Cisco IP Interoperability and Collaboration System (IPICS) Server Administration Guide

Release 2.0(1)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8023-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

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.

Cisco IPICS Server Administration Guide
Copyright © 2006 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xvii

- Introduction xvii
- Audience xviii
- Organization xviii
- Related Documentation xix
  - Cisco Unified CallManager Documentation xxi
  - Cisco Unified CallManager Express Documentation xxi
  - Cisco 7800 Series Media Convergence Servers Documentation xxi
  - Cisco Unified IP Phone Documentation xxi
  - Cisco Land Mobile Radio over IP xxi
  - Cisco Security Agent xxii
  - Cisco IOS Documentation xxii
- Document Notes and Conventions xxii
- Obtaining Documentation xxiii
  - Cisco.com xxiii
  - Product Documentation DVD xxiv
  - Ordering Documentation xxiv
- Documentation Feedback xxiv
- Cisco Product Security Overview xxv
  - Reporting Security Problems in Cisco Products xxv
- Product Alerts and Field Notices xxvi
- Obtaining Technical Assistance xxvii

Cisco Support Website xxvii
Submitting a Service Request xxviii
Definitions of Service Request Severity xxix
Obtaining Additional Publications and Information xxix

CHAPTER 1 **Introducing Cisco IPICS** 1-1
Getting Started 1-2
Cisco IPICS Overview 1-3
Cisco IPICS Server 1-4
Push-to-Talk Management Center 1-4
LMR Gateways 1-5
RMS 1-5
Networking Components 1-5
Cisco Unified CallManager Functionality 1-6
Audio Clients 1-6
Cisco IPICS Roles 1-6
Cisco IPICS Administration Console 1-7
Cisco IPICS Server Usage Guidelines 1-8
Browser Guidelines 1-10
Accessing the Administration Console 1-11
Exiting the Administration Console 1-13
Entering Required Information in Administration Console Windows 1-13
Using Search Windows 1-13
Navigating Item Lists 1-15
Getting Help in the Administration Console 1-16
Viewing Information about Cisco IPICS 1-16
Administration Console Timeout 1-16

CHAPTER 2 **Performing Cisco IPICS System Administrator Tasks** 2-1

Managing PTT Channels and Channel Groups 2-2
Understanding the Channels Window 2-3
Understanding the Channels and Channel Groups Window Icons 2-6
Adding a PTT Channel 2-7
Viewing and Editing Channel Details 2-8
Changing the Status of a PTT Channel 2-20
Understanding Association Attribute Behaviors 2-21
User-Channel Association Example 2-22
Associating PTT Channels to Ops Views 2-23
Associating Users to PTT Channels 2-24
Viewing Channel Associations 2-26
Deleting a PTT Channel 2-27
Understanding the Channel Groups Window 2-28
Adding a Channel Group 2-30
Viewing and Editing Channel Group Details 2-31
Viewing Channel Group Associations 2-34
Removing a PTT Channel from a Channel Group 2-35
Associating Ops Views to Channel Groups 2-36
Deleting a Channel Group 2-37
Managing Locations 2-38
Predefined Cisco IPICS Locations 2-38
Location Associations 2-40
Summary of Access Types and Connections 2-43
Understanding the Locations Window 2-45
Adding a Location 2-45
Viewing or Editing a Location 2-46
Deleting a Location 2-47
Managing the Multicast Pool 2-47
Understanding the Multicast Pool Window 2-48

Guidelines for Using IP Multicast Addresses with Cisco IPICS 2-51
Adding Multicast Addresses 2-51
Viewing and Editing Multicast Address Information 2-53
Deleting a Multicast Address 2-55
Managing the RMS 2-56
Understanding the RMS Window 2-57
Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS 2-59
Editing or Viewing RMS Details 2-59
Deactivating or Activating an RMS 2-63
Adding an RMS 2-64
Viewing and Configuring Loopbacks 2-66
Viewing Detailed Information about a Loopback 2-67
Enabling DS0s in a Loopback 2-67
Disabling DS0s in a Loopback 2-68
Removing a Loopback 2-69
Deleting an RMS 2-69
Managing the RMS Configuration 2-70
Managing Licenses 2-72
Understanding the License Management Window 2-72
Understanding Time-bound License Behavior 2-77
Uploading a License File 2-78
Viewing Active Users 2-79
Managing Activity Logs 2-83
Understanding the Activity Log Management Window 2-84
Viewing and Downloading Activity Logs 2-85
Downloading Archived Activity Logs 2-88
Managing Activity Log Options Per Ops View 2-89
Managing Cisco IPICS Options 2-91
Managing PMC Versions 2-106

Understanding the PMC Versions Window 2-107
Uploading PMC Versions to the Cisco IPICS Server 2-109
Changing the State of PMC Versions 2-110
Deleting PMC Versions 2-112
Managing PMC Alert Tones 2-112
Creating a PMC Alert Tone Set 2-113
Adding PMC Alert Tone Sets 2-115
Viewing or Editing PMC Alert Tone Sets 2-117
Associating an Alert Tone Set to an Ops View 2-117
Deleting PMC Alert Tones 2-118
Managing PMC Skins 2-119
Adding PMC Skins 2-120
Viewing or Editing PMC Skins 2-120
Deleting PMC Skins 2-121
Managing the PMC Installer 2-122
Using the PMC Installer Window 2-122
Generating the PMC Installer 2-123

CHAPTER 3 **Performing Cisco IPICS Operator Tasks** 3-1

Managing Users 3-2
Understanding the Users Window 3-3
Adding a User 3-6
Managing User Information 3-9
Managing General Information for a User 3-9
Managing Address Information for a User 3-11
Managing Roles for a User 3-12
Managing Dial Login Information for a User 3-13
Managing an End Device for a User 3-15
Managing an End Device from the User Management Window 3-15
Managing an End Device from the PMC Tab 3-19

Managing the PMC from the Associations Tab 3-21
Managing Communications Preferences for a User 3-23
Viewing, Adding, Editing, or Deleting Communications Preferences 3-24
Changing the Order of Dial Preferences 3-27
Associating Resources with a User 3-28
Associating PTT Channels with a User 3-28
Associating Users with a User to Configure the Direct Two-Way Channel Feature 3-30
Associating Phones with a User to Configure the Direct Dial Feature 3-31
Associating Policies with a User 3-32
Managing Ops Views for a User 3-34
Choosing an Ops View to Which a User Belongs 3-34
Associating Ops Views with a User 3-35
Managing Prompts for a User 3-36
Viewing Information about VTGs in which a User is a Participant 3-36
Managing User Status 3-37
Changing User Status 3-38
Locking or Unlocking a User Account 3-38
Recovering a Deleted System Administrator User 3-40
Deleting a User 3-41
Managing User Groups 3-41
Understanding the User Groups Window 3-42
Adding a User Group 3-43
Adding Members to a User Group 3-45
Managing Ops Views for a User Group 3-46
Choosing an Ops View to which a User Group Belongs 3-47
Associating Ops Views with a User Group 3-47
Changing the Name of a User Group 3-49
Viewing Information about VTGs in Which a User Group is a Participant 3-49

Deleting a User Group 3-50

CHAPTER 4 **Performing Cisco IPICS Dispatcher Tasks 4-1**

Managing VTGs 4-2

Understanding the Virtual Talk Groups Window 4-3

Understanding Virtual Talk Groups Window Icons 4-6

Managing VTG Templates 4-7

Guidelines for Managing VTG Templates 4-8

Adding a New VTG Template 4-10

Modifying a VTG Template 4-14

Deleting a VTG Template 4-16

Managing Active VTGs 4-17

Guidelines for Managing Active VTGs 4-17

Changing the Status of a VTG Template 4-19

Adding Participants to and Removing Participants from an Active VTG 4-20

Muting or Unmuting a PMC User in an Active VTG 4-23

Enabling or Disabling the Latch Feature in the User Details Window 4-26

Notifying and Dialing Out to Participants, and Setting PMC Attributes in an Active VTG 4-29

Reactivating a VTG 4-32

Using the Search Utility 4-34

Best Practices for Managing VTGs 4-37

CHAPTER 5 **Performing Cisco IPICS User Tasks 5-1**

Logging in to Cisco IPICS 5-1

Managing Your User Profile 5-2

Managing Communications Preferences 5-10

Viewing, Adding, Editing, or Deleting Communications Preferences 5-10

Specifying the Order of Dial Preferences 5-13

Managing User Associations 5-14
Viewing User Associations 5-18
Downloading the PMC 5-19

CHAPTER 6 **Configuring and Managing Cisco IPICS Operational Views 6-1**
Managing Cisco IPICS Ops Views 6-1
Understanding the Ops Views Window 6-3
Creating New Ops Views 6-5
Assigning Ops Views Resources 6-6
The Benefits of Using Ops Views 6-6
Understanding Ops Views Attributes 6-7
Understanding Ops Views User Roles 6-9
Understanding Ops Views Caveats 6-11
Understanding VTG and Sub-VTG Caveats 6-13
Understanding How Ops Views Affect VTGs 6-16
VTG Caveats 6-17
Performing Ops Views Tasks 6-17
Adding Ops Views 6-18
Viewing Resources That Belong To and are Accessible To Ops Views 6-23
Viewing Ops Views License Details 6-25
Managing Ops Views License Usage and Limits 6-26
Configuring Licenses for Ops Views Usage 6-28
Allocating Dial Ports for the Dial-In/Invite and Notification Features 6-29
Understanding Dial Port Pools 6-29
Determining How Many Dial Ports to Allocate 6-31
Associating a User or User Group to an Ops View 6-31
Associating a Channel or Channel Group to an Ops View 6-32
Deleting Ops Views 6-32

CHAPTER 7 **Using the Cisco IPICS Policy Engine** 7-1

Policy Engine Overview 7-2

Policy Activities Available for Cisco IPICS Roles 7-3

Understanding the Policies Window 7-4

7-5

Adding a Policy 7-6

Managing Actions for a Policy 7-8

Adding or Updating an Action for a Multi-Purpose Type Policy 7-9

Adding or Updating an Action for an Invitation Type Policy 7-14

Deleting an Action 7-15

Managing Triggers for a Policy 7-16

Adding, Viewing, or Updating a Trigger 7-16

Deleting a Trigger 7-19

Associating Users with a Policy 7-19

Activating a Policy Manually 7-21

Deleting a Policy 7-22

Viewing Information about Executing or Executed Policies 7-22

Viewing Information about Scheduled Policies 7-25

Re-Activating a Policy or an Action 7-26

Using the Policy Engine Telephony User Interface 7-27

Accessing the TUI 7-28

Guidelines for using the TUI 7-28

General Guidelines 7-29

Menu Guidelines 7-30

CHAPTER 8 **Configuring and Managing the Cisco IPICS Policy Engine** 8-1

Obtaining Information about Dial Engine Services 8-2

Managing Tracing for the Policy Engine 8-4

Configuring the Number and Size of Dial Engine Trace Files 8-5
Configuring Trace Levels for Dial Engine Trace Files 8-6
Performing Advanced Tracing Activities 8-8
Obtaining Trace Files 8-9
Interpreting Trace Files 8-10
Managing Prompts 8-10
Managing Languages for Prompts 8-11
Viewing a List of Languages 8-11
Adding a Language 8-12
Renaming a Language 8-12
Deleting a Language 8-13
Managing Standard Script Prompts 8-14
Viewing a list of Standard Script Prompts 8-14
Uploading Standard Script Prompts 8-15
Managing Customized Script Prompts 8-16
Viewing a List of Customized Script Prompts 8-16
Uploading Customized Script Prompts 8-17
Downloading a Customized Script Prompt 8-18
Renaming a Customized Script Prompt 8-19
Deleting a Customized Script Prompt 8-19
Managing Spoken Names Prompts 8-20
Viewing a List of Spoken Names Prompts 8-21
Uploading Spoken Names Prompts 8-22
Downloading a Spoken Names Prompt 8-24
Recording a Spoken Name Prompt 8-25
Recording a Spoken Names Prompt Using the Dial Engine 8-25
Recording a Spoken Names Prompt Using the Windows Sound Recorder 8-27
Changing Information about a Spoken Names Prompt 8-28
Deleting a Spoken Names Prompt 8-29

