Requirements and Support Information, page 56
- Performing Additional Configurations on Your Server and Your PC, page 57
- Performance Guidelines, page 62

Supported Deployment Solutions

In this release, Cisco IPICS enhancements include support for two deployment solutions, as documented in the following topics:

- Central Site Server Solution, page 52
- Remote Locations Solution, page 54
- M1:U12:M2 Configuration Examples, page 55

Central Site Server Solution

In this scenario, the Cisco IPICS server is located in a central site and an RMS is distributed with the PMC and other end-user clients in a remote site that is connected via a high latency, low bandwidth connection. In this situation, the Cisco IPICS server must control the distributed RMS, and the dispatcher at the central site needs to be able to communicate with remote PMC clients in the field.

This deployment solution provides the ability to remotely control the RMS over the high latency, low bandwidth links. Communications are enabled by the support of an M1:U12:M2 connection trunk between the RMS in the central site and a remotely-located RMS.

The M1:U12:M2 connection trunk also provides the capability for IP phone XML services and PMC clients to communicate between sites.

Note M1:U12:M2 (Multicast1:Unicast1-Unicast2:Multicast2) provides a unicast connection path between two multicast islands. An M1:U12:M2 connection trunk maps multicast to unicast on one side of the network, provides transport over the unicast wide area network (WAN) as a unicast Voice over IP (VoIP) call, and then converts it back to multicast on the other side of the connection, such that multicast 1 is connected to multicast 2 via a unicast connection between 1 and 2 M1:U12:M2 transports only the multicast traffic that is configured on the trunk as contrasted to Generic Routing Encapsulation (GRE) tunnels, which transport all multicast traffic.

Tip See the "Performing Additional Configurations on Your Server and Your PC" section on page 57 for additional configurations that apply to this deployment.

Caveats

Be aware of the following caveats when you use this deployment solution:

- Because all RMS commands flow over the high latency, low bandwidth link, this solution results in reduced throughput and slower response time.
- Some RMS-related operations may take over 3 minutes. Throughput considerations are based on factors such as the number of active channels that are included in the VTGs, the number of DS0s that are being used on the RMS, and the number of PMC users that are communicating between the sites. This limitation is due to inherent Transmission Control Protocol/Internet Protocol (TCP/IP) limitations over high latency, low bandwidth links. For information about RMS configuration updates when you use this deployment solution, see the "Updating the RMS Configuration" section on page 57.
- If you do not have a local router installed at the central site, you may need to configure Address Resolution Protocol (ARP) commands to increase the ARP timer so that the RMS remains reachable. For more information, see the "Adjusting ARP Commands" section on page 58.
- The RMS and Cisco IPICS server automatic synchronization mechanism must be disabled in this scenario. Therefore, you must manually synchronize these components. For more information about the manual configurations that you must perform, see the "Disabling the RMS Comparator" section on page 58 and the "Merging the Configuration" section on page 59.
- To conserve bandwidth, you must disable the PMC upload log frequency in this release. For more information, see the "Disabling the PMC Upload Activity Log Frequency" section on page 60.
- Although the M1:U12:M2 connection trunk consumes dedicated bandwidth between the central site and the remote site, it does provide for bandwidth optimization by allowing transcoding to the G.729 codec.
- This deployment does not support the use of IP phone XML services at the remote locations.
  - IP phone XML services are available only at the central site.
- There is no support for direct PMC access to the remote locations.
  - The PMC clients can be at the remote site or the central site but they cannot remotely connect across sites.

Remote Locations Solution

In this scenario, a Cisco IPICS server, RMS, PMC, and other end-user clients are located at two remote sites. High latency, low bandwidth links that connect these remote sites enable communications flow.

This deployment solution enables communications by the use of fixed M1:U12:M2 tunnels that are configured between the channels that are hosted on each RMS at each remote site, such that each channel is mirrored on the other sites.

The M1:U12:M2 connection trunk also provides the capability for IP phone XML services and PMC clients to communicate between sites.

Tip See the "Performing Additional Configurations on Your Server and Your PC" section on page 57 for additional configurations that apply to this deployment.

Caveats

Be aware of the following caveats when you use this deployment solution:

- The M1:U12:M2 connection trunks consume dedicated bandwidth between the remote sites, however bandwidth optimization is enabled by allowing transcoding to the G.729 codec.
- If you use multiple Cisco IPICS servers that each control their own RMS, care must be taken not to duplicate VTGs when defining channels. Because each channel is mirrored on the other remote site, audio loops can occur between the sites when you use the same VTGs at each site.
- This deployment provides support for IP phone XML services at either the central site or the remote sites.
  - The IP phone XML services must be local to the site where they are deployed.
- There is no support for direct PMC access to the remote locations.
  - The PMC clients can be at the remote site(s) or the central site, but they cannot remotely connect across the sites (they must be local to the site where they are deployed).

M1:U12:M2 Configuration Examples

The following tables provide configuration examples for the M1:U12:M2 connection trunks.

Note For complete and more detailed configuration examples, refer to the "Cisco IPICS Deployment Models" chapter in the *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*.

The two multicast addresses that are being tunneled in the following configuration examples are 239.192.21.3:21000 and 239.192.21.5:21000.

Table 7 illustrates the manual commands that are required to configure the voice port and dial peer entries in RMS location #1 to enable the M1 portion of the M1:U12:M2 connection trunk.

Table 7 RMS Location #1 Configuration

RMS Location #1 Voice Port Configuration	RMS Location #1 Multicast Dial Peer M1 Configuration

`voice-port 0/0:1`
`auto-cut-through`
`lmr m-lead audio-gate-in`
`lmr e-lead voice`
`no echo-cancel enable`
`playout-delay mode adaptive`
`playout-delay maximum 250`
`playout-delay minimum high`
`playout-delay nominal 100`
`no comfort-noise`
`timeouts call-disconnect 3`
`timing hookflash-in 0`
`timing hangover 40`
`connection trunk 2001`
	`dial-peer voice 3 voip`
	`destination-pattern 2001`
	`session protocol multicast`
	`session target`
	`ipv4:239.192.21.3:21000`
	`(RMS M1)`
	`codec g711ulaw  vad aggressive`

Table 8 illustrates the manual commands that are required to configure the voice port and dial peer entries in RMS location #2 to enable the M2 portion of the M1:U12:M2 connection trunk.

Table 8 RMS Location #2 Configuration

RMS Location #2 Voice Port Configuration	RMS Location #2 Multicast Dial Peer M1 Configuration

`voice-port 0/0:2`
`auto-cut-through`
`lmr m-lead audio-gate-in`
`lmr e-lead voice`
`no echo-cancel enable`
`playout-delay mode adaptive`
`playout-delay maximum 250`
`playout-delay minimum high`
`playout-delay nominal 100`
`no comfort-noise`
`timeouts call-disconnect 3`
`timing hookflash-in 0`
`timing hangover 40`
`connection trunk 1001`
	`dial-peer voice 3 voip`
	`destination-pattern 1001`
	`session protocol multicast`
	`session target`
	`ipv4:239.192.21.5:21000`
	`(RMS M2)`
	`codec g711ulaw  vad aggressive`

Requirements and Support Information

This release provides the following levels of support:

- Delay—Provides support for up to three seconds end-to-end latency.
- Packet Loss—Supports up to 10% packet loss over the network.
- Jitter buffer—Enables support for up to 250 ms of maximum jitter on the network (to support burst latency).
- Link outages—Provides support for temporary link outages such that if the connection from the PMC is interrupted, the connection automatically continues when it becomes available again (the user is not informed of the outage).
- Bandwidth—Supports 64 kbps bandwidth per channel configured over an M1:U12:M2 connection trunk.

PMC Caveat

The following caveat pertains to the first time that the PMC logs in to the server:

- Upon the first PMC login, an error message displays to inform the user that the channels are being disabled. This error occurs because of the time delay to connect. To recover from this error, click **OK**. After the server completes its tasks, the channels will display on the PMC (this timing will vary based on latency).

Performing Additional Configurations on Your Server and Your PC

This section includes information about additional configurations that are required on the Cisco IPICS server and on the PC that you use to access the Cisco IPICS Administration Console.

The following additional configurations are required when you use these deployment solutions.

- Updating the RMS Configuration, page 57
- Adjusting ARP Commands, page 58
- Disabling the RMS Comparator, page 58
- Merging the Configuration, page 59
- Disabling the PMC Upload Activity Log Frequency, page 60

The following additional configuration is required on the PC that you use to access the Administration Console:

- Adjusting Internet Explorer Browser Settings, page 60

Updating the RMS Configuration

When you use one of these deployment solutions, you must update every RMS that is configured with Cisco IPICS and used over a high latency, low bandwidth connection. This configuration update modifies the maximum TCP outgoing queue on a per-connection basis.

