Release Notes for Cisco IPICS Release 2.1(1)

September 28, 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 2.1(1).

Note To view all of the release notes for Cisco IPICS, go to: http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Before you install Cisco IPICS, Cisco recommends that you review the "Important Notes" section on page 42 for information about issues that may affect your system.

For a list of the open and resolved caveats for Cisco IPICS release 2.1(1), see the "Resolved Caveats for Cisco IPICS - Release 2.1(1)" section on page 64 and the "Open Caveats for Cisco IPICS - Release 2.1(1)" section on page 70. 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:

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

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

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

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(1) includes enhancements to provide support for Tone Remote Control (TRC) functionality. Tone Remote Control (also known as Tone Control) refers to the use of a sequence of audible tones (inband tone sequences) to control a radio that is connected to a Land Mobile Radio (LMR) gateway (typically a base station). This control can be used, for example, to tune the radio to a different frequency (change the channel).

Note Be aware that the version of Cisco IOS software that is required to support the tone remote control functionality may not be available when Cisco IPICS release 2.1(1) becomes available. For updated availability information, refer to the *Cisco IPICS Compatibility Matrix*.

In this release, Cisco IPICS provides support for tone-controlled radios by enabling the definition of radio channels in the Cisco IPICS server configuration and implementing a 36-channel radio console skin in the PMC.

Each radio channel that you define in the server represents a physical radio that can be configured with one or more operational tones, including high level guard tones (HLGT), function tones (such as channel select and channel scan), and low level guard tones (LLGT). The high level guard tone is usually the first tone in a preamble, or the sequence of tones that precedes a transmission. The high level guard tone is set at high volume to alert the radio that a function tone will follow. The function tone follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. The low level guard tone is used as a hold tone or keying tone.

This radio-specific enhancement enables the PMC to send RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis. RFC 2833 dual-tone multifrequency (DTMF) is supported for the generation of DTMF signals when these signals have been previously configured in the server via the tone descriptors and associated to Cisco IPICS channels.) RFC 2198 and RFC 2833 improve reliability by guaranteeing that tones play out in the proper sequence and by making the system more resilient to packet loss conditions.

Although the Cisco IPICS server manages the resources and notifies the PMC and other components about defined radio channels and radio control tones, only the PMC can interoperate with and control these radios. When the PMC transmits on a defined radio channel, it generates defined radio control tones via RFC 2833 packets that flow to the LMR gateway. In the LMR gateway, these encoded packets are converted into audible tones and output via the configured E&M interface to the physical radio.

With these enhancements, Cisco IPICS release 2.1(1) extends the Cisco IPICS solution by allowing customers to more completely use their radios with Cisco IPICS.

Note You can find information about RFC 2198 and RFC 2833, along with various Requests for Comment (RFCs), by accessing the RFC repository that is maintained by the Internet Engineering Task Force (IETF) at the following URL: http://www.ietf.org/rfc.html.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.1(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.1(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 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 7. The server also supports several different system user roles and groups. For more information, see the "System User Roles and Groups" section on page 9.
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 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, 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 the *Cisco IPICS Compatibility Matrix.*

Where to Find More Information

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

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 12
- PMC Requirements, page 13

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 the *Cisco IPICS Compatibility Matrix* at the following URL:

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Note Make sure that you install and configure Cisco IPICS release 2.1(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*.

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 the *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 2.1(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 2.1(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 the *Cisco IPICS Compatibility Matrix* at the following URL:

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

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. 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 this release of Cisco IPICS, refer to the following documentation:

- *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 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 2.1(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 2.1(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 2.1(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 2.1(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/en/US/products/ps7026/tsd_products_support_series_home.html

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 22
- PMC Installation and Upgrade Guidelines, page 24
- Cisco IPICS Security Enhancements, page 26
- Cisco IPICS Server Enhancements, page 27
- Cisco IPICS PMC Enhancements, page 33
- Upgrading to Cisco IPICS Release 2.1(1), page 39
- Support for Additional Hardware Platforms, page 40
- Support for Additional Cisco Unified IP Phone, page 40
- Update to the Cisco IPICS RMS Configuration, page 41

Server Installation Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.1(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 2.1(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 2.0(x) license(s) for use with release 2.1(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 2.1(1)*

Server Upgrade Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 2.1(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 the *Cisco IPICS Compatibility Matrix*.
- Make sure that you have the installation CDs that pertain to both the Cisco IPICS release 2.1(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 2.1(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 23.

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 2.1(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 2.1(1) server. That is, you must use PMC release 2.1(1) with a Cisco IPICS server that also has release 2.1(1) installed.
- When a PMC that is running version 2.0(2) or earlier logs in to a 2.1(1) server, Cisco IPICS forces the PMC to upgrade to the 2.1(1) supported version.
- If you try to use a pre-2.1(1) version of the PMC with a server that has release 2.1(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 2.1(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 2.1(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 13.