Managing Dial Engine Scripts 8-30
Viewing a List of Dial Engine Scripts 8-31
Adding a Dial Engine Script 8-31
Viewing or Changing Information about a Custom Dial Engine Script 8-32
Deleting a Custom Dial Engine Script 8-33
Configuring SIP 8-34
Configuring Dial Engine Parameters 8-36
Managing the Direct Dial Feature 8-37
Viewing a List of Direct Dial Numbers 8-38
Designating a Dial Prefix for Direct Dial Numbers 8-39
Adding a Direct Dial Number 8-39
Viewing or Changing Information about a Direct Dial Number 8-40
Deleting a Direct Dial Number 8-41
Configuring the SIP Provider 8-41
Configuring Cisco Unified CallManager as the SIP Provider 8-42
Configuring a Cisco Router as the SIP Provider 8-46

CHAPTER 9 **Performing Cisco IPICS Database Backup and Restore Operations 9-1**
Overview of Cisco IPICS Database Backup and Restore Operations 9-1
Backing up the Cisco IPICS Server Database 9-2
Managing Database Backups from the Database Management Window 9-3
Performing a Manual Database Backup 9-3
Understanding Naming Conventions for Backup Directories 9-8
Changing the Default Settings for a Scheduled Database Backup 9-9
Choosing a Destination for the Database Backup 9-11
Caveats for Remote Host Database Backups 9-11
Restoring Data from a Database Backup 9-12
Options for Using the Restore Procedure 9-13
Performing the Restore Procedure 9-14

Checking the Restore Status in the Database Log 9-17
Downloading and Viewing the Backup and Restore Logs 9-19
Using CLI to Export and Import the Cisco IPICS Databases 9-21
Understanding the Cisco IPICS Databases 9-22
Using the Database Export Utility 9-23
Using the Database Import Utility 9-26
Troubleshooting Cisco IPICS Backup and Restore Procedures 9-30
Backing Up Data to a Remote Host Without scp Support 9-31
Restoring Data from a Remote Host Without scp Support 9-32
Unable to Log In To the Administration Console After Restoring Data 9-34
Unable to Retrieve a Database Backup from a Remote Host after Reinstalling Cisco IPICS 9-36

CHAPTER 10 **Understanding Cisco IPICS Serviceability and Diagnostic Information** 10-1
Introducing the Serviceability Drawer 10-1
Viewing the Information in the Dashboard Window 10-2
Understanding the System Dashboard 10-3
Understanding the Channel Dashboard 10-5
Understanding the Virtual Talk Group Dashboard 10-5
Understanding the User Dashboard 10-6
Understanding the License Dashboard 10-6
Understanding the RMS Dashboard 10-7
Viewing Cisco IPICS Server Diagnostic Information 10-8
Downloading the Server Diagnostic Information 10-11
Viewing the Cisco IPICS System Logs 10-13
Understanding the System Log Entries 10-13
Sorting the System Logs By ERROR or WARNING Messages 10-15
Downloading System Logs 10-16
SNMP Support for Cisco IPICS 10-18

Supported MIBs and RFCs **10-18**

Configuring an SNMP Management Console and MIB Browser for Use with Cisco IPICS **10-25**

APPENDIX A **Configuring the Cisco IPICS RMS Component** **A-1**

Configuring Security Features **A-2**

Connecting and Configuring T1/E1 Controllers **A-5**

RMS Connectivity Guidelines **A-6**

RMS IP Address Selection Guidelines **A-8**

Configuring T1/E1 Controllers, Interfaces, and Voice Parameters **A-9**

APPENDIX B **Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device** **B-1**

Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager **B-2**

Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager Express **B-3**

Subscribing to the Cisco IPICS Service **B-4**

Using the Cisco IPICS Service on a Cisco Unified IP Phone **B-5**

APPENDIX C **Frequently Asked Questions** **C-1**

GLOSSARY

INDEX

Preface

Introduction

The *Cisco IP Interoperability and Collaboration System (IPICS) Server Administration Guide* provides the information that you need to understand, configure, manage, and use the Cisco IP Interoperability and Collaboration System (IPICS) 2.0 application.

This preface contains the following sections:

- Audience, page xviii
- Organization, page xviii
- Related Documentation, page xix
- Document Notes and Conventions, page xxii
- Obtaining Documentation, page xxiii
- Documentation Feedback, page xxiv
- Cisco Product Security Overview, page xxv
- Product Alerts and Field Notices, page xxvi
- Obtaining Technical Assistance, page xxvii
- Obtaining Additional Publications and Information, page xxix

Tip If you use Cisco IPICS only for communicating with other users and do not require any other introductory material, go to Chapter 5, "Performing Cisco IPICS User Tasks," which provides information about logging into Cisco IPICS, downloading and setting up your PMC, and completing your user profile.

Audience

Cisco IPICS Server Administration Guide is intended for users who configure, operate, and manage tasks for the Cisco IPICS server. It also is intended for users who perform any of all of the Cisco IPICS roles.

Organization

This document is organized as follows:

Chapter 1, "Introducing Cisco IPICS"	Provides an overview of Cisco IPICS and directs users to the appropriate sections in this document for their particular roles.
Chapter 2, "Performing Cisco IPICS System Administrator Tasks"	Describes the tasks that the system administrator can perform in the Admin Console.
Chapter 3, "Performing Cisco IPICS Operator Tasks"	Describes the tasks that the operator can perform in the Admin Console.
Chapter 4, "Performing Cisco IPICS Dispatcher Tasks"	Describes the tasks that the dispatcher can perform in the Admin Console.
Chapter 5, "Performing Cisco IPICS User Tasks"	Discusses how a user interacts with the Admin Console. Topics covered include logging in, downloading the PMC application, and setting up a user profile.

Chapter 6, "Configuring and Managing Cisco IPICS Operational Views"	Explains the Cisco IPICS operational view functions.
Chapter 7, "Using the Cisco IPICS Policy Engine"	Describes many of the day-to-day activities that you perform with the Cisco IPICS IP Policy Engine
Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"	Describes how to configure and manage the Dial Engine, and how to configure a SIP provider for the Cisco IPICS IP Policy Engine
Chapter 9, "Performing Cisco IPICS Database Backup and Restore Operations"	Describes the procedures that you perform to back up and restore the Cisco IPICS database
Chapter 10, "Understanding Cisco IPICS Serviceability and Diagnostic Information"	Describes serviceability and diagnostic information that is available for Cisco IPICS
Appendix A, "Configuring the Cisco IPICS RMS Component"	Describes how to configure and RMS for use with Cisco IPICS.
Appendix B, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device"	Describes how to set up and use supported Cisco IP Phones with Cisco IPICS.
Appendix C, "Frequently Asked Questions"	Provides answers to frequently asked questions regarding Cisco IPICS.

Related Documentation

For more information about Cisco IPICS and the PMC application, refer to the following documentation:

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*—Describes how to install, configure, manage, and operate the Cisco IPICS PMC application
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.0(1)*—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 Guide, Release 2.0(1)*—Provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS Server Quick Start Guide, Release 2.0(1)*—Condensed version of this *Cisco IPICS Server Administration Guide* to help the administrator to quickly get started with Cisco IPICS.
- *Cisco IPICS Server Quick Start Reference Card, Release 2.0(1)*—Provides tips, quick references, and usage guidelines for the Cisco IPICS server.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*—Describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system.
- *Cisco IPICS Server Quick Start Installation Reference Card, Release 2.0(1)*—Provides tips and quick references for installing and upgrading the Cisco IPICS server.
- *Cisco IPICS Troubleshooting Guide, Release 2.0(1)*—Contains reference material about how to maintain and troubleshoot the Cisco IPICS system.
- *Cisco IPICS PMC Command Line Interface, Release 2.0(1)*—Describes the commands that you can use from the command line interface (CLI) to obtain information or to change settings for the Cisco IPICS PMC.
- *Release Notes for Cisco IPICS Release 2.0(1)*—Contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.
- *Cisco IPICS 2.0(1) Resources Card (Documentation Locator)*—Provides a summary of the documentation that is available for this release of Cisco IPICS.
- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*— Provides information about design considerations and guidelines for deploying the Cisco IPICS solution.
- *Cisco IPICS Compatibility Matrix*—Contains information about compatible hardware and software that is supported for use with Cisco IPICS.

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

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

Cisco Unified CallManager Documentation

For information about Cisco Unified CallManager, refer to the documentation at this URL:

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

Cisco Unified CallManager Express Documentation

For information about Cisco Unified CallManager Express, refer to the documentation at this URL:

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

Cisco 7800 Series Media Convergence Servers Documentation

For information about Cisco 7800 Series Media Convergence Servers, refer to the MCS data sheets at this URL:

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_data_sheets_list.html

Cisco Unified IP Phone Documentation

For information about Cisco Unified IP Phones, refer to the documentation at this URL:

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

Cisco Land Mobile Radio over IP

For information about Cisco Land Mobile Radio (LMR) over IP, refer to the documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/lmrip/index.htm

Cisco Security Agent

For information about Cisco Security Agent, refer to the documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/

Cisco IOS Documentation

The Cisco IOS software documentation set describes the tasks and commands necessary to configure certain system components and other Cisco products, such as access servers, routers, and switches. Each configuration guide can be used in conjunction with its corresponding command reference.

For information about Cisco IOS software configuration, refer to the documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/

Document Notes and Conventions

This document uses the following conventions for instructions and information:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution This caution symbol means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Convention	Description
boldface font	Commands and keywords appear in **boldface**.
italic font	Command input for which you supply the values appear in *italics*.

Convention	Description
[ ]	Optional keywords and default responses to system prompts appear within square brackets.
{**x** | **x** | **x**}	A choice of keywords (represented by **x**) appears in braces separated by vertical bars. You must select one.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen` font	Examples of information displayed on the screen.
`boldface screen` font	Information that you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

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

Documentation Feedback

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

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For nonemergencies—psirt@cisco.com

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

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

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

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

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

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

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

Product Alerts and Field Notices

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Support Website

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

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

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

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

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

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

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

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

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

Introducing Cisco IPICS

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

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

Tip If you use Cisco IPICS only for communicating with other users and you do not require any introductory material, go to Chapter 5, "Performing Cisco IPICS User Tasks." That chapter describes how to log in to Cisco IPICS, download your Push-to-talk Management Center (PMC), set up push-to-talk (PTT) channels for the PMC and Cisco IP Phone, and complete your user profile

This chapter includes these sections:

- Getting Started, page 1-2
- Cisco IPICS Overview, page 1-3
- Cisco IPICS Roles, page 1-6
- Cisco IPICS Administration Console, page 1-7

Getting Started

After you install Cisco IPICS, you perform a series of procedures to set up and configure Cisco IPICS for use. Table 1-1 lists these procedures and provides references to more information about each one.