To modify the maximum TCP outgoing queue, perform the following procedure on each RMS:

Procedure

Step 1 Enter global configuration mode by entering the following command:

Router# **configure terminal**

Step 2 To set the maximum TCP outgoing queue to 100000 packets, enter the following command:

```
Router(config)# ip tcp queuemax 100000
```

Step 3 To save your configuration, enter the following command:

```
Router(config)# write mem
```

Step 4 To exit the router configuration mode, enter the following command:

```
Router# exit
```

Adjusting ARP Commands

If you use the central site server solution and you do not have a local router installed at the central site, you may need to increase the ARP timer in the server. This adjustment helps to prevent timeouts and ensure reachability between the server and the RMS when these components are connected via Ethernet and separated by a high latency link.

If you encounter issues with ARP timeouts and ping response times, contact the Cisco IPICS Support Team to obtain information about how to resolve these issues.

To contact the Cisco IPICS Support Team, send an email to ask-ipics-support@external.cisco.com

Disabling the RMS Comparator

The RMS comparator is the mechanism that checks the responsiveness of the RMS and if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized.

Because this synchronization mechanism can interject delay, the RMS comparator needs to be manually disabled in this release. To disable the RMS comparator, perform the following procedure.

Note Be aware that this change is a global change and affects all RMS components that are configured in the server.

Procedure

Step 1 Log in to the server by using the ipics user ID and password.

Step 2 From the Administration Console, navigate to **Administration** > **Options**.

Step 3 From the General tab, check the **Disable RMS Comparator** check box that is located in the RMS pane.

This change disables the RMS comparator so that it does not run.

Step 4 Click **Save** to save your change.

Step 5 In the RMS pane, verify that the Disable RMS Comparator check box is checked and that the RMS Polling Frequency field is dimmed.

Merging the Configuration

After you have disabled the RMS comparator, you must merge the configuration to make sure that the router is synchronized with the server.

Note As a best practice, make sure that you merge the RMS configuration whenever manual changes have been made to the RMS. This process ensures that the components are synchronized. Perform this procedure before you perform any configuration changes, such as activating a VTG.

To merge the configuration, perform the following procedure:

Procedure

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

Step 2 To manage the RMS configuration, check the check box that corresponds to the RMS that you need to manage.

Step 3 From the Configuration drop-down list box, choose **Merge** to merge the RMS configuration.

Wait while this process completes. Cisco IPICS displays the changes in the Edit Router Details area.

Disabling the PMC Upload Activity Log Frequency

To conserve bandwidth, you must disable the PMC upload log frequency in this release. To disable the PMC upload log frequency, perform the following procedure.

Note Be aware that this change is a global change and affects all PMC clients that connect to the server.

Procedure

Step 1 Log in to the server by using the ipics user ID and password.

Step 2 From the Administration Console, navigate to **Administration > Options**.

Step 3 Click the **PMC** tab to access the PMC configuration options.

Step 4 In the Configuration pane, check the **Disable PMC Activity Log Upload** check box.

This change disables the PMC log upload mechanism so that the PMC clients that are connect to this server never upload their logs to the server.

Step 5 Click **Save** to save your change.

Step 6 In the Configuration pane, verify that the Disable PMC Activity Log Upload check box is checked and that the PMC Send Logs on Rollover, PMC Activity Log Update, and PMC Log Upload Frequency fields display as dimmed.

Adjusting Internet Explorer Browser Settings

When you use a high latency, low bandwidth connection, you may encounter browser timeout errors when you try to update the RMS configuration for any RMS that is configured with twelve or more loopback interfaces.

To resolve this issue, you must modify the Internet Explorer settings on your PC to adjust the timeout duration. This configuration modifies the ReceiveTimeout data value to allow for the additional delay.

Caution Please use extreme caution when you modify the registry. If you are not familiar with editing the registry, you should seek technical support assistance before you perform this procedure. If you modify the registry incorrectly, you may need to reinstall the operating system. Therefore, make sure that you back up the registry before you modify it and are aware of how to restore the registry, if a problem occurs.

Tip For more information about how to back up, restore, and modify the registry, access the Microsoft Support site at http://support.microsoft.com and search the Microsoft Knowledge Base for a description of the Microsoft Windows registry.

To modify the ReceiveTimeout data value, perform the following procedure on the PC that you use to access the Cisco IPICS Administration Console:

Procedure

Step 1 On the PC that you use to access the Administration Console, choose **Start** > **Run**.

Step 2 In the Open dialog box, enter **regedit**.

The Registry Editor displays.

Step 3 Click the + sign that displays next to the **HKEY_CURRENT_USER** entry.

The folders that contain root configuration information for the user who is currently logged in displays.

Step 4 Click the + signs that display next to each of the folder names to navigate to the **Software\Microsoft\Windows\CurrentVersion\** folder.

Step 5 Click the + sign that displays next to the **Internet Settings** folder.

At this point, you have navigated to the following folder: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**.

Step 6 In the Internet Settings folder, look for the **ReceiveTimeout** name.

Step 7 To modify this setting, right-click the **ReceiveTimeout** name; then, click **Modify**.

The Edit DWORD Value dialog box displays. The current DWORD value displays in hexadecimal format.

Alternatively, you can choose to delete the ReceiveTimeout name altogether by clicking **Delete**. If you choose to take this action, be aware that you could wait indefinitely for the server to respond.

Step 8 Click the **Decimal** radio button to display this value in decimal format.

Step 9 To configure this value to the recommended setting to accommodate high latency, low bandwidth links, enter **480000** in the Value data field.

This modification configures the timeout value to 8 minutes.

Step 10 Click **OK** to save your change.

Step 11 To exit the Registry Editor, choose **Registry > Exit**.

Step 12 Restart your PC for the change to become effective.

Performance Guidelines

Be aware of the following guidelines that pertain to this release of Cisco IPICS:

- Each RMS can support a predefined number of commands, such as VTG activation, VTG deactivation, and PMC SIP (remote) connections. If the number of commands that the RMS receives exceeds this threshold, the excess commands fail and must be resubmitted.
- For high latency, low bandwidth deployments, allow 1.5 minutes for every three channel/VTG activations.
- If five dispatchers submit commands, or if the same dispatcher submits multiple commands, a wait time of 1.5 minutes should be allotted before resubmitting new command requests.
- For constant load conditions, a frequency of about 18 seconds per simple VTG command should be allotted on 2811 routers (RMS components), on average. Additional RMS components must be installed to support above average load conditions.

Where to Find More Information

- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

Cisco IPICS PMC Enhancements

The Cisco IPICS PMC has been enhanced to include new functionality, such as the ability to log in to another server and the use of several different channel types, along with the introduction of alert tones, visible connectivity indicators, and new and upgraded skins.

This section describes the PMC enhancements and includes information about the following topics:

- PMC Skin Design Enhancements, page 65
- Channel Appearance on the PMC, page 67
- New and Enhanced PMC End-User Features, page 68
- Managing PMC Version Numbers, page 71
- Support for Automatic Upgrades, page 73

This release of Cisco IPICS includes the following PMC enhancements:

- For enhanced usability, this release supports the capability for the PMC to log in to the server that has been configured as the default server or an alternate server if the default server becomes unavailable. The PMC login includes a field where you can enter or choose the server IP address or host name

Note Be aware that login user names are case-insensitive; that is, you can enter either upper case or lower case characters for your PMC user name. However, passwords and server host names are case-sensitive.

- Additional password security has been implemented in this release. For more information, see the "PMC Usage Guidelines" section on page 89.
- Increased PMC serviceability includes the use of visible connectivity status indicators for different scenarios:

  - When the PMC is connected to the server, a green connectivity indicator displays. When connectivity with the server is lost, a red indicator and an alert icon display; clicking this indicator opens the Status menu.
  - When SIP-based remote connections fail, the PMC displays a warning indicator in the form of a yellow triangle next to the specific channel that lost connectivity. This indicator signifies that a problem exists with the remote end (PMC, RMS, or server) and that it may not be able to send or receive traffic. During this interruption, the PMC continues to attempt to reconnect.
- The server configuration sets the permissions that relate to latch, audio, and listen-only, and advanced permissions to specify the use of the multiselect, alert tones, DTMF, and All Talk button features. The server also implements the use of channel coloring for unique channel identification.
- This release implements certain visual indicators, such as visual indication of secure channels, channel type, and channel label.
- The PMC provides support for a maximum of 3 simultaneous multicast voice streams per channel or VTG.
  - The PMC does not transmit any voice streams that exceed the maximum allowable number. The PMC continually tracks the number of voice streams and transmits only when the limit is not exceeded.
  - The PMC does not provide visual or audible indication when the channel or VTG is not transmitting. As a best practice, monitor the receive indicator for PMC traffic; when the receive indicator shows activity, the PMC is receiving traffic. If you talk while the receive indicator shows activity, you are likely not being heard.
- Provides support for the PMC automatic update feature by using upgrade packages that can include customized content. (The contents of the update package determine whether the PMC skins, alert tones, and online help are also updated as part of the automatic update process.) For more information, see the "Support for Automatic Upgrades" section on page 73.
- Includes updated PMC hardware requirements based on CPU load and support for a specific number of active channels; for example, there are different PMC hardware requirements to support up to 4 active channels, up to 6 active channels, and up to 18 active channels. For detailed configuration information, see the "PMC Requirements" section on page 12.

