Release Notes for Cisco IPICS Release 2.2(1)

June, 2009

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (Cisco IPICS) and the Push-to-Talk Management Center (PMC) release 2.2(1).

Note To view all of the release notes for Cisco IPICS, go to: www.cisco.com/go/ipicstechdocs.

Before you install Cisco IPICS, Cisco recommends that you review the "Important Guidelines" section on page 17 for information about issues that may affect your system.

For information about caveats that apply to Cisco IPICS release 2.2(1), see the "Caveats for Cisco IPICS" section on page 50.

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

www.cisco.com/go/ipicstechdocs

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

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

http://www.cisco.com/public/sw-center/index.shtml

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

The Cisco IPICS solution provides a cost-effective and highly-efficient IP standards-based solution to enable voice interoperability among disparate systems. By interconnecting voice channels, talk groups, and virtual talk groups (VTGs), Cisco IPICS bridges communications from radio networks to the Cisco IPICS Push-to-Talk Management Center (PMC) PC application and supported models of Cisco Unified IP Phones.

Cisco IPICS release 2.1(2) includes a variety of new features and functions. For more detailed information, see the "What's New in this Release" section on page 15.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.2(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*

Cisco IPICS Components

Table 1 describes the major components in the Cisco IPICS solution.

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 *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 graphical user interface (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 hosts the Cisco IPICS policy engine, which enables telephony dial functionality and maintains responsibility for the management and execution of policies and user notifications. The Cisco IPICS server supports several different user roles. For more information, see the "User Roles" section on page 6. The server also supports several different system user roles and groups. For more information, see the "System User Roles and Groups" section on page 8.
Push-to-Talk Management Center (PMC)	The PMC is a PC-based audio application that simulates a handheld radio to enable PTT functionality for PC users. It connects Cisco IPICS users via an IP network to enable participation in and monitor of one or more talk groups or VTGs at the same time. The PMC is supported for use only with the Windows XP operating system. The PMC includes several skins that allow PMC users to change the appearance of the PMC user interface. These skins may include Cisco-provided skins or a custom skin.

Table 1 Cisco IPICS System Components (Continued)

Component	Description
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. They also provide keying signals to key radio transmissions. 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.
Router Media Service	The Router Media Service (RMS) component enables the PMC to remotely attach to a VTG. This component also provides support, through its loopback functionality, for remotely attaching (combining) two or more VTGs. 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. In addition, the RMS component provides support for unicast M1:U12:M2 connection trunks. 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 *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, gateways, switches, firewalls, mobile access routers, wireless access points, and bridges.

Table 1 Cisco IPICS System Components (Continued)

Component	Description
Cisco Unified Communications Manager and VoIP Services	Cisco IPICS provides support for SIP-based interoperability with supported versions of Cisco Unified Communications Manager (formerly known as Cisco CallManager) and a Cisco router that is running a supported version of Cisco IOS with Cisco Unified Communications Manager Express (formerly known as Cisco Unified CallManager Express) to enable selected Cisco Unified IP Phone models to participate in channels and VTGs. These applications help extend the reach of PTT technology to the IP network by enabling these phones to work with Cisco IPICS as IP phone multicast client devices. They also serve as the SIP provider for the Cisco IPICS policy engine to provide SIP telephony support for calls to and from the dial engine.

Note For the most updated information about supported hardware and software that is compatible for use with Cisco IPICS, refer to *Cisco IPICS Compatibility Matrix.*

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.2(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*

User Roles

Every Cisco IPICS user is assigned one or more roles. The Cisco IPICS solution authorizes access to different features based on the role that is assigned to each user. In this way, roles help to provide system security.

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.
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.
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.
Dispatcher	The dispatcher is responsible for setting up inactive VTGs, activating the VTGs to begin groups or conferences, and adding and/or removing participants in VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and manages policies, which activate and/or deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.
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.

Table 2 Cisco IPICS User Roles (Continued)

User Role	Description
All	This role is equivalent to being assigned each of the above Cisco IPICS roles.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.2(1)*
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.2(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.

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

System User Roles and System Groups	Description
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.
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).

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

System User Roles and System Groups	Description
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 2.1(1)*
- *Cisco IPICS Server Administration Guide, Release 2.2(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*

Cisco IPICS Support Team Communications

The Cisco IPICS Support Team provides an external mailing list that you can use to obtain additional support. Send your request to physec-questions@external.cisco.com.