Use this information as a guide when you set up Cisco IPICS for the first time.

For information about installing Cisco IPICS, refer to *Cisco IPICS Server Installation and Upgrade Guide*.

Table 1-1 Overview of Getting Started with Cisco IPICS

Procedure	Reference	Checkoff
Become familiar with Cisco IPICS		
1. Learn about the hardware and software components that are part of Cisco IPICS	Cisco IPICS Overview, page 1-3	❑
2. Learn about the roles that Cisco IPICS users can have	Cisco IPICS Roles, page 1-6	❑
3. Learn about the Cisco IPICS Administration Console, including how to access this application	Cisco IPICS Administration Console, page 1-7	❑
Set Up and Configure Cisco IPICS		
1. Configure RMS components	See the Chapter 2, “Managing the RMS.”	❑
2. Configure locations	See the Chapter 2, “Managing Locations.”	❑
3. Configure the multicast pool	See the Chapter 2, “Managing the Multicast Pool.”	❑
4. Create push-to-talk channels	See the Chapter 2, “Managing PTT Channels and Channel Groups.”	❑
5. Determine user roles and add users	See the “Managing Roles for a User” section on page 3-12	❑
6. Create VTG templates	See the “Managing VTG Templates” section on page 4-7	❑
7. Ensure that the server is hosting the current version of the PMC	See the “Managing PMC Versions” section on page 2-106	❑

Table 1-1 Overview of Getting Started with Cisco IPICS (continued)

Procedure	Reference	Checkoff
8. Configure the Cisco IPICS policy engine, if needed	See Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"	❑
9. Create operational views, if needed	See Chapter 6, "Configuring and Managing Cisco IPICS Operational Views"	❑
10. Set up Cisco Unified IP Phones, if needed	See Appendix B, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device"	❑

Cisco IPICS Overview

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

- Cisco IPICS server—Provides the core functionality of the Cisco IPICS system. For more information, see the "Cisco IPICS Server" section on page 1-4.
- Push-to-Talk Management Center—Standalone PC-based software application that PTT functionality for end-users, dispatch personnel, and administrators. For more information, see the "Push-to-Talk Management Center" section on page 1-4.
- LMR gateways—Provide radio network interoperability and application integration. For more information, see the "LMR Gateways" section on page 1-5.
- RMS—Enables a PMC to remotely attach to a VTG or channel, enables channels to be joined in VTGs, and performs other mixing functions. For more information, see the "RMS" section on page 1-5.
- Networking components—Include switches, routers, firewalls, mobile access routers, and wireless access points and bridges. For more information, see the "Networking Components" section on page 1-5.

- Cisco Unified CallManager functionality—Provide voice interoperability between radio and non-radio networks. For more information, see the "Cisco Unified CallManager Functionality" section on page 1-6.
- Audio clients—Devices such as land mobile radios (LMRs) and Cisco Unified IP Phones that let users participate in VTGs. For more information, see the "Audio Clients" section on page 1-6.

Cisco IPICS Server

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

- Hosts the Administration Console, which gives you control over operation and administration of Cisco IPICS
- Hosts the Cisco IPICS policy engine
- Provides Cisco IPICS authentication and security services
- Stores data that is required for operation
- Enables integration with various media resources, such as RMSs, PMCs, and Cisco IP Phones

Push-to-Talk Management Center

The Push-to-Talk Management Center (PMC) is a PC-based software application that enables end-users, dispatch personnel, and administrators to participate, via an IP network, in one or more talk groups or VTGs at the same time. The PMC acts as an LMR or PTT audio application. Through an intuitive interface, the PMC application lets users monitor and participate in one or multiple PTT channels or VTGs at the same time.

The PMC runs on the Microsoft Windows 2000 and Windows XP operating systems.

You install the PMC application on your PC after downloading the software from the Cisco IPICS server. For more information, see the "Downloading the PMC" section on page 5-19. After you install the application the first time, Cisco IPICS automatically upgrades your PMC with new versions when they become available.

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

You can change the look of the PMC user interface by choosing another Cisco-provided or custom skin, as explained in *Cisco IPICS PMC Installation and User Guide*.

LMR Gateways

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

RMS

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

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

Networking Components

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

Cisco Unified CallManager Functionality

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

Audio Clients

Audio clients are devices through which users participate in VTGs. They include PMC clients, LMR gateways and various models of the Cisco Unified IP Phone.

Cisco IPICS Roles

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

Table 1-2 describes the Cisco IPICS roles.

Table 1-2 Cisco IPICS Roles

Role	Description	Reference
User	Has the ability to maintain personal information, download the PMC client application, specify communication preferences that are used to configure audio devices, activate a policy, and view associated policies. Each Cisco IPICS user is assigned the user role. The user may have additional roles.	See Chapter 5, "Performing Cisco IPICS User Tasks."

Table 1-2 Cisco IPICS Roles (continued)

Role	Description	Reference
System administrator	Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. Also creates, edits, or deletes ops views, manages Cisco IPICS licenses and PMC versions, performs activities relating to the dial engine, activates policies, views certain policies, and monitors the status of the system and its users via the activity log files and the Dashboard.	See Chapter 2, "Performing Cisco IPICS System Administrator Tasks."
Ops view administrator	Has the ability to manage and monitor the activity logs that are filtered by ops views and accessible in the Administration Console (Administration > Activity Log Management) window.	See Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Operator	Responsible for setting up and managing users and user groups, granting access to Cisco IPICS and the PMC, assigning user channels, roles and ops views, and creating and managing policies.	See Chapter 3, "Performing Cisco IPICS Operator Tasks."
Dispatcher	Responsible for setting up VTG templates, activating VTGs to begin conferences, and adding or removing participants in VTG templates and active VTGs. Creates and manages policies. Also monitors active VTGs and events and can mute and unmute users, as necessary.	See Chapter 4, "Performing Cisco IPICS Dispatcher Tasks."
All	Equivalent to being assigned each of the other Cisco IPICS roles.	—

Cisco IPICS Administration Console

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

This section includes these topics.

- Cisco IPICS Server Usage Guidelines, page 1-8
- Accessing the Administration Console, page 1-11
- Exiting the Administration Console, page 1-13
- Entering Required Information in Administration Console Windows, page 1-13
- Using Search Windows, page 1-13
- Navigating Item Lists, page 1-15
- Getting Help in the Administration Console, page 1-16
- Viewing Information about Cisco IPICS, page 1-16
- Administration Console Timeout, page 1-16

Cisco IPICS Server Usage Guidelines

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

- The Cisco IPICS Administration Console contains the following tabs:
  - Server tab—Provides access to drawers and windows in which you perform Cisco IPICS administration and management activities. These activities include configuring and managing Cisco IPICS components, uploading licenses, managing the database, monitoring activity logs, setting system performance options, and monitoring system performance. You can also perform VTG, user, and PMC management operations.
  - Policy Engine tab—Provides access to drawers and windows in which you perform policy engine and dial engine administration and management activities. These activities include creating and managing policies, configuring SIP and dial engine parameters, managing prompts, and monitoring policy engine services, and managing tracing for the dial engine.
- Many of the Administration Console windows let you enter a variety of information. You might enter information by typing in fields, choosing from drop-down lists, or checking check boxes, depending on the window. An

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

- Most windows contain a **Save** button and a **Cancel** button. The **Save** button saves any changes that you make in a window and often closes the window. The **Cancel** button discards any changes that you have made and often closes the window.
- Many Cisco IPICS resources, such as channels, users, and VTGs, display in lists in the Administration Console. These lists include check boxes that you can check to select resources for which to perform certain functions. Most resource lists include a check box at the top of the list that allows you to select all resources at one time.
- Many of the Administration Console windows include drop-down lists. Some of these lists become available only after you perform certain functions. If you do not perform the required function, the drop-down list is dimmed to indicate that it is not available.
- For some resources, separate windows display in which you can take the following actions:
  - To move an item from one list to another list, click the item to highlight it and then click **>** or **<**, or double-click the item.
  - To move several items from one list to another list at one time, Shift+click or Ctrl+click to select the items and then click **>** or **<**.
  - To move all items from one list to another list at one time, click **>>** or **<<**.
- Cisco IPICS provides connection support for both multicast and unicast communications. Make sure that users are aware of the appropriate location information to use when they log in to Cisco IPICS.
- When configuring IP multicast addresses, Cisco strongly recommends that you configure IP multicast addresses that are only in the 239.192.0.0 to 239.251.255.255 range. This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in a local domain. This address range is less likely to cause an addressing conflict in an existing multicast domain. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51.
- Users who are in the same multicast domain are also in the same Cisco IPICS location.

- 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 supports more than one RMS component in the same location.
- When you configure an RMS component, make sure that you perform all of the configuration procedures that are described in Appendix A, "Configuring the Cisco IPICS RMS Component."
- Be aware of the number of participants in a conference and of each connection type so that you can avoid resource contention.
- If a VTG becomes active or inactive unexpectedly, a policy may have activated or deactivated the VTG. For more information about policies, see Chapter 7, "Using the Cisco IPICS Policy Engine."

Browser Guidelines

When you access the Cisco IPICS Administration Console by using Internet Explorer version 6.0.2, follow these guidelines:

- Windows in the Administration Console do not refresh automatically. As a best practice, update your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update in a window that does not display the most current data, the update 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 window displays the most up-to-date information, refresh it by clicking the button or tab that you used to display it. Some windows in the Administration Console provide a **Refresh** button, which you can use to refresh the window. or click Refresh on the. Cisco IPICS does not support the use of the browser **Refresh** button to refresh a window in the Administration Console.
- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.

- Cisco IPICS does not support accessing the Administration Console in more than one browser session at the same time on the same machine. If you use multiple browser sessions to access the Administration Console, you may experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.
- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.

Accessing the Administration Console

After you install Cisco IPICS, you can access the Administration Console from any computer that meets these requirements:

- Has IP connectivity to the Cisco IPICS server
- Running either of these operating systems:
  - Windows 2000 SP4 or higher
  - Windows XP SP2 or higher
- Running Internet Explorer version 6.0.2

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

Procedure

Step 1 Start Internet Explorer and, in the Address field, enter the IP address or the host name of the server on which Cisco IPICS is running.

The Authentication window displays.

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

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

User names and server host names are not case-sensitive.

Step 3 Click **Log In**.

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

You can perform a variety of activities in the User Details window. Table 1-3 describes these activities.

Table 1-3 User Details Window Activities

Activity	Reference
Update your user information	See the "Managing Your User Profile" section on page 5-2
Choose a tab and drawer to access additional windows	See the appropriate chapter: • Chapter 2, "Performing Cisco IPICS System Administrator Tasks" • Chapter 3, "Performing Cisco IPICS Operator Tasks" • Chapter 4, "Performing Cisco IPICS Dispatcher Tasks" • Chapter 5, "Performing Cisco IPICS User Tasks" • Chapter 7, "Using the Cisco IPICS Policy Engine" • Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"
Obtain online help	See the "Getting Help in the Administration Console" section on page 1-16

Table 1-3 User Details Window Activities (continued)

Activity	Reference
Obtain information about Cisco IPICS	See the "Viewing Information about Cisco IPICS" section on page 1-16
Log out and exit from the Administration Console	See the "Exiting the Administration Console" section on page 1-13

Exiting the Administration Console

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

Entering Required Information in Administration Console Windows

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

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

Using Search Windows

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

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

The following guidelines apply to Search or Search Results windows:

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

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

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

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

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

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

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

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

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

- To view the results in a results list at the bottom of a Search or a Search Results window, see the "Navigating Item Lists" section on page 1-15.