- 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 the 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 2.1(1)*

Cisco IPICS Security Enhancements

This release of Cisco IPICS includes the following server security enhancements:

- Cisco IPICS now supports password encryption when you perform a remote host backup operation.
- For additional security, this release now accepts the establishment of only Secure Shell (SSH) version 2 connections to the Cisco IPICS server and has removed support for SSH version 1.
- Reconfiguration that sets the ForwardX11 parameter to “no” to prevent the SSH client from automatically sending X-Windows system information across the network.
- Requirement to use medium or strong encryption ciphers (128 bits or greater) within Transport Layer Security (TLS) sessions and discontinuance of support for weak and null encryption ciphers (less than 128 bits).
- Modification of the server debug log file to no longer display dial-in user ID and password values.
- To protect data integrity, all Cisco IPICS server components now use the restricted ipicsadmin account to access the Informix database.

Cisco IPICS Server Enhancements

This section describes the new features and enhancements that this release implements and includes information about the following topics:

Support for Tone-Controlled Radios

The Cisco IPICS server has been enhanced to include the following new features in support of tone-controlled radios:

- Support for a new radio channel connection type in the Cisco IPICS Administration Console.
- Capability to define a tone-controlled radio in the Cisco IPICS server and enable assignment of a radio channel connection type to an end-user.
  - Each radio channel that the administrator defines in the server represents a physical radio that can be configured with one or more tone sequences.
  - These tone sequences are used to control various tones and functionality on the radio.
  - Each tone sequence includes parameters, such as the frequency or frequencies, volume (RF power), and duration, that are necessary to generate a specific tone and invoke an action on the radio.
- Ability to associate and disassociate a tone-controlled radio with user(s).
- Enhancement to channel and user associations to include radio configuration and enable system administrator management of the following entities via the Cisco IPICS server Administration Console:

  - Radio Profile Management—To manage radio profiles, navigate to the **Configuration > Radios** window. This functionality includes the ability to define multiple radio profiles for a single channel so that the same channel can reside on multiple radio profiles. This window includes support for list pagination.
  - Tone/Signal Management—To manage tones and signals, navigate to the **Configuration > Channels >** <*channel name*> **Associations > Signals** window.
  - Channel Association with Radio Profile—To associate channels with radio profiles, navigate to the **Configuration > Channels >** <*channel name*> **Associations** window.
  - User Association with Radio Profile—To associate users with radio profiles, navigate to the **User Management > Users >** <*user name*> **> Associations > Radios** window.
- Capability to add, update, or delete a radio descriptor file or a tone descriptor file via the Cisco IPICS server Administration Console:
  - Radio/Tone Descriptor Management—To manage radio and tone descriptor files, navigate to the **Configuration > Descriptors** window. The Cisco IPICS server includes sample radio and tone descriptor files that you can use as a guide if you need to create additional descriptor files for your specific radio hardware. This window includes support for list pagination.
  - Radio descriptors are .xml files that contain commands that control radio functionality. For each radio capability, the radio descriptor defines the tones that are sent to the radio to enable or disable that capability. The radio descriptor files include channel selectors, which are used to change the frequency on a radio, and control functions, which may be stateful (such as power settings and encryption on/off) or simple/momentary controls, such as monitor and scan.
  - Tone descriptors are .xml files that define a sequence of momentary controls and signals that transmit over-the-air. These tones and signals can be associated with one or more Cisco IPICS channels. Unlike momentary controls, signals do not cause the radio to change configuration; instead, signals are treated like voice and transmitted over the currently-tuned radio channel frequency.
  - Cisco IPICS supports only RFC 2833 for tone control sequences and a maximum of six tones per control sequence.

    - Cisco IPICS supports a maximum of six consecutive RFC 2833 tones for signaling tone sequences. However, you can enter additional tones by separating them with a pause (such as 1 millisecond (ms) or a DTMF entry (such as digit 1 for 200 ms). There is no limit to the number of DTMF entries that are allowed in a signaling tone sequence, and these entries can co-exist with RFC 2833 tone entries.
    - When you send DTMF digits, be sure to configure a delay between the digits as required by local specifications. Most US specifications require an interdigit delay of at least 40 ms.
    - Pauses are defined by a tone with a frequency of zero; for example, <Rfc2833Tone db="0" frequency="0" duration="40" />
- Enable the configuration of specific user radio permissions:
    - The system administrator can select the level of permission that pertains to each individual radio channel selector button.
    - Because channel permissions are configured separately from radio channel selector button permissions, PMC users who have access to a radio may be able to use all, or only some, of the channel selector buttons.
    - The server configuration determines the order in which the PMC displays the radio channel selector buttons on the PMC.
    - If the system administrator does not configure any radio channel selector buttons for a user, the user is able to listen to the channel but is not able to change the channels or control the radio.

Cisco IPICS Policy Engine Notification Enhancements

The Cisco IPICS policy engine implements the following new features and enhancements in this release:

- The Cisco IPICS policy engine includes a new notification action, which sends notifications to designated recipients who are not configured as Cisco IPICS users and provides them with information that you specify.

Note This feature is not configurable via the Cisco IPICS Administration Console. Instead, you must configure one or more dedicated dial servers, which are Cisco IPICS servers that perform the dial-out functionality to the external recipients.

The external notification action performs the following actions:

- Simultaneously calls many external users at telephone numbers that Cisco IPICS obtains from a file that you specify.

  To designate a recipient list, you create an .xml file that contains the telephone numbers of all users who you want to contact.

- Plays a designated message to each user who answers the call.

  To designate a message file, you create a .wav file that contains the message that you want to play to the recipients.