PMC Skin Design Enhancements

In this release, Cisco IPICS includes redesigned skins that provide additional choices to enable greater communications flexibility.

- Support is provided for a maximum of eighteen channels and several different skins that you can use for the PMC. (The PMC allows the assignment of up to 50 channels, but only 18 channels may be active at the same time.)
- You can create your own personalized interface by accessing the **Settings** > **Skin** menu in the PMC application and choosing from one of the available skins (the 4-channel, 6-channel, and 18-channel skins may be available in lighter and darker versions):
  - 4-Channel Mode—This PMC client displays 4 channels that you control with your mouse. It includes the standard set of Cisco IPICS features.
  - 6-Channel Mode—This PMC client displays 6 channels that you control with your mouse.
  - 4-Channel Touch Screen Mode—This PMC client displays 4 channels in a low resolution touch screen format. It includes the standard set of Cisco IPICS features.

Note The touch screen skins include a transmit indicator that blinks red when you are transmitting traffic.

  - 8-Channel Touch Screen Mode—This PMC client displays 8 channels in a low resolution touch screen format. It includes the standard set of Cisco IPICS features.
  - 18-Channel Advanced Console—This PMC advanced console displays 18 channels that you control with your mouse. It includes the Cisco IPICS advanced feature set, including new menus and buttons. Table 9 describes the features of the 18-channel skin.

Table 9 Cisco IPICS PMC 18-Channel Skin

Button/Menu	Description
Activation/Deactivation Button	Activates and deactivates a channel. This button highlights and changes orientation when activated.
PTT Channel Button with Receive Indicator and Latch Indicator	Click and hold to talk. In transmission mode, this button highlights in a different color. In receive mode, the receive indicator blinks green. If you have permission to use the latch functionality, you can click the latch indicator to latch the channel(s) and talk on one or more channels at the same time. **Note** When a SIP-based remote connection failure occurs, the PTT channel button also displays a warning indicator in the form of a yellow triangle next to the specific channel that encountered the connectivity failure.
Channel Select Check Box	Check to select or deselect the channel for PTT communications.
Voice Replay Controls	Plays back buffered voice transmissions.
Volume Up, Volume Down, Volume Indicator	Increases, decreases, and displays the current volume level on the channel.
Server Status Connectivity Indicator	Dynamically specifies PMC connectivity status with the server. • When the PMC is connected to the server, a green connectivity indicator displays. • When the PMC is not connected to the server, a red connectivity indicator and an alert icon display.
Menu Button	Enables access to the PMC settings menus and online help.
All Talk Channel Button	Click the All Talk channel to simultaneously talk on all of the channels that you selected.
Select All and Deselect All Buttons	Selects and deselects all channels on the PMC (multiselect).

Table 9 Cisco IPICS PMC 18-Channel Skin (Continued)

Button/Menu	Description
Alert Tone Button	Plays out alert tones only on the channel(s) that you select.
Skin Menu	Use to reconfigure the PMC skin.
Status Menu	Provides information about the PMC and its connectivity to the server and enables easy access to the server via your browser.
Channels Menu	Enables channel configuration via certain settings, such as such as spatial positioning, key mapping, and channel reordering.
Advanced Menu	Provides the option to modify settings, such as the All Talk button key mapping and VPN settings.

Channel Appearance on the PMC

Be aware of the following modification to the appearance of PMC channels in this release:

- Channels that appear in blueprint mode on the PMC indicate that the channel/VTG is available and waiting for you to activate.
- If the channel has been disabled, you will not be able to activate the channel (none of the buttons will appear).
- If your ability to transmit on a channel has been disabled by the server, the channel appears dimmed on the PMC.
- When the channel appears dimmed, the PMC is not transmitting traffic. For instance, if you mute the microphone and click the PTT button or if there is a network transmission problem, the channel appears dimmed on the PMC to indicate that transmission is not occurring.

For more information about channel states, see the "PMC Usage Guidelines" section on page 89.

New and Enhanced PMC End-User Features

This release includes many new and enhanced PMC features that enable further user configuration and flexibility. Table 10 describes these features, some of which may be available only with the 18-channel PMC advanced console skin.

Table 10 Cisco IPICS New and Enhanced PMC End-User Features

PMC Feature	Description
Keyboard mapping	This feature has been enhanced to support user-customizable key-to-channel mapping. With this change you can assign specific keys to each of your channels and transmit by pressing and holding the assigned key. (This feature is accessible from the **Settings** > **Channels** menu.) Cisco IPICS also supports the use of a device that simulates key down and key up events, such as a footswitch or other USB device. Key mapping is stored locally on the PMC client machine for the individual user who configured the key mapping assignments. If you change PMC client machines, you must reconfigure the key mapping assignments. This release removes the static key mappings that were available in release 1.0(x).
DTMF tones	Enables transmission of DTMF tones for a fixed time duration to channels that you select. Supports DTMF tone generation by using inband signaling.
Select and multiselect and All Talk button	Includes select and multiselect features to allow selection of one or more channels for audio transmission and alert tones. Channel selection is done by checking the check box that displays in the lower left corner of the channel(s) on the PMC. Alternatively, you can select all channels by clicking the Select All (multiselect) button, which is located in the bottom portion of the 18-channel PMC skin, and use the All Talk channel to talk.

Table 10 Cisco IPICS New and Enhanced PMC End-User Features

PMC Feature	Description
Alert tones	Plays out alert tones on one or more channels that you select on the PMC. (You must have permission to use alert tones.) To play out an alert tone, you must first select a channel (or multiple channels) by checking the channel select check box; then, click the tone that you want to play out. The PTT channel highlights to indicate that transmission is occurring. Alert tone buttons do not actively display on the PMC until you select at least one channel by checking the channel select or multiselect check box.
Voice replay	This release introduces support for play back of buffered audio on a per-channel basis. Each channel maintains its own recording buffer. Upon activation of a channel, the voice replay controls display on the lower half of the PMC channel when there is audio in the buffer; when there is no audio in the buffer, the voice replay controls appear dimmed on the PMC. **Note** You must click the jump back, or rewind, button to enter voice replay mode and play out the available, recorded audio.
Channel reordering	Implements channel reordering to allow the repositioning of channels that display on the PMC. (This feature is accessible from the **Settings > Channels** menu.) The ability to reorder your channels allows you to place channels in the order that you want to see them; for example, the channels that you use most often can be positioned at the top of the PMC. This feature helps to optimize the space on your PMC skin so that you may be able to use a skin that includes fewer channels.

Table 10 Cisco IPICS New and Enhanced PMC End-User Features

PMC Feature	Description
Direct two-way and direct dial channels	Provides support for point-to-point connectivity via direct two-way and direct dial channels. The direct two-way channel allows PMC users to talk directly from one online user to another by using the PMC. The direct dial channel allows a PMC user to use the PMC PTT features to directly dial a telephone that is connected via the PSTN or an IP phone that is reachable via the customer network. (Direct dial calls are SIP-based calls that route from the PMC through the RMS to the SIP provider.) There is no capability to connect to other third parties when you use these channels.
Support for high latency, low bandwidth links	Includes an option for users who connect via a high latency and/or low bandwidth link. This option allows audio quality optimization, on a per-channel basis, when the channel connection is via a high latency (high delay) and/or low bandwidth link, such as when you use a satellite connection. (This feature is accessible from the **Settings** > **Channels** menu.)

- If the focus changes when you are using a mouse, keyboard, or USB device to transmit on a channel, the transmission stops when the PMC detects that it is no longer the active application (or has lost focus). In this case, the PTT button changes color to indicate that it is no longer transmitting; this break in transmission occurs even if you continue to hold down the mouse or mapped key. After the PMC regains focus, you can begin transmitting again.
- Alert tone playout is not affected when the PMC loses focus; that is, alert tones continue to play out even if the PMC loses focus.

Managing PMC Version Numbers

Note Cisco IPICS does not support the use of the 1.0(x) release of the PMC with a Cisco IPICS release 2.0(1) server. That is, you must use PMC release 2.0(1) with a Cisco IPICS server that also has release 2.0(1) installed. If you try to use a pre-2.0(1) version of the PMC with a server that has release 2.0(1) installed, the PMC pops up a message to alert you of the version mismatch. In this situation, you must access the Cisco IPICS server via your browser to download and then install the 2.0(1) version of the PMC. Be aware that you will not be able to connect to your server by using the PMC until you upgrade your PMC.

The Cisco IPICS server maintains information about version compatibility to ensure version control. This version control extends to alert tone upgrades and skin downloads.

When the PMC initially starts up, the server communicates the PMC versions that are configured in the server and available to be run. Table 11 describes the range of PMC versions that Cisco IPICS release 2.0(1) supports.

Table 11 Cisco IPICS Server–PMC Version Information

Version Information	Description
Recommended	This version represents the recommended software version that should be run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform you. The server then sends this version to the PMC and the PMC installs it after you respond positively to the message prompt or if other installed versions are not supported.