- To choose one or more items that display in the results list in a Search or a Search Results window, check the check box next to each item.
- To exit a Search or a Search Results window, take one of these actions:
  - Click the **OK** button—The window closes and then results that you checked are entered in the window that you return to.
  - Click the **Cancel** button—The window closes and the results that you checked are not in the window that you return to.

Navigating Item Lists

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

To view items in these lists, follow these guidelines:

- Lists are divided into *pages* of information. To specify how many rows of items are included in a page, choose the desired value from the Rows per page drop-down list at the top of the window, and then click the **Go** button next that list. You may need to use the scroll bar next to the result list to see all items in a page.
- You can navigate pages of information in a list by using the following navigation controls at the bottom of the list:
  - Page field—To go to a specific page, enter the page number and press **Enter**.
  - |< (First Page button)—Displays the first page in the list. This button is not available when the first page is displayed.
  - < (Previous Page button)—Displays the previous page in the list. This button is not available when the first page is displayed.
  - > (Next Page button)—Displays the next page in the list. This button is not available when the last page is displayed.
  - >| (Last Page button)—Displays the last page in the list. This button is not available when the last page is displayed.

Getting Help in the Administration Console

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

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

Viewing Information about Cisco IPICS

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

- Cisco IPICS version that is running
- Ops view to which the logged-in user belongs
- Ops view to which the logged-in user is accessible
- Current server date and time
- Server operating system (this information appears only if you are assigned the Cisco IPICS system administrator role)
- Date and time of the most recent database backup (this information appears only if you are assigned the Cisco IPICS system administrator role)

Administration Console Timeout

For increased system security, the Administration Console times out after 30 minutes of 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, and then click **Log In**. To exit the Administration Console, click **Logout** in any Administration Console window.

Performing Cisco IPICS System Administrator Tasks

The Cisco IPICS system administrator is responsible for installing the Cisco IPICS software and for setting up Cisco IPICS resources, including servers, routers, multicast addresses, locations, and PTT channels. The system administrator also manages the Cisco IPICS licenses and PMC versions, monitors the status of the system, reviews log files, as needed, and creates operational views.

In addition, the system administrator is responsible for performing backup and restore operations. For more information, see Chapter 9, "Performing Cisco IPICS Database Backup and Restore Operations."

Most of the system administrator activities that you perform are accessible from the Administration Console Configuration and Administration drawers. To access these drawers, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-11, then choose the **Configuration** or the **Administration** drawer.

Note You must be assigned the system administrator role to access the Configuration and Administration drawers.

The following sections describe many of the system administrator activities that you can perform from the Cisco IPICS Administration Console:

- Managing PTT Channels and Channel Groups, page 2-2
- Managing Locations, page 2-38

- Managing the Multicast Pool, page 2-47
- Managing the RMS, page 2-56
- Managing Licenses, page 2-72
- Viewing Active Users, page 2-79
- Managing Activity Logs, page 2-83
- Managing Activity Log Options Per Ops View, page 2-89
- Managing Cisco IPICS Options, page 2-91
- Managing PMC Versions, page 2-106
- Managing PMC Alert Tones, page 2-112
- Managing PMC Skins, page 2-119
- Managing the PMC Installer, page 2-122

For information about managing operational views in the Ops Views window, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

For information about managing database backup and restore operations in the Database Management window, see Chapter 9, "Performing Cisco IPICS Database Backup and Restore Operations."

Managing PTT Channels and Channel Groups

*A P*TT channel, also referred to as a channel, is a communications path that allows users to communicate with each other.

A channel group is a logical grouping of PTT channels. Channel groups allow Cisco IPICS dispatchers to work with multiple PTT channels efficiently. For example, instead of dragging individual PTT channels one at a time to set up a VTG, a Cisco IPICS dispatcher can drag a channel group to move all associated channels in the group. A PTT channel can be in as many channel groups as you require.

As a Cisco IPICS system administrator, you can perform the following PTT channel and channel group management tasks:

Channel Management Tasks

- Adding a PTT Channel, page 2-7
- Viewing and Editing Channel Details, page 2-8
- Changing the Status of a PTT Channel, page 2-20
- Understanding Association Attribute Behaviors, page 2-21
- Associating PTT Channels to Ops Views, page 2-23
- Associating Users to PTT Channels, page 2-24
- Viewing Channel Associations, page 2-26
- Deleting a PTT Channel, page 2-27

Channel Group Management Tasks

- Adding a Channel Group, page 2-30
- Viewing and Editing Channel Group Details, page 2-31
- Viewing Channel Group Associations, page 2-34
- Removing a PTT Channel from a Channel Group, page 2-35
- Associating Ops Views to Channel Groups, page 2-36
- Deleting a Channel Group, page 2-37

You perform the PTT channel management tasks in the Channels and Channel Groups windows, located in the Configuration drawer of the Administration Console. For more information about these windows, including how to access them, see the "Understanding the Channels Window" section on page 2-3 and the "Understanding the Channel Groups Window" section on page 2-28.

Understanding the Channels Window

The Channels window lists information about each of the channels that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS channels and general information for each channel. By default, this area displays all channels, but you can choose to display only channels that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of channels that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to perform several channel management functions. To display the Channels window, access the Configuration drawer; then click **Channels**.

Table 2-1 describes the items in the Channels window.

Table 2-1 Items in the Channels Window

Item	Description	Reference
Filter		
Channel Name field	This field allows you to display only channel names that include the character string that you enter (characters are not case-sensitive).	To limit the display of channels or to display a certain channel, enter the desired search criteria in the filter field and then click **Go**.
Ops View drop-down list box	This field allows you to display only channels for which the associated ops view matches the information that you choose.	
Go button	Click this button to display channels by the filters that you choose.	
Clear Filter button	Click this button to remove filter selections and display an empty list of channels. Click the **Channels** link again to display the full list of entries.	
Channel Information		
Channel Name field	This field allows you to assign a unique identification to the channel.	See the "Viewing and Editing Channel Details" section on page 2-8 and the "Adding a PTT Channel" section on page 2-7

Table 2-1 Items in the Channels Window (continued)

Item	Description	Reference
Ops View field	This field indicates the ops view to which the channel belongs.	See the "Associating PTT Channels to Ops Views" section on page 2-23
Secure field	This field indicates whether the channel is secure.	See the "Viewing and Editing Channel Details" section on page 2-8
Codec field	This field specifies the codec (G.711 or G.729) that is used by this channel.	
VTG field	This field indicates whether the channel is allowed in a Virtual Talk Group (VTG).	See the "Viewing and Editing Channel Details" section on page 2-8 and the "Adding a PTT Channel" section on page 2-7
Users field	This field indicates whether the channel is allowed to be associated to users to affect all endpoints such as the PMC and IP phone.	
Channel Status field	This field indicates whether the channel is enabled, disabled, or active.	See the "Changing the Status of a PTT Channel" section on page 2-20
Prompt field	This field indicates whether a spoken name prompt is recorded for the channel. This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface. You can record the spoken name prompt for a user by clicking the **Not Recorded** or the **Recorded** link in the Prompt column. When you click a link in the Prompt column, the Spoken Names window displays.	See Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"
Add button	Click this button to add a new channel in Cisco IPICS.	See the "Adding a PTT Channel" section on page 2-7
Delete button	Click this button to delete the specified channel(s).	See the "Deleting a PTT Channel" section on page 2-27

Table 2-1 Items in the Channels Window (continued)

Item	Description	Reference
Change Status drop-down list box	Choose from the enable or disable option to change the status of a channel.	See the "Changing the Status of a PTT Channel" section on page 2-20
Associations button	Click this button to view associations for the specified channel.	See the "Associating Users to PTT Channels" section on page 2-24 and the "Viewing Channel Associations" section on page 2-26

For information about the icons that appear in the Channels and Channel Groups windows, see the "Understanding the Channels and Channel Groups Window Icons" section on page 2-6.

Understanding the Channels and Channel Groups Window Icons

Icons in the Channels and Channel Groups windows provide information about each channel name and channel group, as described in Table 2-2.

Table 2-2 Channel Group and Channel Icons

Icon	Meaning
	PTT channel
	Channel group
	Busy PTT channel A channel is busy when it is use by an active VTG
	Secure PTT channel You can designate a PTT channel as secure when you add the channel in Cisco IPICS

Table 2-2 Channel Group and Channel Icons

Icon	Meaning
	Unavailable PTT channel A channel is unavailable when it is disabled.
	PTT Channel Not Present—A channel is not present when it is used by an active VTG
	VTG
	User

Adding a PTT Channel

Adding a PTT channel makes it available for use by Cisco IPICS.

Before you add a PTT channel, configure locations as described in the "Managing Locations" section on page 2-38.

To add a new channel, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to **Configuration > Channels**.

Step 2 In the Channels window, click **Add**.

The General tab for a new channel displays.

Step 3 Follow the steps in the "Viewing and Editing Channel Details" section on page 2-8.

Step 4 Enter appropriate information in the Ops Views fields as described in the "Configuring and Managing Cisco IPICS Operational Views". This field is optional.

Step 5 Click **Save** to add the channel without exiting the current window.

If you do not want to add the channel, click **Cancel**.

Viewing and Editing Channel Details

You can view and edit information for any channel.

To view or edit channel details, perform the following procedure:

Procedure

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

Step 2 In the Channel Name column, click the link for the channel for which you want to view or change information.

The General tab for the selected channel displays. This window contains general information for that channel. Table 2-3 provides descriptions of the fields in the General tab.

Note If an endpoint, such as the PMC or dial engine, does not support the attributes that are described in Table 2-3, then the attributes will not display in the General tab of the Channels window.