System Requirements

The Cisco IPICS server and the PMC require specific versions of hardware and software. 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 11

Server Requirements

Hardware

For a list of supported hardware platforms, including Cisco Media Convergence Servers (MCS), Cisco IPICS-Mobile Platforms, and Cisco routers and gateways that you can use with Cisco IPICS, refer to *Cisco IPICS Compatibility Matrix* at the following URL:

www.cisco.com/go/ipicstechdocs

Note Make sure that you install and configure Cisco IPICS only on a supported Cisco platform.

Software

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

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

PMC Requirements

Hardware

The PMC supports minimum hardware requirements that depend on the number of active PME channels that you use. For information about the PMC minimum hardware requirements that Cisco IPICS supports, refer to *Cisco IPICS Compatibility Matrix*.

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 2.2(1)*.

Software

In this release, Cisco IPICS supports the use of only Windows XP Professional SP2 on the PMC client machine.

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 Compatibility Matrix*
- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*

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 *Cisco IPICS Compatibility Matrix* at the following URL:

www.cisco.com/go/ipicstechdocs

Note Make sure that you check *Cisco IPICS Compatibility Matrix* for the most current versions of compatible hardware components and software versions for use with Cisco IPICS. Be sure to upgrade your RMS components and SIP and LMR gateways to the latest, supported releases before you install this release of Cisco IPICS.

Related Documentation

For more information about Cisco IPICS, refer to the following documentation.

Note *Cisco IPICS PMC Installation and User Guide, Release 2.2*, *Cisco IPICS Server Administration Guide*, and *Cisco IPICS 2.2(1) Resources Card (Documentation Locator)* are updated for this release. The Cisco IPICS 2.1(1) versions of the other documents apply to this release.

- *Cisco IPICS PMC Quick Start Reference Card, Release 2.1(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 2.1(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.

- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*—This document provides information about installing and using the Cisco IPICS PMC.
- *Cisco IPICS PMC Command Line Interface, Release 2.1(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.
- *Cisco IPICS Server Administration Guide, Release 2.2(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 2.1(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 2.1(1)*—This document provides tips, quick references, and usage guidelines for the Cisco IPICS server.
- *Using Cisco IPICS on Your IP Phone Quick Start Reference Card, Release 2.1(1)*—This document contains information about accessing Cisco IPICS from your IP phone and tips and guidelines for using this service.
- *Using the Cisco IPICS TUI Quick Start Reference Card, Release 2.1(1)*—This document describes the steps that you follow to dial in to, or receive a call from, the policy engine telephony user interface (TUI) and guidelines for using the system.
- *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1)*—This document contains examples of valid and invalid radio control and signaling descriptor file entries and guidelines for creating these entries.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(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 2.1(1)*—This document provides tips and quick references for installing and upgrading the Cisco IPICS server.
- *Cisco IPICS Troubleshooting Guide, Release 2.1(1)*—This document contains reference material about how to maintain and troubleshoot the Cisco IPICS system.

- *Release Notes for Cisco IPICS Release 2.2(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 2.2(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*— 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:

www.cisco.com/go/ipicstechdocs

What's New in this Release

Cisco IPICS release 2.2(1) includes the following features:

- Serial radio control of EF Johnson and iDEN radios—Users who are working from either the Cisco IPICS Administration Console or the Cisco IPICS PMC can remotely control radio functions. The functions include secure transmit mode, scanning, monitoring, and changing channels or talk groups, and initiating private (unit-to-unit) calls and dynamic group calls. Cisco IPICS can also detect changes in radio state, including talker ID and emergency "man down" signals. This features provides enhanced interoperability to Motorola SmartNet/SmartZone, P25 and Sprint/Nextel radio networks.
- Cisco IPICS Server Web Services Application Programming Interface (API)—Third-party application developers can access many Cisco IPICS server administrative functions and policy engine functions. This capability enables the integration of Cisco IPICS push-to-talk services into higher level applications such as command and control, dispatch, notification, and physical security applications. Examples of Web Services API functions include:
  - Create, delete, activate—VTG
  - Enable, disable—User, channel, VTG