Table 11 Cisco IPICS Server–PMC Version Information (Continued)

Version Information	Description
Staged	This version represents the software version that the PMC downloads according to the discretion of the administrator. The server sends this version to the PMC for download but the PMC does not install it until the administrator changes the state of this version to recommended or operational. At that time, the PMC may install the new version after you respond positively to the message prompt or if other installed versions are not supported.
Operational	This version represents a version of PMC software that is operational. This version is supported for use with the server but there may be a later version that is also supported. **Note** The server always extends priority to the PMC versions that it marks as recommended.
Not supported	This version represents an unsupported PMC software version. The server does not send this version to the PMC so that you cannot choose an unsupported version from the drop-down list box in the location dialog box. **Note** The server forces an upgrade on any PMC that is currently running an unsupported version of software.

By using the version information that is provided by the server, the PMC can take the following actions:

- Force a download and installation of a new PMC version if the version that is currently running is not supported.
- Allow you to continue to use a PMC version that is marked as operational.
- Prompt you to download the recommended version (the current version may be marked as operational).

  - You have the option to continue to use the earlier version or download and install the later version.
  - If you choose to download the recommended version, the PMC downloads and installs this version. Then, the PMC prompts you to log in again and choose the latest version from the location selection dialog box. For more information, see the "Support for Automatic Upgrades" section on page 73.
  - If the current version is not supported, the PMC forces an upgrade to the recommended version.
  - If the PMC is running the recommended version, no action is taken.
- Download the staged version without installing it. The PMC may download this version but does not install it until the server configuration has been updated to reflect this version as recommended or operational.
- Delete the versions that are not supported.

Support for Automatic Upgrades

This section contains information about the automatic PMC update process. It also includes information about managing skin downloads, as part of the PMC update process, and managing alert tone upgrades in the following topics:

- Managing Skin Downloads, page 74
- Managing Alert Tone Upgrades, page 74

If your PMC client machine does not have the recommended version of the PMC software, a pop-up message displays to prompt you to download the recommended version.

- When you click **Yes** to this prompt, the PMC package for the recommended version downloads to the PMC client machine.

  The PMC package may include the PMC.dll file, PMC skins, alert tones, and online help, or a combination of components, depending on the specific configuration of the package.

After the PMC package downloads, the PMC version installs and the PMC prompts you to run the recommended version.

- When you click **Yes** to this prompt, the PMC login dialog box displays so that you can log in to the system again and choose the latest version from the location selection dialog box.

Note The PMC automatic update process may install only the PMC.dll file or it may install other components as well, depending on the contents of the package. The contents of the update package determine whether the PMC skins, alert tones, and online help are also updated as part of the automatic update process.

Managing Skin Downloads

Cisco IPICS manages downloads of PMC skins, including customized skins, that are included in the PMC package as part of the automatic update process. To minimize any impact to performance, Cisco IPICS downloads the skin files when the PMC starts up. Upon download, the skin files become available to all PMC users who connect to any Cisco IPICS server.

The server downloads the skins in a compressed .zip file format and then automatically uncompresses the file on the PMC client machine. If the server downloads a new version of the skin that you currently use, you must reselect the skin from the **Settings** > **Skin** menu to use the most updated version.

Note

- When you upgrade the PMC from one version to the next, the PMC provides support for only the most current version of the skins, as displayed in the **Settings** > **Skin** menu. However, the PMC does not remove the obsolete skins from the Skins directory that resides on the PMC client machine hard drive.
- Be aware that when you download skin names that match existing skin names, the PMC overwrites these names in the Skins directory on the PMC client machine hard drive.

Managing Alert Tone Upgrades

In this release, Cisco IPICS provides the capability for the PMC to broadcast .wav files that contain alerting tones (hereafter referred to as alert tones) to a variety of Cisco IPICS users at the same time. Cisco IPICS stores alert tones in a set on the server. An alert tone set is associated with an ops view; therefore, each PMC user can see only one tone set based on the ops view association. For more information about ops views, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1).*

You must be authorized to use alert tones, as configured in the server. If you are authorized to use alert tones, the PMC downloads the defined tone set from the server. To ensure that you have the appropriate tones, and to minimize impact to voice quality, Cisco IPICS downloads the alert tone set when the PMC starts up.

If the association between a tone set is modified in the ops view to which you belong and after the PMC has started up, a pop-up message displays to inform you that a tone set is available for download. You may choose to proceed with the download or cancel the operation.

- If you click **Yes** to the download prompt, the tone set downloads and the PMC refreshes to display the new alert tones.
- If you click **No**, the PMC cancels the operation and prompts you the next time that you log in to Cisco IPICS.

The server manages the alert tone download process in a similar manner to the automatic update process such that the server can force the download or prompt you to download the new alert tone set. Cisco IPICS supports the following alert tone version control categorizations:

- Required—When the server determines that the alert tone download is required, the file is automatically downloaded to the PMC.
- Recommended—If the download is recommended, Cisco IPICS prompts you to download the alert tone file now or at a later time. (If you choose to download at a later time, the system prompts you the next time that you log in to the server.)

Note Be aware that voice quality may be affected when you download alert tone sets.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*
- *Cisco IPICS Compatibility Matrix*

Upgrading to Cisco IPICS Release 2.0(1)

If your Cisco IPICS server is running release 1.0(2) and the 1.0(2) operating system or the 1.0(3) operating system, you can upgrade your server to release 2.0(1) by using the Cisco-provided CD-ROM format that is available for this upgrade.

This upgrade software is only available on CD-ROM format; it is not available via web download. If you are not sure about how to obtain this software, contact your Cisco representative for information.

Note Your server must be running Cisco IPICS release 1.0(2) with the 1.0(2) operating system or the 1.0(3) operating system to upgrade to Cisco IPICS release 2.0(1).

Tip To verify which versions of Cisco IPICS are compatible for upgrade, refer to the most recent version of the *Cisco IPICS Compatibility Matrix* at http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

The Cisco IPICS operating system was modified as part of this release to accommodate support for additional hardware drivers and to provide hardware detection logic. Therefore, you must follow the exact sequence of steps that are documented in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)* to fully upgrade your operating system and server software to Cisco IPICS release 2.0(1).

1. Deactivate all active VTGs.
2. Perform a remote backup of your data.
3. Install the Cisco IPICS operating system, release 2.0(1), which is an updated version of the operating system.
4. Reinstall the Cisco IPICS release 1.0(2) server software.
5. Restore the data that you backed up to a remote server.
6. Upgrade the Cisco IPICS release 1.0(2) server software to Cisco IPICS release 2.0(1).
7. Reactivate any VTGs that you deactivated in Step 1.

Note Cisco IPICS release 2.0(1) does not support the use of GUI mode for the Cisco IPICS release 2.0(1) server software installation.

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

For guidelines about Cisco IPICS server installation and upgrade procedures, see the "Server Installation Guidelines" section on page 17 and the "Server Upgrade Guidelines" section on page 20.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*
- *Cisco IPICS Compatibility Matrix*

Support for Additional Cisco Unified IP Phone Models

In this release, Cisco IPICS expands its IP phone lineup by adding support for the following phones:

- Cisco Unified Wireless IP Phone 7921
- Cisco Unified IP Phone 7940G/7941

With this addition, the Cisco Unified Wireless IP Phone 7921 and the Cisco Unified IP Phone 7940/7941 joins the Cisco Unified IP Phone 7960/7961 and the Cisco Unified IP Phone 7970/7971 as part of the Cisco IPICS portfolio to provide enhanced productivity and call-handling capabilities.

For information about how to subscribe, access, and use the Cisco IPICS service on the Cisco Unified Wireless IP Phone and Cisco Unified IP Phone supported models, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device" appendix in the *Cisco IPICS Server Administration Guide.*

For a list of phones that are supported for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix.*

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.0(1)*

- *Cisco IPICS Compatibility Matrix*

Support for Additional Cisco IPICS Hardware Platforms

This release of Cisco IPICS adds support for additional Cisco MCS servers and the Cisco IPICS-Mobile Platform. The Cisco IPICS-Mobile Platform runs VMware and is supported only through a Cisco certified systems integrator. For additional details, please contact your Cisco sales representative.

For details about the additional hardware platforms that are supported for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix.*

Where to Find More Information

- *Cisco IPICS Compatibility Matrix*

Revision to the Cisco IPICS PMC CLI Commands

The Cisco IPICS PMC Command Line Interface (CLI) enables the use of CLI commands to perform specific PMC activities, such determining whether a specified PTT channel is active, enabled, latched, or muted, playing out a .wav audio file to a specified PTT channel, and toggling the activate button to activate/deactivate the specified PTT channel.

In this release, Cisco IPICS reduces support for the CLI commands that you can use to perform specific PMC activities to the following six commands:

- Activate Command—Toggles the Activate/Deactivate button on the specified PTT channel.
- IsActivate Command—Returns a code that designates whether the specified PTT channel is active.
- IsEnabled Command—Returns a code that designates whether the specified PTT channel is enabled.
- IsLatch Command—Determines whether the PMC PTT button for the specified PTT channel is latched.
- IsTxMuted Command—Returns a code that designates whether the specified PTT is muted by Cisco IPICS.
- Play Command—Outputs a wave audio file to the specified PTT channel.