Table 2-3 General Tab Fields in Channels Window

Field	Description
Channel Information	
Channel Name	This field represents the name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: ". , – ' # ( ) / :_". Choose a unique and recognizable name that accurately describes the PTT channel. It is often helpful to name the PTT channel according to the department or organization that will use it, or for a particular geographic region (for example *Fire Department* or *North Area*). **Note** The PMC may truncate the channel name if the name includes more characters than the PMC can display.
Description—*Optional*	This field allows you to enter a description for this channel.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Preferred Codec	This drop-down list box allows you to choose the Codec (G.711 or G.729) that will be used by this channel. Use G.711 if this channel should be available to Cisco Unified IP Phone users or if it will be part of a VTG. Use G.711 or G.729 if this channel will be available to PMC users. G.729 requires digital signal processor (DSP) resources for transcoding. **Note** The codec and media connection attributes cannot be edited if users, who are associated to the channel, are logged in to an IP phone or a PMC. For more information about codecs, refer to the *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*.
Secure Channel	This drop-down list box allows you to specify whether this channel is a secure channel. This field is for reference only and should be set to reflect the configuration of the channel in your network. Changing this setting does not affect the security configuration of the channel. **Note** This field displays as read-only if the channel is a participant in an active VTG. To make the field editable, either disable the channel, or deactivate the VTG of which the channel is a participant.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Allow association to users	This check box allows you to indicate whether this channel is available to PMC users. It is used to prevent certain channels from being associated to users. If the channel is configured to disallow association to a user (attribute check box is not checked), then the channel does not display as available to users in the User window and is not available on the PMC. The User tab, in the channel Association window, is removed. **Note** If you change the channel status such that the channel can no longer be associated with a user and the channel was previously associated to one or more users, Cisco IPICS automatically removes the channel associations from the users. This attribute is checked by default upon creation of the channel.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Allow use in VTGs	This check box allows you to indicate whether this channel is an available resource for participation in a VTG This setting is used to prevent certain channels from being included in a VTG. For example, a PMC user interacting with a handset user may wish to hear all the call progress tones that the handset generates, to give feedback when a radio channel is available. These types of progress tones can be assigned to this certain channel. Because the tones can be disruptive, however, you might not want to add this type of channel to a VTG with a large group of users; therefore, when you create this channel, you would disallow it to be used in VTGs. If the channel is configured to disallow this channel in a VTG (attribute check box is not checked), the channel does not display in the Resources area of the VTGs in the VTG Management window and is not available for participation in the VTGs. The channel can, however, display as available for association to users and user groups, in the User and User Groups windows. If you change the channel such that it is no longer allowed in a VTG, the channel remains active in any current VTG to which it is a participant. However, the channel is not allowed to join any other VTG. **Note** This attribute is checked by default upon creation of the channel.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Status—*Display only*	This field displays one the following channel states: • Active—Channel is connected to a VTG • Inactive—Channel is not connected to a VTG but could potentially be in use by PMC users or IP phone users • Enabled—Channel is available (channel can be connected to a VTG) and PMC clients can use the channel • Disabled—Channel is not in use and PMC clients cannot use the channel (it is dimmed), and the channel cannot be connected to a VTG. You can still modify connection attributes on the channel.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Media Connection Assignments	
Location	Channels or users who are associated with the same location can communicate with each other without additional network configuration. Users from other locations can only access this channel through a SIP connection. **Note** Channels achieve media connectivity by being mapped to a multicast address in a location. A channel can be assigned to multiple locations. In this case, a channel can have more than one media connection. The count in the **Serviceability > Dashboard** window reflects the total number of media connections. See the "Viewing the Information in the Dashboard Window" section on page 10-2 for more information about the Dashboard window. If the network is configured so that the channel can be accessed by users in every location, set this value to **All**. See the "Managing Locations" section on page 2-38 for more detailed information about how to configure locations.
Type	This field specifies the type of connection that Cisco IPICS and devices use to connect to this channel when connecting from the corresponding location. **Note** The multicast connection type is currently the only type that is available and is selected by default.

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Address	This field specifies the multicast address, in the corresponding location, that is used to connect to this channel **Note** Cisco strongly recommends that you configure only multicast IP addresses that are in the 239.192.0.0 to 239.251.255.255 range. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51. Two channels in the same location cannot have the same multicast address. See the "Managing Locations" section on page 2-38 for more detailed information about locations.
Port	This field specifies the multicast address port number, in the corresponding location, that is used to connect to this channel. This value must be an even number in the range of 21000 through 65534. **Note** Cisco IPICS does not allow the configuration of ports below 21000 or any odd ports.
Ops Views	

Table 2-3 General Tab Fields in Channels Window (continued)

Field	Description
Belongs To	This drop-down list box allows you to choose the ops view to which you want to associate this channel. See the "Associating PTT Channels to Ops Views" section on page 2-23 for detailed information. **Note** To associate a channel to an ops view, you must belong to the SYSTEM ops view. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Accessible To	This drop-down list box allows you to choose the ops views to which you want this channel to be accessible. See the "Associating PTT Channels to Ops Views" section on page 2-23 for information about how to associate ops views to channels. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	This button allows you to make this channel accessible to ops views. See the "Associating PTT Channels to Ops Views" section on page 2-23 for more information. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

Step 3 To view the PMC details for this channel, click the **PMC** tab.

The PMC tab for the selected channel displays. This window contains PMC information for this channel. Table 2-4 provides descriptions of the fields in the PMC tab.

Table 2-4 PMC Tab Fields in Channels Window

Field	Description
PMC	
RX Mute During PTT	This attribute specifies the transmission settings for all channels or only one channel; it controls the audio for the active channels while you are transmitting. The following values affect how the mute functionality is configured on the PMC: • None—When PTT is engaged, the channel is muted. • All—When PTT is engaged, RX (receive transmission) is muted on all channels. • Channel—When PTT is engaged, RX is muted for this channel only. **Note** When you initially assign a channel to the PMC, the RX mute settings that you have configured apply. The PMC user can modify this setting, however, if you change the setting after the channel has been assigned to the user, the changes do not become effective.
Enable Voice Activity Detection (VAD)	When VAD is enabled on Cisco IPICS, the PMC only sends voice traffic when it detects a voice packet. When this attribute is set to true (attribute check box is checked) on a channel/VTG, VAD will be used by the PMC while communicating with the channel/VTG. By default, this attribute is set to true (attribute check box is checked).
Allow Latch	When set to true (attribute check box is checked) on a channel/VTG, the user can use latch (lock in channels) on any channel that you specify. By default, this attribute is set to true (attribute check box is checked).

Table 2-4 PMC Tab Fields in Channels Window (continued)

Field	Description
Listen Only	When set to true (attribute check box is checked), the user can hear, but cannot talk, on the channel.
Channel Color	Color tag that you can choose from a drop-down list box This setting uniquely identifies specific channels by using predefined colors for the background text that appears on the channel. You configure the color by choosing from the options in the drop-down list box. **Note** If you do not want the channel to be tagged with a color, then you can choose **Not colored** from the drop-down list box.

Step 4 To view channel associations, click the **Associations** button that appears at the bottom of the window.

Step 5 To view channel associations, from the Associations window take either of the following actions:

- Click the **Users** tab—This tab displays the Cisco IPICS users who are associated to this channel.

  The users who are currently associated with this channel display. The Users window lists information about each of the users who are associated to the channel.

Table 2-5 describes the items in the Users window.

Table 2-5 Items in the Users Window

Item	Description
User Name field	This field specifies the unique identification name assigned to the user.
Last Name field	This field specifies the last name of the user.

Table 2-5 Items in the Users Window

Item	Description
First Name field	This field specifies the first name of the user.
Status field	This field indicates whether the user is enabled or disabled.
Association Attributes	
Latchable field	This field indicates whether the user can latch (lock in) channels on the PMC.
Disable Audio field	This field indicates whether audio is disabled on the PMC.
Listen Only field	This field indicates that the user is restricted to listening only on the channel; no transmission is allowed.

Note User association values will be appended with a superscript (1) if they are configured as a customized value. See the "Understanding Association Attribute Behaviors" section on page 2-21 for more information about association attribute behaviors.

You can associate additional users to the channel, by performing the steps in the"Associating Users to PTT Channels" section on page 2-24.

- Click the **Virtual Talk Groups** tab—This tab displays the VTGs in which this channel participates.

Step 6 From the Users tab, you can change the PMC status for a user by checking the check box next to selected users.

The Change End Device Status drop-down list box becomes active.

Note The Change End Device Status drop-down list box becomes available only after you have checked the check box next to one or more user names. If a check box is not checked, the Change End Device Status drop-down list box is dimmed.

Step 7 From the Change End Device Status drop-down list box, choose one of the available options:

- **Allow Latch**—PMC user can latch, or lock in, channels
- **Disallow Latch**—PMC user cannot latch channels
- **Set Listen Only**—PMC user can only listen on the channel; transmission is not allowed
- **Unset Listen Only**—PMC user can listen and transmit on the channel
- **Enable Audio**—Audio is enabled on the PMC
- **Disable Audio**—Audio is disabled on the PMC

Note Be aware that when you choose the Disable Audio feature from any location in the Cisco IPICS server, the audio on all end user devices (PMC, IP phones), except for radios, is disabled.

Changing the Status of a PTT Channel

Cisco IPICS allows you to change the status (enable/disable) of a channel from either the main Channels window, or in the individual channel configuration windows.

Changing the status of a channel affects whether the channel is available to the PMC, IP phones, dialed-in users, or whether the channel can connect to a VTG. If the channel is disabled, it cannot be connected to a VTG.

For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide*.

A channel can have either of the following statuses:

- Enabled—Channel is available for use
- Disabled—Channel is not available for use

You can change the status of a single channel, or you can change the status of several channels at one time.

To determine the current status, access the Configuration drawer, click **Channels**, and look at the information in the Status column for the channel.

To change the status of a channel from the main Channels window, perform the following procedure:

Procedure

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

Step 2 Take either of these actions:

- Click the link for the channel in the Channel Name column to display the configuration window for the channel, click **Enable** or **Disable**, and then click **Save**.

  The **Enable** or **Disable** button appears at the bottom of the channel configuration window. The name of the button depends on the current status of the channel.

- In the Channels window, check the check box next to each channel for which you want to change the status, then choose the desired action (**Enable** or **Disable**) from the Change Status drop-down list box.

Understanding Association Attribute Behaviors

Users, channels, and VTGs have attributes that control their behavior. In some cases, these resources may have the same attribute behaviors, so that when you associate channels to users, or users to VTGs, the system determines the resulting PMC behavior by how the attributes are configured for each associated resource. For an example of association attribute behaviors, see the "User-Channel Association Example" section on page 2-22.

Cisco IPICS allows you to override the resulting behaviors for specific associations. When you modify channel or user attributes that are part of an association, the resulting behavior depends on the attribute settings for users within the association. Typically, when resources are part of an association, any attribute changes to the resources also apply to the resource and associations within that resource. Resource attributes may have different settings when they are not part of an association.

The following section provides an example of some of the expected system behaviors when you configure user, channel, and VTG associations.

Changes to channel, user, or VTG attributes that are also present in associations, behave differently, depending on the override status. If the association is not overridden you will be prompted to remove the overrides. An example of some association attribute behaviors is described below.

Note The example in the "User-Channel Association Example" section on page 2-22 is also applicable to user-VTG associations.

To associate an ops view to a channel, see the "Associating Users to PTT Channels" section on page 2-24.

User-Channel Association Example

The following example describes different user-channel association scenarios performed by a Cisco IPICS operator and a system administrator:

- User A is allowed to latch (the Allow Latch attribute check box is checked).
- Channel A is not allowed to latch (the Allow Latch check box is not checked).
- The Cisco IPICS operator associates User A to Channel A.

  The resulting behavior for this association is that the User A is not allowed to latch on Channel A on the PMC. On the server side, the Allow Latch attribute displays as **No** for both the user and the channel for this association, in the Latchable column in the Associations tab.

Note This behavior results because the Allow Latch setting, for both the user and the channel, must have the same value for latching to be allowed in this association. In this example, the value for Allow Latch must be **Yes**.

- You decide to allow all users to latch on Channel A, so you change the Allow Latch attribute on the channel by checking the Allow Latch check box in the **Channels > PMC** window. Because the association settings have not been customized, Cisco IPICS automatically updates the User A-Channel A association. The PMC updates to allow latching on this channel for this association.

- The operator disallows latch on Channel A by navigating to the Association tab (for Channel A), selecting all of the users, clicking **Change End Device Status**, and selecting the Allow Latch menu item.

  Cisco IPICS marks this attribute as a customized value.

Note A superscript (1) displays next to the value in the Latchable column in the Associations tab, for both the user and the channel. The superscript indicates a customized value, meaning that the previous value of the attribute in the association has been overridden.

  After the PMC updates, users in this association can no longer latch on Channel A.

- You decide to allow all users to latch on Channel A and you check the Allow Latch check box in the PMC tab for the channel. Because the association had previously been marked as a customized value the system prompts you with a message stating that this action will override the custom PMC settings for Latch.