To invoke the external notification, you send an HTTP request or a Common Alerting Protocol (CAP) .xml file to the appropriate dedicated dial server.

- Captures results of each call in a log file that you can review at any time.

- In this release, the Cisco IPICS policy notification feature includes the following new action types:
  - IP Phone Notification—This type of notification displays a designated message on supported Cisco Unified IP Phones.
  - Dial Notification—This notification calls out to designated users and plays the selected prompt or sends a message to the Cisco Unified IP Phones of the designated users and plays automatically on the speaker of the phone.
  - Talk Group Notification—This type of notification plays out the selected prompt to all users in the VTG.
- When you configure a new policy notification action, the Message notification types now include the following options: Email, IP Phone Text, Dial, Talk Group, and Dial Engine Script.
- Cisco IPICS now includes the capability for the dispatcher to enter specific notification subject and body text when sending a notification to participants from the **VTG Management > Virtual Talk Groups** window.
- This release includes the ability to export executing and executed policy history to a Microsoft Excel format. To download the execution status history, navigate to the **Policy Management > Execution Status** window and click the **Download Execution Status** button. You can either open the file or save the file to a location of your choice and then open it by using Microsoft Excel to view the report.

Serviceability and Usability Enhancements

This release includes the following serviceability and usability enhancements:

- The addition of server software installation history information in the **Serviceability > Diagnostics** window that includes the date and time that the current version of server software was installed along with a history of installation and uninstallation activity.
- Ability to specify a timeout period for the Cisco IPICS Administration Console browser session in the **Administration > Options** window.

  The default setting specifies 30 minutes.
- Improved system startup performance by decreasing the Cisco IPICS application installer Kudzu utility default timeout period from 3600 seconds to 30 seconds.
- The addition of Quality of Service (QoS) markings to voice packets to reduce latency and improve voice quality.
- Support for up to 50,000 users defined in the database.

Logging Updates

Cisco IPICS implements enhanced capabilities and flexibility for the Cisco IPICS activity logs by enabling the following updates:

- Updated logging capability to track the creation, removal, and update of radios and their related associations.
- Ability to parse new activity log messages from the PMC.

PMC Management Enhancement

Cisco IPICS provides support for the following PMC management enhancement in this release:

- Ability to facilitate the prestaging of PMC downloads so that users can upgrade their PMC versions before you upgrade the server software.
  - This process enhances PMC download management and alleviates the burden of long PMC downloads to all users at one time.

  - Before you upgrade the Cisco IPICS server software, you can set up a new version of the latest, supported PMC so that the PMC download process is staged.
  - When the PMC users log in and connect to the server, the latest PMC version is automatically downloaded.
  - After users have downloaded the latest PMC version, you perform the procedure to upgrade the server software. The upgrade program changes the state of the PMC from staged to recommended and makes the PMC available for use.

Cisco Unified IP Phone Enhancements

The following Cisco Unified IP Phone enhancements are included in this release:

- Capability to specify whether an IP phone times out after a configured period of inactivity, forcing the user to log in again. To configure this timeout period, navigate to the **Administration > Options** window.

  The default setting specifies 45 minutes.

  - Ability to configure whether the Cisco IPICS service requires users to log in before they access the service from a Cisco Unified IP Phone.

    You can configure the Cisco IPICS service so that it does not prompt for user login credentials on the Cisco Unified IP Phone and automatically activates a channel or VTG if only one channel or VTG is assigned.

    If the Cisco IPICS service is configured to bypass the user login and if there is only one channel or VTG that is assigned, Cisco IPICS automatically activates that channel or VTG.

    If the Cisco IPICS service is configured to bypass the user login and if there are more than one channel or VTG that is assigned, Cisco IPICS displays the list of these channels and VTGs on the IP phone.

  - On some model IP phones, the administrator may add a special parameter to the Cisco IPICS server URL configuration to enable the display of the Logout softkey while IP phone users are connected to a channel or VTG. This enhancement simplifies user operation by allowing users to access the Logout softkey from the main display screen.

Support for Network Time Protocol

In this release, Cisco IPICS provides support for Network Time Protocol (NTP) in the following situations:

- Permanent (purchased) licenses—This release of Cisco IPICS supports NTP when NTP is used with Cisco IPICS permanent licenses.
- Time-bound (evaluation or demonstration) licenses—Time-bound licenses also support the use of NTP, however, be aware that updates that alter the system date may cause the Cisco IPICS license to become invalidated if the installed license has an explicitly defined start date.

Where to Find More Information

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

Cisco IPICS PMC Enhancements

The Cisco IPICS PMC has been enhanced to include support for tone-controlled radios. This support includes enhanced functionality in the LMR gateway that enables support for RFC 2198 and RFC 2833 standard messages.

This section includes the following topics:

- Overview, page 33
- Introducing the 36-Channel Radio Console Skin, page 34
- Support for Channel Selector Buttons, page 37
- Support for RFC 2198 and RFC 2833 Packets, page 38
- Support for Anchored Channels, page 38
- Logging Updates, page 38

Overview

With this release, the PMC provides support for radio channels on the 36-channel radio console skin. (The PMC allows the assignment of up to 50 channels, but only 36 channels may be active at the same time.) A PMC radio channel supports tone control for radios. Each defined radio channel represents a physical radio that the administrator configures with one or more tone sequences. With this support, the PMC includes channel selector buttons that display within the radio channel. PMC users can use these buttons to change channels (frequencies), for signaling functionality, or to control tone sequences. (The PMC generates the necessary radio control tone sequences when PMC users press the associated button.) PMC user radio access may include all, or only some, of these buttons.