Note

Make sure that you do not use the CLI commands that were previously documented in the *Cisco IPICS Command Line Interface, Release 1.0(1)* documentation, as these commands are no longer supported for use with Cisco IPICS.

Where to Find More Information

- *Cisco IPICS PMC Command Line Interface, Release 2.0(1)*

Important Notes

The following section contains important information that pertains to this release of Cisco IPICS.

- Using Cisco Security Agent with the PMC, page 79
- Establishing PMC Connectivity with the RMS for SIP-Based Remote Connections, page 80
- Cisco IPICS Usage and Licensing Guidelines, page 81
- Cisco IPICS Voice Quality Tips, page 97

Using Cisco Security Agent with the PMC

When you have Cisco Security Agent (CSA) installed on the PMC client machine, be aware that you may be prompted with CSA access permission dialog boxes for various operations that you are trying to perform.

Note

Whenever CSA prompts you for permission, while you are performing any operation on the PMC, be sure to always click **Yes** to grant permission and continue with that operation.

CSA may prompt you for permission in the following instances:

- If you are prompted with a CSA access permission dialog box during the PMC installation process, be sure to click **Yes** to grant permission to the PMC installation.

- If you are prompted with a CSA access permission dialog box when you launch a new version of the PMC or after a system reboot, make sure that you click **Yes** to grant permission to allow the PMC to monitor the media device (microphone).

Note If you allow CSA to time-out based on its default value of No after you launch the PMC, the PMC will be able to receive traffic but it will not be able to send traffic; that is, you will still be able to listen to any active conversations but you will not be able to transmit.

- If you are prompted with an access permission dialog box when you activate a channel on the PMC, be sure to click **Yes** to grant permission.
- If you are prompted with an access permission dialog box when you uninstall the PMC, click **Yes** to grant permission.
- If the “Don’t ask me again” check box displays as an option, you may check it to instruct CSA not to prompt you again in the future.

For information about using CSA, refer to the Cisco Security Agent documentation at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/index.htm

Establishing PMC Connectivity with the RMS for SIP-Based Remote Connections

To connect the PMC via a SIP-based remote connection, make sure that the PMC can establish connectivity to the RMS router. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) If the PMC cannot establish connectivity to the RMS, PMC users may experience channel activation issues (such as fast busy) when they attempt to use a SIP-based remote connection.

To determine the IP address of the RMS, access the **Settings** > **Channels** menu in the PMC application. (If you cannot determine the IP address of the RMS, contact your System Administrator for assistance.) Click a remote connection channel to highlight it; then, scroll down the Channel Properties to the SIP Proxy field to find the IP address of the RMS for the associated channel. For more information about the Channels menu, refer to the “Configuring the PMC Application” chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1).*

From the PMC client machine command line interface, enter the ping command to ping this IP address and verify connectivity.

C:\ping *<SIP Proxy IP address>*

where *SIP Proxy IP address* represents the RMS component.

Note The PMC must be able to establish connectivity to the RMS to enable SIP-based remote connections. Make sure that you can successfully ping this IP address to ensure PMC connectivity to the RMS. If the PMC cannot connect to the RMS, you may experience channel activation issues (such as fast busy) when you attempt to use a SIP-based remote connection.

For more information, refer to http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd33374

Cisco IPICS Usage and Licensing Guidelines

This section includes information about Cisco IPICS usage and licensing guidelines; it includes the following topics:

- Browser Guidelines, page 81
- Server Usage Guidelines, page 82
- PMC Usage Guidelines, page 89
- License Guidelines, page 95

Browser Guidelines

Cisco IPICS supports the use of Internet Explorer version 6.0.2. Be aware of the following browser-related guidelines and caveats when you use Cisco IPICS:

- The Administration Console times out after 30 minutes of non use. When a timeout occurs, you are prompted to log back in.
- As a best practice, make sure that you update your browser window often and before you perform any server administration tasks to ensure that you are working with the most current information. If you attempt to perform

administration updates 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.

- To ensure that a current browser window displays the most current information, refresh it by clicking the button or tab that you used to display it. 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.

Server Usage Guidelines

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

- Cisco IPICS provides support for various user roles, including system administrator, ops view administrator, operator, dispatcher, and user. The functionality that may be performed is dependent on the specific user role.
- For increased system security, the Administration Console times out after 30 minutes of non 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; then click **Log In**. To exit the Administration Console, click **Logout** in any Administration Console window.
- Server login user names and server host names are case-insensitive; passwords are case-sensitive, so be sure to enter passwords exactly as they are configured in the server.

- Access to the Cisco IPICS server online help system is available from various windows in the Administration Console. To access the server online help, click the **Help** link in any Administration Console window.
- To view information about the version of Cisco IPICS that you are using, click **About** in the Administration Console.
- In this release, the redesigned Administration Console includes two tabs: Server and Policy Engine.
  - Server tab—Access the drawers and windows in this tab to perform Cisco IPICS administration and management functions. In these windows, you can configure and manage Cisco IPICS components, such as the RMS, channels and channel groups, and ops views. You can perform administration functions, such as uploading licenses, managing the database, monitoring activity logs, and setting system performance options. You can also perform VTG, user, and PMC management operations in these windows, as well as monitor system performance and usage.
  - Policy Engine tab—Access the drawers and windows in this tab to perform policy engine and dial engine functionality. In these windows, you can create and manage Cisco IPICS policies, enable the telephony user interface (TUI), configure SIP and dial engine parameters, manage dial-in/dial-out functions, and monitor the system status and set up tracing. Although any Cisco IPICS user can access the policy engine tab, some activities require specific capabilities based on user roles.
- Many of the Administration Console windows allow you to modify the appearance of the results by specifying search criteria and reformatting the results based on rows per window.
  - Depending on the window, you may be able to search, or filter, your results based on resources, locations, roles, and ops views.
  - You enter your search criteria in the Filter field and click **Go**.
  - When you search on a character string, Cisco IPICS returns all results that begin with the specified character(s).
  - To clear the search criteria, click **Clear Filter**.
  - To modify the number of rows that display, choose from the Rows per page drop-down list box that displays at the top of the window; then, click **Go**.

  - To navigate between results windows, click the arrows that display at the bottom of the window.

- Many of the Administration Console windows include drop-down list boxes, some of which become available only after you perform certain functions. If you do not perform the required function, the drop-down list box displays as dimmed to indicate that it is not available for use.
- An asterisk (*) that displays next to a field, drop-down list box, or check box, in the Administration Console indicates required information. You must provide this information before you can save 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; clicking this button may close the window automatically. The Cancel button cancels any changes that you have made.
- 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. As such, this address range is less likely to cause an addressing conflict in an existing multicast domain.
- Cisco IPICS does not support the use of multiple Cisco IPICS servers for the same RMS component because each server must have the use of resources on a corresponding RMS for proper functionality.
- Cisco IPICS provides support for more than one RMS component in the same location.
- When you configure your RMS component, make sure that you perform all of the configuration procedures that are documented in the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1).*
- If you remove the second hard drive from the Cisco MCS 7825-H2 server while Cisco IPICS is running, your system may become inoperable after a reboot. In this situation, the server detects the second hard drive but reflects its status as "degraded" and does not allow the OS to run from either the CD or the hard drive. To resolve this issue, you must fully reload the server, which results in loss of data. If you encounter this problem, make sure that you preserve your data by backing up your database before you reboot the server. For more information about backing up your database, see the "Backup and Restore Guidelines" section on page 21.

- Cisco IPICS provides support for a maximum of 1.5 seconds of network round-trip delay between the Cisco IPICS server and the Cisco Unified CallManager or Cisco Unified CallManager Express components. When the round-trip delay is greater than 1.5 seconds, the following issues may be encountered:
  - Dial-in calls to the policy engine do not succeed; in this case, users hear a busy tone.
  - Users may hear back their own speech, similar to echo, because of the delay.
- Be aware of the number of participants in a conference and their type of connection to avoid resource contention.
- Inform new PMC users about how best to communicate when using the Cisco IPICS solution. For more information, see the "PMC Usage Guidelines" section on page 89.
- The Cisco IPICS server contains the associated connection configuration, which correlates to locations, to determine how users should connect. Cisco IPICS provides connection support for both multicast and unicast communications. Because PMC users need to choose their location, make sure that PMC users are aware of the appropriate location information to use when they log in to Cisco IPICS.
- 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. Users who are in the same multicast domain are also in the same Cisco IPICS location. 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.

    Table 12 provides a description of the ALL and REMOTE locations.

Table 12 Cisco IPICS Predefined Locations

Predefined Location	Description
ALL	• 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. • The ALL location defines the scope or reachability of a multicast address. For this reason, the ALL location is applicable to channels and VTGs, which are associated with multicast addresses, but not applicable to IP phones or RMS components, which are not associated with multicast addresses. • Channels that are designated with the ALL location can be mixed on any RMS, including RMS components that are not configured with the ALL location, because any RMS can send packets to a multicast address that is associated with the ALL location. • VTGs are always associated with the ALL location because every VTG multicast address is dynamically-assigned and associated with the ALL location.