  If you click OK to the message, the overrides are removed and latching on Channel A, for this association, is allowed on the PMC.

See the "Viewing and Editing Channel Details" section on page 2-8 for more information about the specific channel attributes.

For information about associating a channel to a user or ops view, see the "Associating Users to PTT Channels" section on page 2-24.

For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide*.

Associating PTT Channels to Ops Views

You can associate a channel to an ops view in the General tab of an individual window for a channel. When you associate a channel to an ops view, the channel can be seen by the users who belong to that particular ops view.

For more information about the Accessible To and Belongs To attributes for ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

To associate a channel to an ops view, perform the following procedure:

Procedure

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

Step 2 In the Channel Name column, click the link for the channel that you want to make accessible to an ops view.

Step 3 In the General tab, click the **Edit** button that appears in the Ops View pane.

The Ops View to Channel Association window displays the following information:

- Available Ops Views—Ops views that can be made accessible to this channel
- Associated Ops Views—Ops views to which this channel is currently accessible

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it and then click **>** or **<**, or double-click the ops view.
- To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click **>** or **<**.
- To move all ops views from one list to the other at one time, click **>>** or **<<**.

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

If you do not want to save your changes, click **Cancel**.

The ops views that you chose display in the Accessible To: field in the individual window for the channel.

Step 6 To change the ops view to which this channel belongs, choose an ops view from the Belongs To: drop-down list box.

Step 7 Click **Save**.

Associating Users to PTT Channels

You can associate specific users to a channel in the Associations window. When you associate channels with a user, the channels that you choose appear as options on a PMC or a properly-configured Cisco Unified IP Phone.

To determine the ops views to which the channels are currently associated, access the Configuration drawer, click **Channels**, and look at the information in the Ops View column for the channels.

Note You can perform this procedure only if users have already been added in Cisco IPICS.

System administrators and operators who belong to an ops view that is associated to a channel can associate other users to the channel, and add the channel to VTGs, as long as the Allow in association to users and Allow use in VTGs check boxes are checked. See the "Adding a PTT Channel" section on page 2-7 for more information.

To associate users to channels, perform the following procedure:

Procedure

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

Step 2 Take either of these actions to display the Associations window for the channel with which you want to associate users:

- Click the link for the channel in the Channel Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the Channel Name of the channel, then click the **Associations** button at the bottom of the Channels window.

Note The Associations button is dimmed if you do not check a channel or if you check more than one channel.

In the Associations window, make sure that the **Users** tab is selected.

This tab shows a list of the users that are associated with the channel, the status of each user, and information about attributes for devices that the user is using.

Step 3 Click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the channel by choosing criteria based on the following filters:

- User Name field—Specifies the user name of a user

- First Name field—Specifies the first name of a user
- Last Name field—Specifies the last name of a user
- Location drop-down list box—Choose from a list of locations

  See the "Managing Locations" section on page 2-38 for detailed information about how to configure locations.
- Role drop-down list box—Choose from a list of Cisco IPICS roles
- Ops View drop-down list box—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria and then click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the users in Cisco IPICS, click the **Go** button without entering any search criteria.

The results of your search criteria display in a list.

Step 5 To choose a user to associate to the channel, check the check box to the left of the user name and click **OK**.

The user that you choose displays in the user list in the Users tab.

Step 6 To view the VTGs in which the channel participates, click the **Virtual Talk Groups** tab.

If the channel participates in a VTG, the VTG name and status displays.

Viewing Channel Associations

You can view channel associations by performing the following procedure:

Procedure

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

Step 2 To view channel associations, take either of these actions:

- Click the link for the channel in the Channel Name column, then click the **Associations** button, which appears at the bottom of each tab.

- Check the check box to the left of the Channel Name, then click the **Associations** button at the bottom of the Channels window.

Note The Associations button is dimmed if you do not check a channel or if you check more than one channel.

Step 3 From the Associations window, you can view the associations for the channel by clicking either of the following tabs:

- **Users**—View users who are associated with this channel, and associate other users to the channel

Note To associate other users to the channel, see the "Associating Users to PTT Channels" section on page 2-24.

- **Virtual Talk Groups**—View the VTGs in which this channel is participating

Deleting a PTT Channel

If a PTT channel is no longer needed, you can delete it from Cisco IPICS. You can delete a single channel or you can delete several channels at one time.

To delete a channel, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each channel that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the channel(s), click **Cancel**.

Understanding the Channel Groups Window

The Channel Groups window lists information about each of the channel groups that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS channel groups and general information for each channel group. By default, this area displays all channel groups, but you can choose to display only channel groups that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of channel groups that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also provides you with the ability to perform several channel group management functions.

To display the Channel Groups window, access the Configuration drawer and click **Channel Groups**.

Table 2-6 describes the items in the Channel Groups window.

Table 2-6 Items in the Channel Groups Window

Item	Description	Reference
Filter		
Name field	Allows you to display only channel group names that include the character string that you enter (characters are not case-sensitive)	To limit the display of channel groups or to display a certain channel group, enter the desired search criteria in the filter field and then click **Go**.
Ops View drop-down list box	Allows you to display only channel groups for which the associated ops view matches the information that you choose	
Go button	Displays channel groups by the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of channel groups	
Channel Group Information		
Channel Group Name field	Name that is assigned to the channel group	See the "Viewing and Editing Channel Group Details" section on page 2-31 and the "Removing a PTT Channel from a Channel Group" section on page 2-35
Ops View field	Ops view to which the channel group belongs	See the "Associating Ops Views to Channel Groups" section on page 2-36

Table 2-6 Items in the Channel Groups Window (continued)

Item	Description	Reference
Add button	Allows you to add a new channel group in Cisco IPICS	See the "Removing a PTT Channel from a Channel Group" section on page 2-35
Copy button	Allows you to copy information from an existing channel group when you add a new channel group	
Delete button	Allows you to delete a channel group	See the "Deleting a Channel Group" section on page 2-37
Associations button	Displays the Associations window for a channel group	See the "Associating Ops Views to Channel Groups" section on page 2-36 and the "Viewing Channel Group Associations" section on page 2-34

Adding a Channel Group

A channel group provides a way to organize channels. You may find it useful to create and name channel groups according to location (for example, South Area PTT Channels) or function (for example, Executive PTT Channels).

To create a channel group, perform the following procedure:

Procedure

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

Step 2 In the Channel Groups window, take either of these actions:

- To add a channel group starting with a blank New Channel Group window, click **Add**.

- To add a channel group starting with a New Channel Group window that includes information based on an existing channel group, check the check box next to the existing channel group; then click **Copy**.

Note The **Copy** button is dimmed if you do not check an existing channel group or if you check more than one existing channel group.

The New Channel Group window displays. If you clicked Copy, this window includes information from the existing channel group, except for the channel group name.

Step 3 In the General tab, enter information for the channel group as described in the "Viewing and Editing Channel Group Details" section on page 2-31, starting with Step 3.

Note You do not need to perform all of these tasks now. You can enter or update much of this information later.

Step 4 Click **Save** to add the channel group without exiting the current window.

If you do not want to add the channel group, click **Cancel**.

For information about how to associate channel groups to a VTG or VTG template, see the "Managing VTGs" section on page 4-2.

Viewing and Editing Channel Group Details

You can view information about and edit any channel group in your Cisco IPICS network, including adding new channel members to the channel group.

To add a new channel group, see the "Adding a Channel Group" section on page 2-30.

To view and edit channel group details, and add channel members, perform the following procedure:

Procedure

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

Step 2 In the Channel Group Name column, click the link for the channel group that you want to view or edit.

The General tab for channel groups displays. This window contains general information for that channel group.

Step 3 To view or update general information for a channel group, click the **General** tab. Table 2-7 provides a description of the fields in the General tab.

Table 2-7 General Tab Fields in Channel Groups Window

Field	Description
Channel Group Information	
Channel Group Name	Name of the channel group The name can include alphanumeric characters, spaces, and any of these characters: “. , – ‘ # ( ) / :_”.
Description	*Optional*. Description of the channel group
Ops View	
Belongs To	Name of the ops view to which you want to associate this channel group. For general information about ops views, see Chapter 6, “Configuring and Managing Cisco IPICS Operational Views.”

Table 2-7 General Tab Fields in Channel Groups Window (continued)

Field	Description
Accessible To	Name of the ops view to which you want this channel group to be accessible. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	Click this button to associate ops views to the channel group. See the "Associating Ops Views to Channel Groups" section on page 2-36 for detailed information. **Note** To associate a channel group to an ops view, you must belong to the SYSTEM ops view.

Step 4 To view or update members who are associated with this channel group, click the **Members** tab. Table 2-8 provides a description of the fields in the Members tab.

Table 2-8 Member Tab Fields in the Channel Groups Window

Field	Description
Channel Name	Specifies name of the channel member
Ops View	Specifies ops view to which the channel member belongs
Secure	Indicates whether the channel member is configured as a secure channel
Codec	Represents the preferred codec of the channel member
VTG	Indicates whether the channel is configured to be used in a VTG
Users	Indicates whether the channel is configured to be associated with users
Channel Status	Indicates whether the channel is enabled or disabled

Step 5 To add additional channel members to the channel group, click the **Add** button.

The Search Channels window displays. This window allows you to search for channels to add as members by choosing criteria based on the following filters:

- Name field—Allows you to enter a channel name
- Ops View drop-down list box—Allows you to choose from a list of ops views

Step 6 To search for a channel, enter your search criteria and then click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the channels in Cisco IPICS, click the **Go** button without entering any search criteria.

You search results display in a list.

Step 7 To choose a channel to add as a member to the channel group, check the check box to the left of the channel name and click **OK**.

The channel that you choose displays in the channel members list in the Members tab.

To view current channel group associations, see the "Viewing Channel Group Associations" section on page 2-34.

Viewing Channel Group Associations

To view channel group associations, perform the following procedure:

Procedure

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

Step 2 In the Channel Group Name column, click the link for the channel group for which you want to view associations.

The General tab for channel groups displays.

Step 3 To view current channel group associations, take either of the following actions:

- Check the check box of the channel group name; then click the **Associations** button.
- Click the link of the channel group; then click the **Associations** button.

Table 2-9 provides descriptions of the fields in the Associations window.

Table 2-9 Virtual Talk Groups Tab in the Associations Window

Field	Description
VTG Name	VTG to which this channel group is associated
Status	Status of the associated VTG, which includes the following designations: • Active—Channel group is a participant in an active VTG • Idle—Channel group is a member of a VTG template

Removing a PTT Channel from a Channel Group

When you remove a PTT channel from a channel group, the channel is no longer a part of that group. Removing a PTT channel from a channel group does not remove the channel itself from Cisco IPICS, nor does it remove the channel from any other channel group to which it belongs.

To remove a PTT channel from a channel group, perform the following procedure:

Procedure

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

Step 2 In the Channel Group Name column, click the link for the channel group from which you want to remove a channel.

The General tab of the channel group displays.

Note To view the associations for the channel group, click the Associations button.

Step 3 Click the **Members** tab.

Step 4 Check the check box to the left of each channel that you want to remove from the channel group.

Step 5 Click **Delete**.

Tip To delete all the channels from this channel group, check the check box at the top of the channel list and click **Delete**.

To add channel members to a channel group, see the "Viewing and Editing Channel Group Details" section on page 2-31.

Associating Ops Views to Channel Groups

You can associate specific ops views to channel groups from the Channel Groups window. When you associate an ops view to a channel group, the channel group can be seen by the users who belong to that particular ops view.