To enable this functionality, the PMC sends RFC 2198 and RFC 2833 packets on a per-channel basis. At the LMR gateway, the packets are converted into audible tones and output via the configured ear and mouth (E&M) interface to the physical radio to provide tone control for radios.

This release supports the use of only the Windows XP operating system on the PMC client machine.

Introducing the 36-Channel Radio Console Skin

The Cisco IPICS PMC has been enhanced to provide support for tone-controlled radios and introduces a new radio-centric skin. The following enhancements are included in this release:

- Introduction of the 36-channel radio console skin that includes support for up six regions (radio views) with six radio channels in each region and the ability to display a maximum of nine radio channel selector buttons per radio channel.
  - An associated indicator displays next to the currently selected channel selector button so that you know which one is in use. This indicator is dynamic; as you change your channel selection, the indicator illuminates to reflect the currently selected channel
  - The audio that you transmit and receive occurs over the specific channel (frequency) to which the radio is currently tuned.
  - Allow users to dynamically switch among up to six different radio views by the use of tabs that display along the side of the skin.
  - All radio channels can be seen via a summary list that displays along the left side of the skin.
  - This functionality provides the benefit of enabling radio users to simultaneously monitor multiple channels.

Note In this release, only the PMC can interoperate with and control the radios.

The 36-channel radio console skin includes the functionality that is described in Table 4.

Table 4 Cisco IPICS 36-Channel Radio Console Skin Functionality

Button and Menu Functionality	Description
Activation/ Deactivation Button	Activates and deactivates a channel. This button highlights and changes orientation when activated.
Volume Buttons and Volume Indicator	Increases, decreases, and displays the current volume level on the channel in a graphical format.
PTT Channel Button with Receive and Latch Indicators	Click and hold to talk. In transmission mode, this button highlights in a different color. In receive mode, the receive indicator blinks green; in transmit mode, the transmit indicator blinks red. 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.
Voice Replay Controls	Plays back buffered voice transmissions. When you use the radio console skin, the voice replay feature records and plays back audio according to the channel that was tuned (active) at the time of capture.
Channel Selector Buttons	Click to control radio channel functionality, such as tuning a channel to a different frequency or generating a specific tone to invoke an action on the radio. These buttons may consist of channel selector buttons, control buttons, or signal buttons. The PMC can display a maximum of nine buttons per radio channel.

Table 4 Cisco IPICS 36-Channel Radio Console Skin Functionality

Button and Menu Functionality	Description
Channel Select Check Box	Check to select or deselect the channel for PTT communications.
Server Status Connectivity Indicator	Dynamically displays 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 one-click access to the PMC settings menus and online help.
Select All and Deselect All Buttons	Selects and deselects all channels on the PMC (multiselect).
All Talk Channel Button	Click the All Talk channel to simultaneously talk on all of the channels that you selected.
Alert Tone Buttons	Plays out alert tones only on the channel(s) that you select.
Region Tabs	Click the tabs that display along the right side of the PMC to access different radio views. **Note** Individual radio channels can be seen via a summary list that displays along the left side of the radio console skin. This functionality provides the benefit of enabling radio users to simultaneously monitor multiple channels.
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.

Table 4 ***Cisco IPICS 36-Channel Radio Console Skin Functionality***

Button and Menu Functionality	Description
Channels Menu	Enables channel configuration via certain settings, 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.

Support for Channel Selector Buttons

This release includes support for multiple tone-controlled radio channel selector buttons that you can use to change channels, control tone sequences, or use for signaling functionality.

- Each one of these buttons may represent a different channel (frequency), such that switching channels allows you to tune to another frequency or invoke a specific action.
- When these buttons are configured for tone control, they are mapped to the available tone control sequences that are needed to control the physical radio. (A physical radio is associated to each radio channel in the server.)
- Control functions can display on the PMC as single channel selector buttons or as stateful control sequences.
  - Stateful control sequences are comprised of multiple states, where each state displays as a separate channel selector (tone control) button on the PMC. An example of a stateful control sequence is the power level of a radio. In this instance, a stateful control sequence may be defined to change the power level of a radio to high, medium, or low. Each one of these states are mapped to a distinct tone control sequence in the server and displayed as separate buttons on the PMC.

Note In this release, the PMC displays the channel selector buttons as they are received from the server. While the PMC allows you to reorder the channels on the PMC, it does not allow you to reorder the channel selector buttons that display on the radio channel in the radio skin.