Table 12 Cisco IPICS Predefined Locations (Continued)

Predefined Location	Description
REMOTE	• The REMOTE location is available only to PMC users. When a PMC user chooses the REMOTE location from the Location drop-down list box, connectivity is established with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user. – For each channel that is associated with the user, the PMC establishes a SIP-based unicast connection with the RMS that is defined in the same location as the channel. – For each VTG that is associated with the user, the PMC can establish a SIP-based unicast connection with any RMS because VTGs always use a multicast address in the ALL location. • In all cases, the Cisco IPICS server allocates RMS resources upon successful PMC authentication. When additional channels or VTGs are assigned to a logged-in user, the server immediately allocates the necessary RMS resources for each channel or VTG. When the PMC user activates the channel or VTG, the PMC places the SIP call to the appropriate RMS. **Note** For more information about locations, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1).*

Table 13 provides a summary of Cisco IPICS access types and connections.

Table 13 Summary of Cisco IPICS Access Types and Connections

Access	Type of Connection	Description
IP Phone	Multicast (in all cases)	• Can connect to any VTG that the IP phone user is associated with. • Can connect to any channel that the IP phone user is associated with if the channel is in the same location as the location that is defined in the user dial login default location.
Dial-in	Unicast to the dial engine (in all cases)	• Can connect to any channel or VTG that the dial-in user is associated with.
PMC (remote login)	Unicast	• All channels and VTGs are unicast calls to the appropriate RMS.
PMC (non-remote login)	Multicast	• Can connect to any channel via multicast if the user is associated with the channel and the channel is configured with the same location as the location that was chosen by the user at login. • Can connect to any VTG that the user is associated with.
PMC (non-remote login)	Unicast	• Can connect to any channel that is configured with a location that is different from the location that was chosen at login.

For more information about server usage guidelines, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1).*

PMC Usage Guidelines

Note Cisco IPICS only supports the use of PMC release 2.0(1) with a Cisco IPICS server that also runs release 2.0(1).

This section includes guidelines for using the PMC; it includes the following topics:

- Tips for Using the PMC, page 89
- PMC Connectivity Tips, page 90
- PMC Login Caveats, page 91
- Using the PMC in Offline Mode, page 91
- PMC Account Lockout and Password Expiration Guidelines, page 92
- PMC Channel Indicators and States, page 93
- Optimizing Your Audio on the PMC, page 94

Tips for Using the PMC

The following tips will help you to use the Cisco IPICS PMC most effectively:

- Use a high-quality microphone and check the placement and settings of your audio devices before you begin to use the PMC. For more information about optimizing your audio, see the "Optimizing Your Audio on the PMC" section on page 94.
- Your ability to use certain PMC features, such as latch, multiselect, alert tones, DTMF, and All Talk, depend on the configuration in the server.
- You can use only those voice channels that have been assigned to you and which are visible on your PMC.
- When a channel is activated, the PTT button highlights and changes color. (For more information, see the "PMC Channel Indicators and States" section on page 93 and refer to the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* for the various channel states and appearances on the PMC.)
- To talk on a channel, click and hold the push-to-talk (PTT) button before you speak.

- Talk in short bursts and monitor the receive indicator so that you do not talk over other Cisco IPICS users.

Tip Be sure to monitor the receive indicator on the PTT channel button for PMC traffic so that you do not talk over other Cisco IPICS users. When the receive indicator shows activity, you are receiving traffic. If you talk while you are receiving traffic, you are likely not being heard.

- The capability for the PMC application to coexist with other voice applications depends on the operating system that you use. For more information, refer to thee *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

PMC Connectivity Tips

The following tips will help to ensure successful connection of the Cisco IPICS PMC:

- Before you launch the PMC, establish network connectivity to make sure that you have a valid IP address.
- For connections that use the remote location, make sure that the PMC can establish connectivity to the Router Media Service (RMS). For more information, see the "Establishing PMC Connectivity with the RMS for SIP-Based Remote Connections" section on page 80.
- If the Cisco VPN Client is installed on your PMC client machine, disable the "Stateful Firewall (Always On)" option; otherwise SIP and multicast connections may not work correctly.
- For the PMC to work properly with Windows XP, you may need to modify the firewall settings so the PMC can send and receive the required protocols.
- Network limitations may prevent some PMC client machines from sending audio. In this case, choose the remote location to connect to Cisco IPICS.
- Monitor the server status connectivity indicator and other connectivity indicators for connection information. For more information, see the "Cisco IPICS PMC Enhancements" section on page 63.

- If you use a docking station or pluggable audio devices with your client machine, close the PMC client and unplug your audio devices before you undock your PC; otherwise, your PC may become unresponsive and require you to reboot.
- The Cisco IPICS server contains the location information to determine how the PMC should connect. For optimum connectivity and higher quality audio, use the most appropriate location for your connection type when you log in to the PMC. If you choose a location and you do not hear any voice traffic, choose a different location until you hear the audio on the channel.
- If both wired and wireless connections are active, and if you selected a location other than remote, either disable the wireless connection or make sure that the PMC uses the IP address that is assigned to the wired connection.

PMC Login Caveats

Be aware of the following login caveats when you use the PMC:

- The Cisco IPICS system allows only one instance of the PMC application to be open and only one user to be logged in to the PMC application on the client machine at a given time.
- If you need to log in to a PMC on a given client machine that already has another PMC user logged in, the original user must first log out of the application.
- A PMC user can log in to an unlimited number of different PMC applications at the same time; however, Cisco IPICS supports only the most recent PMC instance for use with the direct two-way and direct dial channel features. For more information about these features and other feature enhancements, see the "Cisco IPICS PMC Enhancements" section on page 63.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently. See the "License Guidelines" section on page 95.

Using the PMC in Offline Mode

The following information pertains to accessing and using the PMC in offline mode:

- If the connection to the server goes offline, the PMC enters offline mode with the current list of channels; this mode allows you to continue to communicate during periods of server downtime. You must have at least one successful login to the server before you can use the PMC in offline mode.
- After the server returns to an online state, you may encounter an invalid user or password error when you try to log in to the PMC. This situation may occur if the PMC attempts to connect to the server while the server database is being restored. In this case, the login dialog box may display several times until the server database has been fully restored.
- If the RMS entries become changed while you are running the PMC, your SIP-based channels may become disconnected. The PMC retrieves the updated channel list, with the newly-allocated SIP channels, after successful login to the server.

PMC Account Lockout and Password Expiration Guidelines

The following guidelines apply to the account lockout and password expiration features:

- If you incorrectly enter your password multiple times, such that you exceed the maximum number of consecutive invalid login attempts as configured in the server, your user account may be locked. In this case, the PMC does not allow you to log in to the system. A message displays to alert you to contact your system administrator to unlock your user account.
- If the number of consecutive invalid login attempts has been exceeded while you are already logged in to the PMC, the PMC allows you to continue to use the password for your current session. The PMC does not allow additional logins, however, until your user account is unlocked or your password is reset.
- If the number of consecutive invalid login attempts has been exceeded while you are logged in to the PMC via offline mode, the PMC allows you to continue to use the password after it returns to online mode.The PMC does not allow additional logins, however, until your user account is unlocked or your password is reset.
- If your password has expired, the PMC does not allow you to log in to the system until after you have changed your password. To change your password, log in to the Cisco IPICS server and navigate to **Home > My Profile** to enter your old and new passwords.

- If your password expires while you are logged in to the PMC, the PMC allows you to continue to use the password for your current session. You must change your password before the next login.
- If your password expires while you are logged in via offline mode, the PMC allows you to continue to use the password after the PMC returns to online mode. You must change your password before the next login.

PMC Channel Indicators and States

The PMC channels use the following traffic indicators and may appear in the states that are described in Table 14.

- Receive indicator —This graphical indicator blinks green when you receive traffic and remains illuminated for several seconds after the receive transmission has ended.
- Transmit indicator—The PTT channel button highlights and changes color to indicate that you are transmitting traffic. The touch screen skins include a graphical indicator that blinks red when you are transmitting traffic.

Note When the channel appears dimmed, the PMC is not transmitting traffic.

Table 14 Cisco IPICS PMC Channel States

Channel State	Description
Activating	The Activate button appears highlighted.
Activated	The PTT channel button and volume indicator appear highlighted.
Not Activated	No PMC buttons appear highlighted; channels appear in blueprint mode.
Disabled	No PMC buttons appear highlighted; you cannot activate the channel.
Unassigned	No PMC buttons appear highlighted; you cannot activate the channel.
Listen-only	The PTT channel appears dimmed; you can listen but not talk.

Table 14 Cisco IPICS PMC Channel States (Continued)

Channel State	Description
Secure	The secure indicator displays and all PMC buttons are functional.

- Channels may include visual indicators, such as labels, channel types, and specific colors to provide unique identification.
- The PMC must be in focus when you transmit via the All Talk or PTT buttons.