For more information about the Accessible To and Belongs To attributes for ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

To determine the ops views to which the channel group is currently associated, access the Configuration drawer, click **Channel Groups**, and look at the information in the Ops View column for the channel group.

To associate ops views to channel groups, perform the following procedure:

Procedure

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

Step 2 In the Channel Group name column, click the channel group that you want to associate to an ops view.

Step 3 From the General tab in the Ops View pane, click the **Edit** button.

The Ops View to Channel Group Association window displays the following information:

- Available Ops Views—Ops views that can be made accessible to this channel group
- Associated Ops Views—Ops views to which this channel group is currently accessible

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it and then click **>** or **<**, or double-click the ops view.
- To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click **>** or **<**.
- To move all ops views from one list to the other at one time, click **>>** or **<<**.

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

If you do not want to associate the ops view to the channel group, click **Cancel**.

The ops views that you choose display in the Accessible To: field in the individual window for the channel group.

Step 6 To change the ops view to which this channel group belongs, from the Belongs To: drop-down list box, choose an ops view.

Step 7 Click **Save**.

Deleting a Channel Group

When you delete a channel group, it is no longer available for use in Cisco IPICS. Deleting a channel group does not affect the channels that are contained in the channel group.

To delete a channel group, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each channel group that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this channel group, click **Cancel**.

Managing Locations

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

- Predefined Cisco IPICS Locations, page 2-38
- Location Associations, page 2-40
- Summary of Access Types and Connections, page 2-43

Predefined Cisco IPICS Locations

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

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

Note The ALL 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.

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 An RMS includes digital signal 0 (DS0) resources that are used to connect channels in to VTGs (or VTGs in to VTGs) and to provide SIP-based unicast access to PMC users.

Location Associations

The following Cisco IPICS resources always maintain location associations:

- RMS—Each RMS that you configure for use with Cisco IPICS must be associated with a location. An RMS can host only those channel resources that are assigned to the same location as the RMS or to the ALL location. If the RMS is associated with the ALL location, it can host only those channels that are also assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location to an RMS.
- Channels—You can associate a channel with one or more locations. If you associate a user to a channel, the user is assigned the channel configuration that is associated to the current user location. Whenever possible, user access via multicast communication is preferable over SIP to minimize the user of RMS resources.

  The following examples describe the access that is available based on the specified configurations:

  Configuration:

  - Channel 1 is defined with the Alpha location and the Bravo location
  - Channel 2 is defined with the Delta location
  - Channel 3 is defined with the ALL location
  - User 1 is a member of VTG X
  - User 1 is assigned to Channel 1, 2, and 3 and VTG X

  Example 1: PMC User 1 logs in to Cisco IPICS by using the Alpha location

  - User 1 is given access to Channel 1 via the multicast address that is assigned to Channel 1 in the Alpha location.
  - Channel 2 is not included in the current location of User 1 (Alpha), so the server allocates an RMS resource in the Delta location to provide SIP-based connectivity.
  - Channel 3 is defined with the ALL location, so the server enables User 1 for multicast access to Channel 3.
  - VTG X is, by definition of a VTG, in the ALL location, so the server enables User 1 for multicast access to VTG X.

Example 2: PMC User 1 logs in to Cisco IPICS by using the Delta location

- Channel 1 is not included in the Delta location, so the server allocates an RMS resource in either the Alpha location or the Bravo location to provide SIP-based access to Channel 1.
- Channel 2 is included in the Delta location, so the server enables multicast access.
- Channel 3 is defined with the ALL location, so the server enables User 1 for multicast access.
- VTG X is defined in the ALL location, so the server enables User 1 for multicast access.

Example 3: PMC User 1 logs in to Cisco IPICS by using the REMOTE location

- Channel 1, 2, and 3 and VTG X all require that the server allocate RMS resources for this connection.
- Channel 1 requires that the server allocates an RMS resource from either the Alpha location or the Bravo location.
- Channel 2 requires that the server allocates an RMS resource from the Delta location.
- Channel 3 and VTG X are both defined with the ALL location.

- VTGs—VTGs are always assigned to the ALL location. Each channel that you assign to a VTG uses one RMS resource.
- PMC—During the login process, the PMC user chooses their current location or the REMOTE location.

  When a user chooses the REMOTE location, the server configures all of the user-assigned channels and VTGs for SIP-based access. In this case, the server must allocate one RMS resource for each channel and VTG. If the server has insufficient resources to use in the location that is specified by the channel configuration, the PMC user receives a message to indicate that the channel is not available.

  When the user chooses a location other than REMOTE, the server assigns direct multicast access to each channel that you configure with the same location as the chosen location, and any channel that you configure with the ALL location.

Note The server considers any assigned channels that cannot be accessed directly by using a multicast connection to be in the REMOTE location, which causes Cisco IPICS to allocate RMS resources for each one of those assigned channels.

- IP Phones—IP phones only support multicast connections. To use IP phones with Cisco IPICS, you must assign a location that is the same as the dial login default location. The server assigns the configured default location to an IP phone user when the user logs in to Cisco IPICS. (In this case, there is no user selection for location.) IP phone users can access only the associated channels that are assigned to their default location, along with any assigned VTGs. If the configured default location is the ALL location, IP phone users can access only the channels that are assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location as the default location for the IP phone user.
- Dial-in/Dial-out Users—When a user accesses the telephony user interface (TUI), the user connects to the Cisco IPICS dial engine by using unicast communications. The dial engine allows the TUI user to join any VTG or channel to which the user is associated.
  - When the user selects a channel, the server creates a VTG that contains the selected channel and assigns the VTG an address from the multicast pool. For this VTG, the server uses the RMS that is configured with the same location as the channel that the TUI user has selected.
  - When the user selects a VTG, the server creates a VTG that contains the selected VTG and assigns the VTG an address from the multicast pool. For this VTG, the server can use any RMS.

  In both cases, the server establishes a unicast call flow between the TUI user and the dial engine. The dial engine converts the unicast call flow to multicast by using the address that was assigned from the multicast pool. This multicast traffic flows to the RMS where the VTG was activated. When the VTG traffic reaches the RMS it is bridged to the channel or VTG that the user has selected. Therefore, the dial engine must be in the ALL location, or multicast domain.

- Allocation of RMS resources—When multiple eligible RMS components exist, Cisco IPICS allocates resources by using the "least recently used" algorithm to achieve load balancing. The following examples show how this algorithm works:

  Example 1:

  - Channel A is defined in the ALL location
  - RMS 1 is defined in Location 1
  - RMS 2 is defined in Location 2

  When the server needs to allocate an RMS resource for Channel A, it determines which RMS is the "least recently used" RMS and allocates the resource in the appropriate RMS.

  Example 2:

  - Channel B is defined in Location 2
  - RMS 1 is defined in Location 1
  - RMS 2 is defined in Location 2

  In the above example, the server allocates resources from RMS 2 because RMS 1 is defined in a different location.

Summary of Access Types and Connections

Table 10 shows a summary of the Cisco IPICS access types and connections, as they pertain to locations.

Table 10 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.

You can perform the following location-related management tasks:

- Understanding the Locations Window, page 2-45
- Adding a Location, page 2-45
- Viewing or Editing a Location, page 2-46
- Deleting a Location, page 2-47

Understanding the Locations Window

The Locations window lists information about each of the locations that you have added in Cisco IPICS. It also allows you to perform several locations management functions.

To display the Locations window, navigate to **Configuration > Locations** link.

Note By default, location names appear in ascending alphanumeric order.

Table 2-11 describes the items in the Locations window.

Table 2-11 Items in the Locations Window

Item	Description	Reference
Location Name field	Specifies the name that is assigned to the location	See the "Viewing or Editing a Location" section on page 2-46
Add button	Allows you to add a new location in Cisco IPICS	See the "Adding a Location" section on page 2-45
Delete button	Allows you to delete a location	See the "Deleting a Location" section on page 2-47

Adding a Location

You can add locations to Cisco IPICS, as needed.

To add a location, perform the following procedure:

Procedure

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

Step 2 To add a location starting with a blank New Location window, click **Add**.

Step 3 In the Location Name field, enter a name for the location.

The location can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .

Note The PMC may truncate the location name if the name includes more characters than the PMC can display.

Step 4 Click **Save**.

If you choose not to add this location, click **Cancel**.

Viewing or Editing a Location

You can view or edit a location that is configured in Cisco IPICS.

To view or edit a location, perform the following procedure:

Procedure

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

Step 2 In the Location Name column, click the link of the location that you want to view or edit.

The window for the location that you choose displays.

Step 3 View or edit the location as desired; then click **Save**.

Tip The location can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .

Note The PMC may truncate the location name if the name includes more characters than the PMC can display.

If you do not want to save any changes, click **Cancel**.

To add a location, see the "Adding a Location" section on page 2-45. To delete a location, see the "Deleting a Location" section on page 2-47.

Deleting a Location

You can delete a location when it is no longer needed.

You cannot delete a location if it is associated with a channel or if it is set as the default location for a user. In these cases, you must disassociate the location from the channel or set another default location for the user before you can delete the location.

Note You cannot delete the **ALL** or **REMOTE** locations.

To delete a location from Cisco IPICS, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each location that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you choose not to delete this location, click **Cancel**.

Managing the Multicast Pool

Cisco IPICS stores multicast addresses in the multicast pool. When you activate a VTG, Cisco IPICS automatically assigns an available multicast address from the multicast pool to that VTG.

Note Multicast addresses are dynamically assigned from the multicast pool to VTGs only; channels are explicitly configured with static addresses.

When a VTG deactivates, its multicast address is released for use by another VTG.

Note You cannot activate more VTGs than there are multicast addresses in the multicast pool.

As a Cisco IPICS system administrator, you can perform these multicast pool management tasks:

- Adding Multicast Addresses, page 2-51
- Viewing and Editing Multicast Address Information, page 2-53
- Deleting a Multicast Address, page 2-55

When using multicast communications with Cisco IPICS, Cisco recommends that you follow the guidelines in the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51.

You perform the multicast pool management tasks in the Multicast Pool window. For more information about this window, including how to access it, see the "Understanding the Multicast Pool Window" section on page 2-48.

Understanding the Multicast Pool Window

The Multicast Pool window lists information about each of the multicast addresses that you have added in Cisco IPICS. It also allows you to perform several multicast pool functions.

Note Cisco strongly recommends that you follow the guidelines in the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51 when you use multicast communications with Cisco IPICS.

To display the Multicast Pool window, access the Configuration drawer and click **Multicast Pool**.

Each multicast address in the multicast pool window appears on its own row with related information in various columns. By default, rows of information appear in ascending order by multicast address.

Table 2-12 describes the items in the Multicast Pool window.

Table 2-12 Items in the Multicast Pool Window

Item	Description	Reference
Address field	This field specifies the multicast address and port.	See the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51

Table 2-12 Items in the Multicast Pool Window (continued)

Item	Description	Reference
Location field	This field specifies the location that is assigned to this multicast address. The location name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .	See the “Viewing and Editing Multicast Address Information” section on page 2-53 and the “Deleting a Multicast Address” section on page 2-55 See the “Managing Locations” section on page 2-38 for more detailed information about locations.
Status field	Either of the following designations can display in this field: • Active—Address is assigned to an active VTG • Idle—Address is not assigned to an active VTG	
Connection Type field	Either of the following designations can display in this field: • Used by Channel—Multicast address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG.	
Used By field	This field specifies the name of the active channel or VTG that is using the multicast address, if applicable.	
Add button	Click this button to add a multicast address.	See the “Adding Multicast Addresses” section on page 2-51
Delete button	Click this button to delete a multicast address.	See the “Deleting a Multicast Address” section on page 2-55

Guidelines for Using IP Multicast Addresses with Cisco IPICS

Be aware of the following guidelines when you use multicast communications with Cisco IPICS:

Cisco IPICS strongly recommends IP multicast addresses that are 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.
- For more information, refer to RFC 3171 - Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment and RFC 2365 - Administratively Scoped IP Multicast.