  - Activate—Channel, VTG
  - GetStatus—User, channel, VTG, policy
  - Execute policy
  - Notification
- Cisco IPICS notification enhancements:
  - Text-to-speech—Cisco IPICS now supports automatic text-to-speech conversion so that notification requests can more easily be customized by the requesting operator or application. This feature requires a third-party text to speech server, such as Nuance.
  - IP phone notification to users across multiple Cisco Unified Communications Manager servers.
- PMC enhancements:
  - USB foot pedal support—A user can minimize the PMC application and perform push-to-talk (PTT) actions by using a programmable USB-based foot pedal or desktop PTT device. This feature can be useful in dispatch situations where a dispatcher is busy talking on the phone and entering incident information and might find it convenient to use a foot pedal to activate the PMC PTT button.
  - 50 channel PMC—A PMC skin with 50 channels on a single window is available.
- Support for Cisco Unified Communications Manager 7.x.
- Support for Cisco Unified IP Phone 7925g.

Important Notes for this Release

The following sections provide important information for this Cisco IPICS release:

- Error when Updating the ExampleToneSet.xml Descriptor, page 17
- IP Phone Notification Issue, page 17

Error when Updating the ExampleToneSet.xml Descriptor

The following error message appears when you attempt to update the ExampleToneSet.xml descriptor for the first time:

```
The descriptor name in new descriptor file does not match with
existing name. Please correct the name and try again.
```

Take these actions from the Cisco IPICS Administration Console to work around this issue:

Step 1 Choose **Configuration > Descriptors**, click the **ExampleToneSet.xml** link, and click **Save**, and put a copy of this descriptor on your local disk.

Step 2 Click the radio button next to the ExampleToneSet.xml link, click **Delete**, then click **OK** to delete this descriptor from the Cisco IPICS server.

Step 3 Add the ExampleToneSet.xml descriptor as a Tones descriptor type.

IP Phone Notification Issue

The Cisco Unified Communications Manager configuration for IP phone notification is not restored after an upgrade from Cisco IPICS 2.1(1) SR2 to Cisco IPICS 2.2(1). In this case, you must manually configure the Cisco Unified Communications Manager credentials in the Cisco IPICS 2.2(1) Administration Console so that IP Phone notification works properly.

Important Guidelines

The following sections provide guidelines for using Cisco IPICS:

Server Installation Guidelines

This section contains information about the guidelines that apply to Cisco IPICS 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 2.1(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 following command:

  [root]# **ifconfig eth0**
- 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 may use valid Cisco IPICS release 2.x license(s) with release 2.2(1).
- 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 the 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 and Cisco IPICS-Mobile Platform. You can check the amount of memory that is installed on your hardware platform by entering the following command from the root user account:

  [root] **#top**

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

  ```
  Mem:  2055448k av, 1490160k used,  565288k free, 0k shrd,  142344k
  buff
  ```

  To exit, press **Ctrl-C**.
- 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 before you install the operating system.
- 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 the enforcement of password complexity, or strong passwords, that must adhere to the following 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 Cisco IPICS server software installation program uses 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

    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 2.1(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.
- 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. (The options that the installer displays may differ depending on the current software version that is running on your system.)
  - Install—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. and navigate to **PMC Management > PMC Installer**. 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 2.1(1)*
- *Cisco IPICS Server Administration Guide, Release 2.2(1)*

Server Upgrade Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.2(1) server upgrade procedures.

As a best practice, make sure that you adhere to the following guidelines when you perform Cisco IPICS server installation and upgrade 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 *Cisco IPICS Compatibility Matrix*.

- Make sure that you have the installation CDs that pertain to both the Cisco IPICS release 2.2(1) server software and the Cisco IPICS release 2.0(1) operating system software.
- Before you upgrade your system, make sure that you have available another Linux-based server or a Windows-based PC or server to back up your data.
  - To back up your data files to a remote Linux-based server that supports the Linux Secure Copy (scp) command, use the remote host option.
  - To back up your data files to a remote host that does not support scp, such as a Windows-based PC or server, 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.
- Follow the sequence of steps to upgrade the operating system (if necessary) and server software, as documented in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.
- Make sure that you have valid license(s) for this release. This release supports the use of valid Cisco IPICS release 2.0(x) license(s).

When you upgrade your system, be aware that the options that the installer displays may differ depending on the current software version that is running on your system:

- When you run the Cisco IPICS installer and it does not detect an existing installation of the Cisco IPICS server software, the installer does not display any installation and/or upgrade options (Install/Upgrade/Quit). In this situation, the installer automatically invokes the install option and installs the Cisco IPICS server software on your system.
- When you run the Cisco IPICS installer and it detects an existing version of the Cisco IPICS server software that is part of the supported upgrade path, the installer displays the full installation menu; that is, Install/Upgrade/Quit.
  - If you choose the Install option in this situation, the installer removes the existing version of the Cisco IPICS server software and installs the new version of software.