Support for RFC 2198 and RFC 2833 Packets

Cisco IPICS includes the ability to send RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis, with support for the device control operations:

- Ability to change the active frequency on a tone-controlled radio—This operation enables the PMC to dynamically tune a radio channel to multiple, different frequencies. These channel selector buttons are exclusive, in that you can tune to only one channel at a time.
- Capability to enable specific stateful controls on a tone-controlled radio—A maximum of nine channel selector buttons may be displayed for radio tone control and signaling per radio channel. These buttons may be configured to include certain stateful sequences, such as transmit power settings that include high, medium, and low power states.
  - In this case, the PMC must have three channel selector buttons available to display this sequence (one for each state). If three channel selector buttons are not available, none of the states display.
- Enable momentary controls on a tone-controlled radio— Momentary tones begin to play when you press the associated button. After you press a momentary control button, the button appears to be pressed momentarily before it appears raised again.
- Transmission of momentary signaling tones—Signaling tones send audio to the radio and transmit over the air. These tones broadcast over the radio by using RFC tones and events.

Support for Anchored Channels

This release provides support for channel locations that can be anchored by skin.

- Anchored channels dock in predefined locations on the display; these skins are normally developed by systems integrators or other third party providers.
- Channels may be repositioned when you switch skins. In this case, you may need to manually reorder your channels to view them in the PMC.

Logging Updates

This release includes the following update to the PMC activity log:

- Ability to log radio control operations (such as channel changes) and radio signaling operations (such as paging) in the PMC activity log.

Where to Find More Information

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

Upgrading to Cisco IPICS Release 2.1(1)

If your Cisco IPICS server is running release 2.0(2) or 2.0(2) SR1 and the 1.0(3) operating system, you can upgrade your server to release 2.1(1) by using the Cisco-provided CD-ROM format that is available for this upgrade.

This upgrade software is available only 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 2.0(2) or 2.0(2) SR1 with the 1.0(3) operating system to upgrade to Cisco IPICS release 2.1(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/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 the *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 17 and the "Server Upgrade Guidelines" section on page 20.

Where to Find More Information

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

Support for Additional Hardware Platforms

This release adds support for additional Cisco MCS servers and Cisco IPICS-Mobile Platforms, including the Panasonic Toughbook CF-30, which supports the policy engine dial-in and dial-out telephony functionality. (This platform runs VMware and is supported only through a Cisco certified systems integrator. For additional details, please contact your Cisco sales representative.)

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

Where to Find More Information

- *Cisco IPICS Compatibility Matrix*

Support for Additional Cisco Unified IP Phone

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

- Cisco IP Communicator

Cisco IP Communicator is a desktop application that you install on your computer to enable full-featured Cisco Unified IP Phone functionality. With Cisco IP Communicator, you can place, receive, and perform other call-handling functionality, as you would with a Cisco Unified IP Phone.

With this addition, Cisco IP Communicator joins the Cisco IPICS portfolio to provide enhanced productivity and flexible call-handling capabilities.

For information about how to subscribe, access, and use the Cisco IPICS service on the Cisco Unified IP Phones, 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 Compatibility Matrix*
- *Cisco IPICS Server Administration Guide, Release 2.1(1)*

Update to the Cisco IPICS RMS Configuration

In this release, the Cisco IPICS RMS configuration must be updated to include the Cisco IOS **media-inactivity-criteria rtcp** command. This update is necessary because of a change to Cisco IOS.

The **media-inactivity-criteria rtcp** command, which is entered in gateway configuration mode, enables RTCP keepalive monitoring and specifies the use of RTCP for silence detection.

Note Be aware that this command is required to enable RTCP packet detection as the only mechanism to use for SIP media inactivity criteria and prevent the RMS from disconnecting SIP calls when no RTP packets are detected.

With this change, the updated RMS configuration includes the following command as part of Step 16 in the "Configuring T1/E1 Controllers, Interfaces, and Voice Parameters" section in the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*:

Step 16

Configure the SIP inactivity timeout by entering the following commands:

a. Router(config)# **ip rtcp report interval 5001**

This command configures the average reporting interval between subsequent Real-Time Control Protocol (RTCP) report transmissions.

b. Router(config)# **gateway**

This command enables the H.323 VoIP gateway.

c. Router(config-gateway)# **media-inactivity-criteria rtcp**

This command specifies the use of RTCP for media inactivity (silence) detection. It is required to enable RTCP packet detection as the only mechanism to use for SIP media inactivity criteria to prevent RMS disconnection.

d. Router(config-gateway)# **timer receive-rtcp 5**

This command enables the RTCP timer and configures a multiplication factor for the RTCP timer interval for SIP or H.323.

For detailed information about configuring the RMS, refer to the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 2.1(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 42
- Establishing PMC Connectivity with the RMS for SIP-Based Remote Connections, page 43
- Cisco IPICS Usage and Licensing Guidelines, page 44
- Cisco IPICS Voice Quality Tips, page 62

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/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.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 2.1(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 44
- Server Usage Guidelines, page 45
- PMC Usage Guidelines, page 53
- License Guidelines, page 59

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. For more information, see the "Serviceability and Usability Enhancements" section on page 31.
- 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 the *Cisco IPICS Server Administration Guide, Release 2.1(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 22.
- 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 5 on page 50 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 Usage Guidelines" section on page 53.
- 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 5 provides a description of the ALL and REMOTE locations.

Table 5 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 5 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 2.1(1).*

Table 6 provides a summary of Cisco IPICS access types and connections.

Table 6 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 2.1(1).*

PMC Usage Guidelines

Note Cisco IPICS only supports the use of PMC release 2.1(1) with a Cisco IPICS server that also runs release 2.1(1). When a PMC that is running version 2.0(2) or earlier logs in to a 2.1(1) server, Cisco IPICS forces the PMC to upgrade to the 2.1(1) supported version.