Optimizing Your Audio on the PMC

The following tips can help to enhance voice quality when you use the PMC:

- Use a high-speed connection when you use the PMC; a slow-speed connection may affect voice quality.
- Use the “Optimize for low bandwidth” option when your channel connects via a low bandwidth/high latency link.
- Try to limit the use of applications that consume high-CPU and high-network bandwidth on the PMC client machine at the same time that you use the PMC.
- To limit echo, check to ensure that you are using the preferred or default sound devices in the Windows audio settings.
- Use a high-quality headset and microphone for enhanced voice quality.
- For proper operation, connect a USB DSP headset to the client machine before you launch the PMC; otherwise, you will need to restart the PMC.
- Check the placement of your microphone so that it is positioned about 2 to 6 inches from your mouth.
- Ensure that the microphone is not set to mute. Check the settings in Windows and check that the mute button is not engaged on the headset device.
- Check for microphone availability. If the microphone is busy or if it cannot be opened by the PMC for other reasons, you may listen to active conversations but you will not be able to talk.
- Check the audio recording and playback capability of the microphone by using the Windows Sound Recorder.

- The use of a PC analog sound card and/or analog port on your laptop typically results in lower quality audio.
- If others hear an audible hum when you talk, the headset may be defective. To resolve this issue, replace the headset.
- Check the volume level on the PMC. If it is set too low, slide the bar up on the volume control indicator.
- Ensure that the output speaker volume is not muted or set too low. Check the volume settings in Windows and for the headset device and the PMC.
- Certain operating systems may not be able to run multiple voice applications concurrently and open and use the microphone at the same time. If the PMC cannot use the microphone, close the other audio application(s) and restart the PMC.
- Ensure that the QoS Packet Scheduler is installed on the PMC client machine.

For more information about voice quality, see the "Cisco IPICS Voice Quality Tips" section on page 97.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.0(1)*
- *Cisco IPICS PMC Debug Reference Quick Start Card, Release 2.0(1)*

License Guidelines

To use the Cisco IPICS solution, you must first upload and install one or more licenses that are specific for release 2.0(1).

- You can view the licensed features that are available, and the current license usage, by navigating to the **Administration > License Management > Summary** window.
  - View the License Summary pane to see total ports, current usage, and available ports. This pane also indicates whether the ops view and policy engine functionality has been licensed and enabled.
  - The total number of LMR and multicast ports, PMC, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased.

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

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

  - You can see licensing information for the Cisco IPICS Base Server License and the Policy Engine Base License to determine if the functionality has been licensed and enabled. (A separate license must be purchased to enable the policy engine features.)
  - To view usage by ops views, click the **Usage Per Ops View** tab.

Note The Cisco IPICS server checks the license count for concurrent license usage to ensure that the limits are not exceeded.

This version of Cisco IPICS also includes support for time-bound licenses. Time-bound licenses, such as evaluation or demonstration licenses, differ from purchased (non-time-bound) licenses in that they include a preconfigured license expiration date. For information about time-bound licenses, see the "License Structure and Feature Enhancements" section on page 43.

Tip The data that displays in the License browser window shows the usage at the time that the license window was last accessed. To view the most current license information, make sure that you 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 will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.

A PMC user consumes a license each time that the user logs in to a PMC session.

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

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

Additional licenses may be purchased at any time for some or all of the licensable features.

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.

Note If your server includes more than one network interface card (NIC), make sure that you configure the eth0 interface, as documented in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*. Cisco IPICS requires that you configure the eth0 interface, even if it is disabled, because the Cisco IPICS licensing mechanism performs its validation by using this NIC. Therefore, to ensure proper system operation, always configure the eth0 interface.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

Cisco IPICS Voice Quality Tips

Be aware of the following tips, which can help to ensure enhanced voice quality, when you use the PMC:

- Make sure that you use a high-quality headset and microphone, and check the placement and settings of both components, when you use the PMC. A high-quality and properly-configured headset can greatly enhance voice quality for both receive and transmit activity.

Note The use of a PC analog sound card and/or the use of the analog ports on most laptop computers typically results in lower quality voice transmissions. Therefore, Cisco recommends that you do not use your PC sound card and/or analog ports, as an alternative to a high-quality headset and microphone, for PMC communications.

- For enhanced voice quality, make sure that you plug your USB headset or audio device into a dedicated USB port instead of a USB hub. The use of USB hubs, which multiplex data from USB devices into one data stream, can result in timing issues and impact voice quality.
- If other Cisco IPICS users tell you that they hear a persistent or intermittent noise, such as an audible hum when you talk, the problem may be due to defective headset hardware. In this situation, Cisco recommends that you isolate the source of the audio quality issue by replacing the defective headset with a new, high-quality headset.
- Check your audio settings to make sure that the volume is not set too low. If the volume is set low, increase the input gain on your microphone by sliding the bar up on the volume controls to increase the volume.
- For optimum connectivity, use the most appropriate location for your connection type when you log in to the PMC. For example, if you are using a wireless connection, choose the location that correlates to wireless connectivity for your organization. You can ensure higher quality audio by choosing the appropriate connection type.
- Make sure that you always use the most recent version of the PMC. Newer versions of software often contain voice quality updates that enhance functionality.
- Be aware that a slow-speed connection, such as a digital subscriber line (DSL) connection or any slow wired link, may affect voice quality. If possible, try to use a high-speed connection when you use the PMC.
- Try to limit the use of applications that consume high-CPU and high-network bandwidth on the PMC client machine at the same time that you use the PMC. If your CPU is overburdened by other programs that are running at the same

time, there may insufficient CPU cycles for the PMC to run properly. Check the CPU activity on your PMC client machine and close any programs that do not need to be open.

- To ensure quality of service (QoS), the PMC installer attempts to install the Microsoft QoS Packet Scheduler service on each PMC client machine. The QoS Packet Scheduler ensures voice traffic priority across the network by marking each IP packet in the Differentiated Service Code Point (DSCP) with the highest value (expedited forwarding) during transmission between end points. However, this installation may not succeed if the PMC user does not have local administrative rights; in this situation, the network and the PMC client machine may drop or lose packets that are not marked by the QoS Packet Scheduler, which results in degraded voice quality. Therefore, you should check to make sure that the QoS Packet Scheduler has been installed on each PMC client machine. For additional details and information about how to check for and install the Microsoft QoS Packet Scheduler, go to http://www.microsoft.com and search for "QoS Packet Scheduler."

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*

Resolved Caveats for Cisco IPICS - Release 2.0(1)

You can find the latest resolved caveat information for this release of Cisco IPICS by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

This section includes the following topics:

- Using Bug Toolkit, page 100
- Saving Bug Toolkit Queries, page 101

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use Bug Toolkit, follow this procedure.

Procedure

Step 1 To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Log on with your Cisco.com user ID and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the “Enter known bug ID:” field.

To view all caveats for the Cisco IPICS server, go to the “Search for bugs in other Cisco software and hardware products” section, and enter **Cisco IPICS Server Software** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco IPICS Server Software**.

To view all caveats for the PMC, enter **Cisco IPICS PMC Client Software** in the Product Name field or scroll through the product name list.

Step 4 Click **Next**. The Cisco IPICS search window displays.

Step 5 Choose the filters to query for caveats. You can choose any or all of the available options:

a. Choose the Cisco IPICS version:

- Choose the major version for the major releases (such as, 1.0 or 2.0).

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information; for example, choosing major version 2.0 and revision version 1 queries for release 2.0(1) caveats.

A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

Note This option may not be available with the first release of a product.

b. Enter keywords to search for a caveat title and description, if desired.

c. Choose the Set Advanced Options, which includes the following items:

- Bug Severity level—Click the radio button that displays next to the specific severity level or the range of severity levels that you want to search for. The default specifies 1-3.
- Bug Status Group—Check the **Fixed** check box to search for resolved caveats. The default specifies Open and Fixed; to search for both open and fixed caveats, leave both of these check boxes checked.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

d. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by clicking the **Refine Search** button to submit another query and use different criteria.
- You can save your query for future use. See the "Saving Bug Toolkit Queries" section on page 101.

Note To see detailed online help about using Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

Step 1 Perform your search for caveats, as described in the "Using Bug Toolkit" section on page 100.

Step 2 In the search result window, click the **This Search Criteria** button that displays on the results window.

A new window displays.

Step 3 In the Name of saved search field, enter a name for the saved search.

Step 4 Under My Bug Groups, use one of the following options to save your defects in a bug group:

- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
- Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.

Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches, and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the **My Stuff** link to see a list of all your bug groups.)

Step 5 Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include

  - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
  - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
- **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.

Step 6 To save your changes, click **Save**.

Step 7 A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

Open Caveats for Cisco IPICS - Release 2.0(1)

Table 15 describes possible unexpected behaviors by Cisco IPICS release 2.0(1), sorted by component.

Tip For more information about an individual defect, click the associated Identifier in Table 15 to access the online record for that defect, including workarounds.

Understanding the To-be-fixed and the Integrated-releases Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the “To-be-fixed” or “Integrated-releases” fields. The information that displays in these fields identifies the list of Cisco IPICS interim versions in which the defect was fixed. These interim versions then get integrated into Cisco IPICS releases.