Note Be aware that your data is not preserved during this process. Therefore, make sure that you first back up your data before you perform a new installation.

  - If you choose the Upgrade option, your data is preserved and your system is upgraded to the latest version.
- When you run the Cisco IPICS installer and it detects an existing version of the Cisco IPICS server software that is not part of the supported upgrade path, a warning message displays to inform you that your data will be lost if you proceed.
  - If you choose to proceed, the installer invokes the install option and installs the Cisco IPICS server software on your system.

Note Be aware that your data is not preserved during this process. Therefore, make sure that you first back up your data before you perform a new installation.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*
- *Cisco IPICS Compatibility Matrix*

Backup and Restore Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.2(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 24.

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.
- For optimum performance, Cisco recommends that you back up your database during periods of low activity or other off-peak hours. If you perform a backup during periods of high activity, the length of time that it takes to complete this operation may be significantly increased.
- 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.
  - 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; then, use the SSH Secure Shell Client software, or similar software, to perform a secure copy (scp) to the Windows-based machine.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.2(1)*

PMC Installation and Upgrade Guidelines

Be aware of the following PMC version guidelines:

- Cisco IPICS does not support the use of previous PMC releases with a Cisco IPICS release 2.2(1) server. That is, you must use PMC release 2.2(1) with a Cisco IPICS server that also has release 2.2(1) installed.
- When you upgrade the Cisco IPICS server to the current release, the existing version of the PMC installer is removed automatically. The next time a PMC user logs into the Cisco IPICS, the PMC receives a forced upgrade. If you do not want the system to perform this forced upgrade, review options for handling upgrades in *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*. For additional assistance or instructions about how to obtain a specific version of the PMC installer, contact the Cisco Technical Assistance Center (TAC).
- When a PMC that is running version 2.0(2) or earlier logs in to a 2.2(1) server, Cisco IPICS forces the PMC to upgrade to the 2.2(1) supported version.

- If you try to use a pre-2.2(1) version of the PMC with a server that has release 2.2(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 2.2(1) version of the PMC.
- Support for full PMC upgrades (including PMC online help and skin files) between major releases, such as 2.0 and 2.1, requires that you uninstall the 2.0 PMC and then install the 2.1 PMC by accessing the server via your browser. This action allows for the installation of the latest PMC online help and skin files.

This section includes information about the guidelines that apply to Cisco IPICS release 2.2(1) PMC installation and upgrade procedures:

- 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 11.
- To obtain the PMC application for installation on your client machine, access the Cisco IPICS server and download the software from the **Home > Download PMC** window.
- The PMC installation involves downloading the self-extracting PMC installation program, which includes the PMC installation and configuration files along with the PMC skins. If you are authorized to use alert tones, the PMC installation program may also include alert tones (or they may be downloaded separately).
- When you install the PMC application, 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**.
- You do not need to be connected to the server to install the PMC application software.
- If you have an existing version of the PMC on your client machine, make sure that you close the PMC application before you install a new version.
- 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.

- You do not need the fully executable file to completely update the PMC. The PMC automatic upgrade 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.
- Cisco IPICS provides the capability for the PMC to log in to the primary or 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 retrieves your configuration data from the Cisco IPICS server, which maintains the most current information.
- 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 Cisco Security Agent documentation at the following URL: http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*

Upgrading to Cisco IPICS Release 2.2(1)

If your Cisco IPICS server is running release 2.0(2) SR1 or 2.1(1) SR2 and the 2.0(1) operating system, you can upgrade your server to release 2.2(1) by using the Cisco-provided CD-ROM, or by downloading the binary install file that is available for this upgrade at this location:

http://tools.cisco.com/support/downloads/go/Model.x?mdfid=282636727&mdfLevel=Software%20Version/Option&treeName=Cisco%20Physical%20Security&modelName=Cisco%20IPICS%20Release%202.2&treeMdfId=280588231

If the Cisco IPICS 2.2(1) installer does not present the upgrade option, the release that you are running cannot be upgraded to release 2.2(1). In this case, choosing the Install option will result in a loss of configuration data.