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

- Tips for Using the PMC, page 53
- PMC Connectivity Tips, page 54
- PMC Login Caveats, page 55
- Using the PMC in Offline Mode, page 55
- PMC Account Lockout and Password Expiration Guidelines, page 56
- PMC Channel Indicators and States, page 57
- Optimizing Your Audio on the PMC, page 58

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 58.
- 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 57 and refer to the *Cisco IPICS PMC Installation and User Guide, Release 2.1(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 43.
- 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 59.

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 7.

- 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 7 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 7 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 the *Cisco IPICS PMC Installation and User Guide, Release 2.1(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 the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.1(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(2) licenses may be used with Cisco IPICS release 2.1(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 2.1(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.1(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 the "*Cisco IPICS PMC Installation and User Guide, Release 2.1(1).*

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*

Resolved Caveats for Cisco IPICS - Release 2.1(1)

You can find the latest resolved caveat information for this release of Cisco IPICS by using Cisco 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 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://tools.cisco.com/Support/BugToolKit/

This section includes the following topics:

- Using Bug Toolkit, page 65
- Saving Bug Toolkit Queries, page 68

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

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

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

To use Bug Toolkit, perform the following procedure:

Procedure

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/

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

Step 3 You can view information about specific caveats or obtain a list of caveats by choosing from the following options:

- To access information about a specific caveat, enter the bug ID number in the Search for Bug ID: field; then, click **Go**.
- To view all caveats for Cisco IPICS, follow these steps:

a. Scroll through the Select Product Category: list and click **Interoperability Systems** or enter **Interoperability Systems** in the Select Product Category: input field.

b. In the Select Product: input field, enter keywords to filter the product name search, if desired, or scroll through the product name list and click the applicable component.

To search for caveats that pertain to the PMC, enter or click **Cisco IPICS PMC Client Software**.

To search for caveats that pertain to the policy engine, enter or click **Cisco IPICS Policy Engine.**

To search for caveats that pertain to the Cisco IPICS server, enter or click **Cisco IPICS Server Software**.

Step 4 From the Version drop-down list box, choose the applicable Cisco IPICS major software version number (such as, 1.0, 2.0, or 2.1).

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

For Cisco IPICS release 2.1 caveats, choose **2.1**.

Step 5 From the Advanced Options pane, choose from the following options:

- **Use default settings**—Click this radio button to accept the default settings.
- **Use custom settings for severity, status, and others radio button**—Click this radio button to customize the settings for bug severity, status, level of detail, date modification, and the number of results to display per page. To customize your settings, follow these steps:

a. In the Search for Keyword(s): input field, enter keywords to search for a caveat title or descriptive text, if desired.

b. In the Severity: field, check the check box that displays next to the specific severity level that you want to search for. You can choose from 1-6. The default setting specifies 1-3.

c. In the Status: field, check the check box that displays next to the status that you want to search for. To search for resolved caveats, check the **Fixed** check box. The default setting specifies Open and Fixed.

d. In the Detail Level: field, the default value specifies **Show only bugs containing bug details.** If you choose this default setting, the system returns only bugs that include release note enclosure details.

e. From the Modified Date drop-down list box, choose a date range to filter your search, if desired. The default setting specifies In Last Year.

f. From the Results Displayed Per Page drop-down list box, choose the number of entries to display per page. The default setting specifies 25.

Step 6 Click **Search.**

Bug Toolkit displays the list of caveats based on your search criteria.

Step 7 From the results window, you can save selected bugs for review at a later time, set up email notifications, and export your results to a Microsoft Excel spreadsheet.

- To save certain bugs, check the check box next to each bug that you want to review at a later time and click **Save Checked**.
- In the Place in Group field, choose one of the following options to save your defects in a bug group:
  - **Existing Group—Click this** radio button and choose an existing group name from the drop-down list box.

    When you choose an existing group, the Group Notification Settings are configured to match the existing group. To change your Group Notification Settings, click the **My Notifications** link and edit your options.
  - **Create New Group—**Click this radio button and enter a group name to create a new group for this saved search.

    When you create a new group, you can configure your Group Notification Settings to enable automatic notification of bug status changes.
- To export your results to a Microsoft Excel spread sheet, click the **Export All to Spreadsheet** link. From the File Download dialog box, you can choose to open or save the file.

Step 8 In the Email Updates section, choose from the following options to set email notification preferences for automatic bug status change updates:

- **No emailed updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Yes, email updates to:**—Click this radio button and enter your email address to receive automatic updates. Then, choose a schedule from the On a schedule: drop-down list box.

Step 9 To save your changes, click **Save Bug**.

Step 10 If desired, you can filter your results by choosing from the following options:

- From the **Filter Options > Severity** drop-down list box, choose an individual severity.
- From the **Filter Options > Status** drop-down list box, choose an individual status.
- To filter by technology, click the **Across any technology** or **Across specific technologies such as IP Routing, Voice Quality, or WLAN Security** radio button.

Step 11 Click **Submit**.