Some versions include identification for Maintenance Releases (MR), Service Releases (SR) and/or Engineering Specials (ES). The following examples show the version number and its mapping to MR, SR, and ES releases:

- 1.0(1.1) = Cisco IPICS release 1.0 MR1 SR1
- 1.0(3.2.1) = Cisco IPICS release 1.0 MR3 SR2 ES1
- 1.2(2.0.201) = Cisco IPICS release 1.2 MR2 ES1 (in this example, no SR was released between MR2 and ES1)

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco IPICS release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 1.0(1.008) = Cisco IPICS release 1.0(2)
- 1.1(0.012) = Cisco IPICS release 1.1(1)
- 1.1(2.020) = Cisco IPICS release 1.1(3)
- 2.0(0.029) = Cisco IPICS release 2.0(1)

Note Because defect status continually changes, be aware that Table 15 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "Using Bug Toolkit" section on page 100.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 15 Open Caveats for Cisco IPICS Release 2.0(1)

Identifier	Headline
	Server Caveats
	Component: audio-ipphone
CSCsh93823	The Cisco Unified IP Phone stops sending and receiving voice traffic if you press the channel softkey immediately after the phone receives a burst of data. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh93823
	Component: db-server

Table 15 Open Caveats for Cisco IPICS Release 2.0(1) (Continued)

Identifier	Headline
CSCsh64942	New prompts cannot be uploaded because the database space allocation has been exceeded. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh64942
	Component: installer-server
CSCsh52229	Pressing the SysRq key during the operating system installation causes a kernel panic condition on your server, which requires a hard reboot to fix. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh52229
	Component: license-server
CSCsh23903	Cisco IPICS time-bound licenses are not invalidated when the server date is changed to a past date. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh23903
	Component: log-server
CSCsi01092	On certain platforms, the Activity Log Management window may display outdated PMC log information if you change the system date to a past date. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi01092
	Component: other-server
CSCsh35692	When PMC logout functionality does not succeed because of server usage that exceeds the published specifications, PMC session and DS0 resources appear to be in use. A server restart is required to clean up these resources. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh35692
	Component: ui-server
CSCsh55884	Under certain conditions, a PMC version package upload on the server may cause the browser to become unresponsive. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh55884
	Policy Engine Caveats
	Component: ippe-admin-ui

Table 15 Open Caveats for Cisco IPICS Release 2.0(1) (Continued)

Identifier	Headline
CSCsh72788	Recorded spoken name prompts do not play out via the TUI if the default language for an ops view is different from the language that was used to record the spoken name. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh72788
CSCsh76837	After uploading standardized or customized script prompts, Cisco IPICS does not display the user ID of the actual user who uploaded the prompts. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh76837
CSCsh77264	When configuring a policy action, Cisco IPICS displays a different list of VTGs in the drop-down list box from the list that it displays via the search field. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh77264
	Component: ippe-dial-engine
CSCsh62057	Voice quality degrades on dial calls when there is high network traffic on local area networks (LAN) and no quality of service (QoS) prioritization on voice packets. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh62057
CSCsh78393	When a dial user enters an incorrect digit ID, the system does not capture the failed authentication attempt in the activity logs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh78393
CSCsh83738	The system drops a dial-out call when a dial-out user attempts to change their digit PIN (password) via the TUI. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh83738
	Component: ippe-ipics-api
CSCsh77263	Dial-out calls do not succeed because the dial engine does not correctly update license resources after you upload and apply the license file. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh77263
CSCsh84698	Multiple dial-in users may be able to talk at the same time when a channel is joined into a VTG. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh84698
	Component: ippe-policy-engine

Table 15 Open Caveats for Cisco IPICS Release 2.0(1) (Continued)

Identifier	Headline
CSCsh85367	To view scheduled run times, you must belong to the same ops view as the policy for which the trigger was set. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh85367
	PMC Caveats
	Component: audio-pmc
CSCsf15667	The PMC may connect to a remote channel by using a codec that is different from the configured codec, which can result in network bandwidth overutilization. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf15667
CSCsh57600	Sending DTMF/Alert Tones on a large number of channels at the same time causes high CPU usage, which results in distorted transmissions at the receiving end. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh57600
	Component: installer-pmc
CSCsh60379	When you downgrade a PMC version by executing the installer of an earlier version, the current installation becomes corrupted and unusable. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh60379
	Component: login-pmc
CSCsg68533	When a user is disabled via the server, the PMC window closes before the notification dialog displays. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg68533
CSCsh53034	The PMC prompts users to restart when a database restore is performed while users are logged in to the PMC. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh53034
	Component: other-pmc
CSCsd82546	A docked laptop may become unresponsive if the laptop is undocked while the PMC is running. To resolve this issue, always close the PMC before undocking the laptop. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd82546

Table 15 Open Caveats for Cisco IPICS Release 2.0(1) (Continued)

Identifier	Headline
CSCsg27114	A docked laptop displays resource warnings when the laptop is undocked while the PMC is running. To resolve this issue, always close the PMC before undocking the laptop. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg27114
CSCsh89505	Deactivating and reactivating RMS resources while the PMC is connected via SIP causes a persistent error condition. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh89505
	Component: ui-pmc
CSCsg88874	The **Settings > Channels** menu does not distinguish channels from VTGs; if the same name is assigned to a channel and a VTG, the name displays twice in this menu. To resolve, assign different names to channels and VTGs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg88874
CSCsh25628	If there is a lapse between key presses when generating DTMF tones, the silence intervals are sent as separate transmissions. Press the key sequences in rapid succession to resolve the inability of affected remote ends to interpret the reception of sequences in separate transmissions. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh25628
CSCsh35842	Unplugging or removing an active audio device (such as a headset, speakers, or microphone) while in use by the PMC may cause Windows to crash. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh35842
CSCsh41809	The PMC channel button highlights to appear that it is transmitting alert tones when the network is actually unavailable. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh41809
CSCsh44064	The channel stops transmitting when you press a mapped key and click the channel button at the same time. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh44064

Table 15 Open Caveats for Cisco IPICS Release 2.0(1) (Continued)

Identifier	Headline
CSCsh72274	The PMC incorrectly dims the channel during alert tone playout if you reorder channels while the alert tone is being played out. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh72274
CSCsh77012	The Activation button remains in a pending state, or does not display on the touch screen skin, when you reorder channels while the PMC is activating the channel. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh77012

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco IPICS release 2.0 documentation suite was released.

This section contains the following types of documentation updates:

- Errors, page 109
- Changes, page 110
- Omissions, page 110

Errors

This section includes information about errors in the Cisco IPICS Documentation suite.

- Clarification to the Managing Locations Information in the Server Online Help, page 109

Clarification to the Managing Locations Information in the Server Online Help

The “Predefined Cisco IPICS Locations” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* online help states that the server establishes a SIP-based unicast connection with the RMS. While the server facilitates this connectivity by configuring the dial peer(s) on the RMS and providing this information to the PMC, the PMC (not the server) actually establishes the SIP-based connection with the RMS.

Therefore, it is more accurate to state that the PMC establishes the SIP-based unicast connection with the RMS.

The following update provides a clarification to this section:

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

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

For more information about locations, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Changes

This section contains changes that have occurred since the original release of the Cisco IPICS release 2.0 documentation. These changes may not appear in the current documentation or the online help for the Cisco IPICS application.

There are no documentation changes that are applicable to this release.

Omissions

This section lists new and additional information that the current version of the Cisco IPICS documentation may not include:

- Update to the Procedure to Upload Spoken Name Prompts, page 111

Update to the Procedure to Upload Spoken Name Prompts

The "Uploading Spoken Names Prompts" procedure in the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* online help omits some procedural tasks that should have been included in Step 5.

The following information updates Step 5 in its entirety and replaces the information that is currently documented in the server online help.

Step 5

If you are uploading a .zip file, take the following actions to associate the prompts in that file with the appropriate Cisco IPICS resources.

When you associate prompts with a resource, you make the prompts available to resources of the designated type.

a. Click **Associate**.

   The Prompt Association window displays.

b. In the Prompts Available list, click the prompt to associate with the resource.

c. In the Resources Available list, click the resource to associate with the prompt.

   If the resource that you want does not appear in the Resources Available list, from the Resources drop-down list, choose the Cisco IPICS resource type (channel, channel group, location, ops view, policy, user, user group, or VTG) that you want, click **Search** and, in the Search Results window, locate and choose the resource or resources with which to associate the prompt.

   For information about using the Search Results window, see the "Using Search Windows" section on page 1-13.

d. Click **Associate**.

   The Prompt Association area displays the prompt name and its associated resource.

   If you want to undo one or more associations, in the Prompt Association area, check the check box next to each prompt name to disassociate and click **Remove**.

e. Repeat b, c, and d as needed to associate other prompts in the .zip file with resources.

f. To save associations that you made, click **Save**.

If you do not want to save the associations, click **Cancel**.

For more information about uploading spoken name prompts, including the complete procedure, refer to the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Release Notes for Cisco IPICS, Release 2.0(1)