If you are running a Cisco IPICS 2.0 release that is earlier than 2.0(2) SR1 or a 2.1 release that is earlier than 2.1(1) SR2, you can upgrade to the 2.0(2) SR1 or 2.1(1) SR2 release. Then you can upgrade to release 2.2(1). In this case, you cannot restore data that is backed up. Use the upgrade procedure to migrate data.

Tip To verify which versions of Cisco IPICS are compatible for upgrade, refer to the refer to most recent version of the *Cisco IPICS Compatibility Matrix* at http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

When you upgrade your Cisco IPICS server software, make sure that you do not disconnect your SSH session during the upgrade process. If your SSH session becomes disconnected, you may need to reinstall the software or perform other actions to recover. For detailed procedures about upgrading your server software, refer to *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.

For guidelines about Cisco IPICS server installation and upgrade procedures, see the "Server Installation Guidelines" section on page 18 and the "Server Upgrade Guidelines" section on page 21.

Where to Find More Information

- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*
- *Cisco IPICS Compatibility Matrix*

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, the following URL:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

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 2.2(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 Use and Licensing Guidelines

[This section includes information about Cisco IPICS use and licensing guidelines. It includes the following topics:

- Server Usage Guidelines, page 32
- PMC Use Guidelines, page 39
- License Guidelines, page 45

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:

- By default, the Administration Console times out after 30 minutes of non use. When a timeout occurs, you are prompted to log back in.

Note You may configure this session timeout period for a different duration by accessing the **Administration > Options** window and entering a new value in the Cisco IPICS Session Timeout Period field.

- 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.
- By default, 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.
  - You may configure this setting for a different timeout value by accessing the **Administration > Options** 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.
- The 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, radios, descriptor files, channels and channel groups, users and user 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 Cisco IPICS resources, such as channels, users, and VTGs, display in lists in the Administration Console. These lists include check boxes that you can check to select resources for which to perform certain functions. Most resource lists include a check box at the top of the list that allows you to select all resources at one time.
- Many of the Administration Console windows include drop-down 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 *Cisco IPICS Server Administration Guide, Release 2.2(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 23.
- 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 Communications Manager (formerly known as Cisco Unified CallManager) or Cisco Unified Communications Manager Express (formerly known as Cisco 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.
- Cisco IPICS provides connection support for both multicast and unicast communications. The Cisco IPICS server contains the associated connection configuration, which correlates to locations, to determine how users should connect.
  - 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. See Table 4 on page 36 for a description of these locations.
- 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.
  - Inform new PMC users about how best to communicate when using the Cisco IPICS solution. For more information, see the "PMC Use Guidelines" section on page 39.
- 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.

  Table 4 provides a description of the ALL and REMOTE locations.

Table 4 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 4 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 2.2(1).*

Table 5 provides a summary of Cisco IPICS access types and connections.

Table 5 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 2.2(1).*

PMC Use Guidelines

Note Cisco IPICS only supports the use of PMC release 2.2(1) with a Cisco IPICS server that also runs release 2.2(1). When a PMC that is running version 2.0(2) or earlier logs in to a 2.2(1) server, Cisco IPICS forces the PMC to upgrade to the 2.2(1) supported version.

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

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 44.
- To talk on a channel, click and hold the push-to-talk (PTT) button before you speak. Or, or click latch if you have permission.
- When you are done talking, release the left mouse button to return to listen-only mode.
- 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.

- 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 43 and refer to the *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)* for the various channel states and appearances on the PMC.)
- Your ability to use certain PMC features, such as latch, multiselect, alert tones, DTMF, and All Talk, depend on the permissions that are configured for you in the server.
- Whenever Cisco Security Agent (CSA) prompts you, click **Yes** to grant permission and continue.

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 30.
- 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.
- 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 supports 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.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently. See the "License Guidelines" section on page 45.

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 6.

- 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 radio console and touch screen skins include a graphical indicator that blinks red when you transmit traffic.

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

Table 6 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.

Table 6 Cisco IPICS PMC Channel States (Continued)

Channel State	Description
Listen-only	The PTT channel appears dimmed; you can listen but not talk.
Secure	The secure indicator displays and all PMC buttons are functional.