Step 12 To modify your results, choose from the following options in the Search Again Here section:

- In the Product: field, choose from one of the following options:
  - **Search only:** <*product name*>—Click this radio button to search for the same product.
  - **Specify a different product**—Click the radio button to search for a different product.
- From the Version drop-down list box, choose the applicable Cisco IPICS major software version number (such as, 1.0, 2.0, or 2.1).
- Choose Advanced Options, as documented in Step 5.

Step 13 Click **Search**.

You can save your query for future use. See the "Saving Bug Toolkit Queries" section on page 68.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and 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 monitored, or the network profile.

To save your Bug Toolkit queries, perform the following procedure:

Procedure

Step 1 Perform your search for caveats, as described in the "Using Bug Toolkit" section on page 65.

Step 2 In the search result window, click the **Save Search** button.

Under the Save Search Settings section, the system displays the bug information, including the Cisco product, software version, technology, and severity level.

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

Step 4 In the Place in Group field, choose one of the following options to save your defects in a bug group:

- **Existing Group—**Click this radio button and choose an existing group name from the drop-down list box.
  - When you choose an existing group, the Group Notification Settings are configured to match the existing group. To change your Group Notification Settings, click the **My Notifications** link and edit your options.
- **Create New Group—**Click this radio button and enter a group name to create a new group for this saved search.
  - When you create a new group, you can configure your Group Notification Settings to enable automatic notification of bug status changes.

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.

Step 5 In the Email Updates section, you can choose from the following options to set email notification preferences for automatic bug status change updates:

- **No emailed updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Yes, email updates to:**—Click this radio button and enter your email address to receive automatic updates. Then, choose a schedule from the On a schedule: drop-down list box.

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

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.

Bug Toolkit saves your bugs and searches and makes them available through the My Notifications link. Click the **My Notifications** link to view your saved searches, edit your notifications, and/or delete existing bug groups and saved searches.

Open Caveats for Cisco IPICS - Release 2.1(1)

Table 8 describes possible unexpected behaviors by Cisco IPICS release 2.1(1), sorted by component.

To view caveats that were opened in previous releases of Cisco IPICS, follow the instructions as described in the "Using Bug Toolkit" section on page 65.

Tip For more information about an individual defect, click the associated Identifier in Table 8 to access the online record for that defect, including workarounds.

Understanding the 1st Found-In and the Fixed-in Fields in the Online Defect Record

In each online defect record, Bug Toolkit may display the following version fields:

- 1st Found-In—The value in this field correlates to the product version number that the defect was first found in.
- Fixed-In—The value in this field correlates to the product version number(s) in which the defect was resolved.

When you open the online record for a defect, you may see data in the "1st Found-In" and/or the "Fixed-In" fields. The information that displays in these fields identifies the list of Cisco IPICS versions in which the defect was first found and/or fixed. 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:

- 2.0(1) = Cisco IPICS release 2.0 MR1
- 2.0(2) SR1 = Cisco IPICS release 2.0 MR2 with SR1
- 2.0(2) ES2 = Cisco IPICS release 2.0 MR2 with ES2
- 2.0(2) SR1+ES1 = Cisco IPICS release 2.0 MR2 with SR1 and ES1

MR, SR, and ES versions are cumulative and can be installed only on the appropriate previous version that is in the upgrade path. For these releases, the following guidelines apply:

- MR, SR, and ES releases include the contents of the previous release. For example:
  - 2.0(1) SR2 includes 2.0(1) SR1
  - 2.0(1) ES2 includes 2.0(1) ES1
  - 2.0(1) SR1+ES2 also includes 2.0(1) SR1+ES1
- Releases must be installed on top of the previous release. For example:
  - 2.0(1) ES1 can only be installed on 2.0(1); it cannot be installed on 2.0(1) SR1
  - 2.0(2) SR1+ES1 can only be installed on 2.0(2) SR1; it cannot be installed on 2.0(1) SR1
- If you encounter an issue for which you want to obtain the fix, you must obtain the appropriate version in which the defect was resolved.

Obtaining Upgrade Software

- MR upgrades are available via Cisco-provided CD-ROM format. To obtain an MR upgrade, contact your Cisco representative for information. For customers who have an SAS contract, MR upgrades can be obtained by using the Product Upgrade Tool (PUT) at the following URL: http://www.cisco.com/upgrade
- SR upgrades are available via web download from Cisco.com. To obtain an SR upgrade, go to http://www.cisco.com/cgi-bin/tablebuild.pl/ipics
- ES upgrades are available only through the Technical Assistance Center (TAC).

Note Because defect status continually changes, be aware that Table 8 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 65. You can also use Bug Toolkit to view caveats that were opened in previous releases of Cisco IPICS and which may still be open.