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

For more information about channel states, refer to *Cisco IPICS PMC Installation and User Guide, Release 2.2(1).*

Optimizing Your Audio on the PMC

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

- For optimum voice quality, 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 minimize echo, check to ensure that you use the preferred or default sound devices in the Windows audio settings.
- The use of a PC analog sound card and/or analog port on your laptop typically results in lower quality audio.
- Use a high-quality headset and microphone for enhanced voice quality.
- For proper operation, connect a USB DSP headset to the PMC client machine before you launch the PMC; otherwise, you will need to restart the PMC.
- If other users hear an audible hum when you talk, the headset may be defective. To resolve this issue, replace the headset.
- 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.
- 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.
- Ensure that the QoS Packet Scheduler is installed on the PMC client machine.
- Be aware of the following radio skin caveats, which may affect functionality and/or voice quality:
  - When the PMC connects via SIP, radio function is limited; RFC tones may get translated into audible inband tones and cause the physical radio to retune.
  - The voice replay feature plays back audio on the radio channel that was tuned (active) at the time of capture.
  - Mixing remote and multicast PMC users on the same radio may cause voice quality and operational issues.

For more information about voice quality, refer to *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.1(1)*
- *Cisco IPICS PMC Debug Reference Quick Start Card, Release 2.1(1)*

License Guidelines

To use the Cisco IPICS solution, you must first upload and install one or more licenses. Cisco IPICS 2.0 and 2.1 licenses may be used with Cisco IPICS release 2.2(1). Cisco IPICS does not overwrite older license files with newer license files.

- As a best practice, Cisco recommends that you take the following action when license changes occur, such as when you replace a time-bound (demonstration or evaluation) license with a permanent license:
  - Make sure that you remove the old license file(s) from the directory where Cisco IPICS stores the license(s).

    For information about deleting time-bound licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.
  - After you remove the old license(s), restart the server by entering the following command:

    [root]# **service ipics restart**
- To view the licensed features that are available, and the current license usage, navigate 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 and 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. When functionality is enabled, the License Management window displays “Licensed.” (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.

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 2.1(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 2.1(1)*
- *Cisco IPICS Server Administration Guide, Release 2.2(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.2(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.”
- The following caveats are applicable when you use the radio console skin and may affect functionality and/or voice quality:

- When the PMC connects by using SIP, radio functionality is limited because the RMS does not pass the RFC tones. Instead, the RFC 2198 and RFC 2833 packets sent by PMC clients get translated by the RMS loopback interface into audible inband tones. These tones may cause the physical radio to retune.
- The voice replay feature records and plays back any audio that is played out to the speakers across radio channels. That is, the voice replay feature records and plays back audio according to the channel that was tuned (active) at the time of capture. The voice replay feature does not track or provide indication of the channel that was active when the audio was received.
- Control and signaling tones that are normally not audible to multicast users may become audible to participants in VTGs and those who are connected remotely. This situation can cause some tones to play out for the entire duration of the audio.
- Mixing remote and multicast PMC users on the same radio may cause voice quality and operational issues. For more information, refer to the "Communicating with Cisco IPICS Users via Tone-Controlled Radios" section in the "Using the PMC Application" chapter in *Cisco IPICS PMC Installation and User Guide, Release 2.2(1).*

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.2(1)*

Caveats for Cisco IPICS

Use the Bug Toolkit to find information about the caveats (bugs) for the current release of Cisco Video Surveillance Media Server, including a description of the problems and available workarounds. The Bug Toolkit lists both open and resolved caveats.

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

Step 4 To look for information if you do not know the bug ID number:

a. Choose **Physical Security** from the Select Product Category menu.

b. Choose the desired product from the Select Product menu.

c. Choose the version number from the Software Version menu.

d. Under Advanced Options, choose **Use default settings** or **Use custom settings**. The default settings search for severity 1, 2 and 3 bugs, open and fixed bugs, and only bugs containing bug details. Use the custom settings to change the severity and status parameters, or to search for keywords within the bug headline and description.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco IPICS release 2.1 documentation suite was released.

This section contains the following types of documentation updates:

- Errors, page 52
- Changes, page 52
- Omissions, page 52

Errors

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

Correction to the Channel Status Information in the Cisco IPICS Server Administration Guide and the Server Online Help

Table 2-2 in the "Viewing and Editing Channel Details" section in the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* and in the server online help incorrectly reflect a channel status of "inactive." This section should reflect the available channel states, which include active, enabled, and disabled.

Table 2-1 in the "Understanding the Channels Window" section in the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* and in the server online help correctly reflect the channel states as active, enabled, and disabled.

For more information about the applicable channel states, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(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:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

\

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

Release Notes for Cisco IPICS, Release 2.2(1)