Tip Bug Toolkit requires that you have an account with Cisco.com. 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://tools.cisco.com/Support/BugToolKit/

Table 8 Open Caveats for Cisco IPICS Release 2.1(1)

Identifier	Headline
	Server Caveats
	Component: db-server
CSCsi59002	If the Cisco IPICS database becomes corrupted after an unexpected system shutdown, you may not be able to configure the SIP provider or use customized script prompts and spoken names. Corrupted database records may be removed by running the 2.0(2) SR1 installer or a script for release 2.1(1). http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsi59002
CSCsk00010	Under load conditions that exceed the Cisco IPICS specifications, the Cisco IPICS database may become unresponsive. In this situation, certain system operations, such as activating VTGs, do not succeed. To resolve this issue, restart the server. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk00010
CSCsk19924	Under load conditions that exceed the Cisco IPICS specifications, the Cisco IPICS application may become unresponsive. In this situation, certain system operations, such as activating VTGs, do not succeed. To resolve this issue, restart the server. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk19924

Table 8 Open Caveats for Cisco IPICS Release 2.1(1) (Continued)

Identifier	Headline
	Component: installer-server
CSCsj91924	If your server loses connectivity or power during an upgrade, the SSH shell process terminates and the upgrade does not successfully complete. The steps to resolve this issue vary depending on the status of the database backup at the time that connectivity or power was lost. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsj91924
CSCsk05990	When you install Cisco IPICS from the CD on the Cisco MCS 7825-H1 server, the CSA installation may output certain warning or memory error messages; these messages do not affect the operation of the system and you do not need to take any action. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk05990
	Component: ipphone-interface
CSCsj61772	When connected to the Cisco IPICS service, the Cisco Unified IP Phone 7960 may stop receiving and transmitting audio after a period of time. To reconnect to the audio stream, reselect the channel or VTG from the Cisco IPICS service menu. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsj61772
	Component: lmr-interface
CSCsk48382	Cisco IPICS does not process the value that you enter for the low level guard tone (LLGT) in the **Configuration > Radios** window. Instead, you must specify the LLGT that you need to use in the radio descriptor file. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk48382
	Component: mp-server
CSCsk24395	After you upgrade the Cisco IPICS-Mobile Platform from Cisco IPICS release 2.0(2) SR1 to release 2.1(1), the license file is not recognized. You can resolve this issue by performing a pre-upgrade or a post-upgrade task. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk24395

Table 8 Open Caveats for Cisco IPICS Release 2.1(1) (Continued)

Identifier	Headline
	Component: rms-interface
CSCsk18050	Under maximum load conditions over an extended period of time, some RMS resources may no longer be actively used by the system. To resolve this issue, restart the server. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk18050
	Component: ui-server
CSCsi87239	You cannot delete a radio if the radio is used as a media connection for the channel. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsi87239
CSCsj17579	Cisco IPICS does not provide visual indication of the currently-tuned radio channel selector when a PMC user tunes the radio to another channel selector that is associated with the radio. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsj17579
CSCsj35416	Cisco IPICS does not support the use of the Listen Only attribute for users who are dialed into radio channels. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsj35416
CSCsk23712	To change the settings for user associations to a channel, make sure that you click **Save** before you click the **Associations** button; otherwise, the setting does not change. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk23712
	Policy Engine Caveats
	Component: ippe-dial-engine
CSCsk27532	The tooltip for the Disable Audio check box incorrectly states that this attribute affects dial-in users. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk27532

Table 8 Open Caveats for Cisco IPICS Release 2.1(1) (Continued)

Identifier	Headline
CSCsk43894	When an outbound policy engine call is unanswered by the user, but the call is answered by voice mail, the GUI displays an inaccurate status. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk43894
CSCsk43906	When an outbound policy engine call is results in a busy tone, but the call is answered by voice mail, the GUI displays an inaccurate status. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk43906
	Component: ippe-notification
CSCsk21738	When a Cisco Unified Wireless IP Phone 7920 user needs to return to a channel or VTG after exiting a notification, the user must reselect the channel or VTG from the channel menu. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk21738
CSCsk25301	When one dial number is registered to multiple phones, the policy engine sends the dial notification to only the first phone that is registered for this dial number in Cisco Unified Communications Manager. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk25301
CSCsk25429	When a Cisco Unified Wireless IP Phone 7920 user receives a long audio notification from the policy engine, the user can only terminate the notification by powering off the phone. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk25429
	PMC Caveats
	Component: installer-pmc
CSCsj63490	If you try to repair or uninstall the PMC while it is running, the operation does not succeed. Close the PMC and then reattempt the operation. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsj63490

Table 8 Open Caveats for Cisco IPICS Release 2.1(1) (Continued)

Identifier	Headline
CSCsk01203	When you install the PMC, the Cisco Security Agent may repeat the message about installing the pmc.exe. To continue, click **OK**. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk01203
	Component: other-pmc
CSCsj47859	The PMC does not provide audible indication when a channel selector has been changed by another PMC user or when tones or signals are being sent or received. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsj47859
CSCsk18537	If you install the PMC on a PC that runs VMware, your PMC session may be logged out unexpectedly. (Cisco IPICS does not support the installation of the PMC on a PC that runs VMware.) http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk18537
CSCsk27505	The Cisco IPICS server may reflect an exception for the PMC activity log if the activity log is empty or incomplete. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk27505
	Component: ui-pmc
CSCsi90449	You must reselect any channels that you had previously selected after you switch regions on the PMC radio console skin. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsi90449
CSCsk14314	The PMC may display a channel multiple times after you reorder channels between skin regions. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk14314
CSCsk23662	The PMC may terminate unexpectedly when you connect by using the Cisco Systems VPN Client version 4.8.010300. http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsk23662

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 77
- Changes, page 78
- Omissions, page 78

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, page 77

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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Release Notes for Cisco IPICS, Release 2.1(1)