For additional information about the use of IP multicast addressing, refer to the following URL:

http://www.cisco.com/en/US/tech/tk828/tsd_technology_support_protocol_home.html

Adding Multicast Addresses

When you add a multicast address to the multicast pool, it becomes available for use by active VTGs.

If you later assign the address to a channel, it will no longer be available for use by active VTGs.

Before you add a multicast address, configure locations, as described in the "Managing Locations" section on page 2-38.

To add one or more multicast addresses to the multicast pool, perform the following procedure:

Procedure

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

Step 2 Click **Add**.

The New Multicast Pool window displays.

Step 3 In the Address field, enter the multicast address that you want to add.

Be sure to enter a valid multicast address that begins with 239.

Note Cisco strongly recommends that you configure only addresses that are in the 239.192.0.0 to 239.251.255.255 range. For more information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51.

Step 4 In the Number of Addresses field, enter the number of IP addresses that you want Cisco IPICS to generate.

You can enter a number between 1 and 255.

Cisco IPICS can generate a list of multicast addresses and add them to the multicast pool. This feature can be useful when you need to add several multicast addresses.

When you choose to have Cisco IPICS generate a sequence of multicast addresses, you specify the first address and the number of addresses that you want. Cisco IPICS returns the number of addresses that you specify, starting with the first address that you specified and incrementing the fourth octet of each additional address by one. You can generate a sequence of up to 255 multicast addresses at a time.

For example, if you request five addresses and specify the first address to be 239.195.5.1, Cisco IPICS generates this sequence of addresses:

```
239.195.5.1
239.195.5.2
239.195.5.3
239.195.5.4
239.195.5.5
```

Note When you generate multicast addresses in this way, Cisco IPICS assigns the port number that you designate to each address. After Cisco IPICS generates the list of addresses, you can change the number or port for any address, and you can delete any addresses that you do not want in the multicast pool. For more information, see the "Deleting a Multicast Address" section on page 2-55.

Step 5 In the Port field, enter the port number for this address.

This value must be an even number in the range of 21000 through 65534.

Step 6 Click **Save**.

If you choose not to add this address, click **Cancel**.

Step 7 If you want to add other individual addresses, repeat Step 3 through Step 6.

Viewing and Editing Multicast Address Information

You can view information for any multicast address, and you can change a multicast address and port number. You do so in the Multicast Pool window.

To view or edit multicast address information, perform the following procedure:

Procedure

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

Step 2 To view or edit a multicast address, click the link for the multicast address that you want to view or change.

The Multicast Address Pool Information window for the selected multicast address displays.

Step 3 View or update the information that is described in Table 2-13.

Table 2-13 Multicast Address Details Area Fields

Field	Description
Address	This field represents the multicast address. You add an address, enter a valid multicast address, and make sure to enter all 4 octets of the address. Each octet must be in the range of 0 through 255. **Note** Cisco IPICS strongly recommends addresses that are configured in the 239.192.0.0 to 239.251.255.255 range. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-51.
Port	This field represents the port number assigned to the multicast address. This value must be an even number in the range of 21000 through 65534. **Note** Cisco IPICS does not allow the configuration of any port below 21000 or any odd ports.
Connection Type—*Display only*	This field can include either of the following designations: • Used by Channel—Address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG.
Status—*Display only*	This field can include either of the following states: • Active—Address is assigned to an active VTG • Idle—Address is not assigned to an active VTG

Table 2-13 Multicast Address Details Area Fields (continued)

Field	Description
Location—*Display only*	Location that is assigned to this multicast address An address for a PTT channel has a specific location, either location ALL or another location name. Regardless of the location in this field, a VTG can contain only channels that are in the same multicast domain as the RMS that is used to mix the channels. See the "Managing Locations" section on page 2-38 for more detailed information about locations.
Used By—*Display only*	Name of the active channel or VTG that is using the multicast address, if applicable
Last Released—*Display only*	This field displays when the multicast address was last released.

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

If you do not want to save your changes, click **Cancel**.

Deleting a Multicast Address

You can delete a multicast address when it is no longer needed.

Note You cannot delete a multicast address that is assigned to an active VTG. You must deactivate the VTG before you can delete the address. You also cannot delete a multicast address that is assigned to a channel. To delete the address in this case, delete the channel, which automatically removes the multicast address from the multicast pool.

To delete a multicast address from the multicast pool, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each multicast address that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you choose not to delete this address, click **Cancel**.

Managing the RMS

An RMS is a component that enables the Cisco IPICS PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.

Note Before you perform the RMS management procedures that are described in the following sections, you must configure the RMS. For more information see Appendix A, "Configuring the Cisco IPICS RMS Component."

As a Cisco IPICS system administrator, you can perform these RMS management tasks:

- Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS, page 2-59
- Adding an RMS, page 2-64
- Viewing and Configuring Loopbacks, page 2-66
- Deleting an RMS, page 2-69
- Managing the RMS Configuration, page 2-70

You perform the RMS management tasks in the RMS window, which is located in the Configuration drawer. For more information about this window, including how to access it, see the "Understanding the RMS Window" section on page 2-57.

Note Cisco IPICS is not intended to provide complete management capabilities for an RMS. Cisco IPICS manages only the voice-specific parameters that are necessary to set up audio services for Cisco IPICS.

Understanding the RMS Window

The RMS window lists the RMS components that are available in your Cisco IPICS network. This window also allows you to perform the RMS management functions.

To display the RMS window, navigate to **Configuration > RMS**.

The Routers pane in the RMS window displays the name of each RMS that is configured in your Cisco IPICS network.

For detailed RMS configuration information, see the Appendix A, "Configuring the Cisco IPICS RMS Component."

Table 2-14 describes the items in the RMS window.

Table 2-14 Items in the RMS Window

Item	Description	Reference
RMS Name field	This field specifies a unique name that is assigned to the RMS.	See the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-59 and the "Adding an RMS" section on page 2-64 See the "Managing Locations" section on page 2-38 for detailed information about configuring locations
Location field	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this RMS.	
IP Address field	This field specifies the IP address of the Loopback interface.	
Router Type field	This field specifies the model number of the RMS.	
Status field	This field indicates whether an RMS is operational, configured, stopped, deactivated, or unreachable.	
Available field	Number of DS0s that are available for use in Cisco IPICS	See the "Viewing and Configuring Loopbacks" section on page 2-66
In Use field	Number of DS0s that are currently being used in Cisco IPICS	
Reserved field	Number of DS0s that are reserved for non-Cisco IPICS use	
In Error field	Number of DS0s that are misconfigured	

Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS

You can view and edit information for any RMS in your Cisco IPICS network. You can also deactivate an RMS, which makes it unavailable for use by Cisco IPICS, or reactivate an RMS. You perform these tasks in the Edit Router Details area.

By default, Cisco IPICS polls the RMS every 10 minutes, using the RMS comparator mechanism. The RMS comparator checks the responsiveness of the RMS if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. (You can change the polling period by entering a new value in the **RMS Polling Frequency field** in the Options window in the Administration drawer. For more information, see the "Managing Cisco IPICS Options" section on page 2-91.)

Tip Because the RMS comparator mechanism can interject delays, you can disable it by navigating to **Administration > Options** and checking the **Disable RMS Comparator** check box. You should check this check box if you are connected via a high latency (high delay), low bandwidth connection, such as a satellite link. Be aware that when you disable the RMS Comparator, you must merge the RMS configuration to make sure that the router is synchronized with the server. For information about how to merge RMS configuration, see the "Managing the RMS Configuration" section on page 2-70. For more complete configuration and deployment details, refer to the *Solution Reference Network Design (SRND) for Cisco IPICS, Release 2.0(1)*.

Note Disabling the RMS Comparator affects every router in the network.

Editing or Viewing RMS Details

You can edit or view a variety of information for an RMS. To do so, perform the following procedure:

Procedure

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

Step 2 In the RMS Name column, click the link of the RMS that you want to view or change.

The General tab for the selected RMS displays.

Step 3 To change any RMS information, except updating the name, configuring loopbacks, or reserving or unreserving DS0s, click **Deactivate**.

This action makes the RMS temporarily unavailable to Cisco IPICS.

Tip Before you make changes, wait until all RMS resources are not in use, or manually disable the channel or deactivate any VTG that uses the resources of this RMS. For more information about how to disable a channel, see the "Changing the Status of a PTT Channel" section on page 2-20. For information about how to deactivate a VTG, "Changing the Status of a VTG Template" section on page 4-19.

Step 4 To view or update the information in the General tab, see Table 2-15.

Table 2-15 Fields in the General Tab of the RMS Window

Field	Description
Identification	
Name	This field specifies the name of the RMS. The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :.
Location	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this RMS. An RMS must be configured with the same location that is configured for the channels that it serves. See the "Managing Locations" section on page 2-38 for detailed information about locations.
Description	This field specifies a description for the RMS.

Table 2-15 Fields in the General Tab of the RMS Window (continued)

Field	Description
Status—*Display only*	This field can include any of the following statuses: • Operational—RMS has at least one loopback configured and that is operating. • Unconfigured—RMS has no loopbacks. • Stopping—RMS has been deactivated but has at least one DS0 in use by Cisco IPICS. The RMS will become deactivated when Cisco IPICS no longer uses any of its voice ports. **Note** If one or more VTGs are active and you try to deactivate an RMS, the RMS status displays as Stopping. You must deactivate the VTG(s) before the RMS displays a deactivated status. To deactivate a VTG, see the "Changing the Status of a VTG Template" section on page 4-19. • Deactivated— RMS has been deactivated and has no DS0s in use. **Note** You can change the user name, password, multicast address, or location of the RMS only when it is in the Deactivated state. • Unreachable—RMS cannot be reached by the Cisco IPICS server.
Hardware Settings	
IP Address	This field specifies the IP address of the Loopback interface.
Host Name—*Display only*	This field specifies the host name of the RMS.

Table 2-15 Fields in the General Tab of the RMS Window (continued)

Field	Description
User Name	This field specifies the user name that Cisco IPICS uses to access the RMS. This name must have administrator privileges on the RMS.
Password	This field specifies the password that Cisco IPICS uses to access the RMS.
Router Type—*Display only*	This field specifies the model number of the RMS.
Controllers—*Display only*	This field displays the T1/E1 connections on the RMS. The number in parentheses is the number of ports on the corresponding controller.
Loopbacks—(Click the **Loopbacks** Tab to access the Loopback information)	This field specifies the mappings between two controllers that are physically connected. To change a loopback, choose a pair of controllers from the two Loopback drop-down list boxes and click **Add**. A controller appears in gray if it is in use. Each configured loopback appears in a list near the bottom of this area. To see detailed information about a loopback, click the right arrow next to its name. To see detailed information about all loopbacks, click **Expand All**. To collapse an expanded view of a loopback, click the down arrow next to its name. To collapse detailed information about all loopbacks, click **Collapse All**. For an explanation of the detailed loopback information, see the "Viewing and Configuring Loopbacks" section on page 2-66.

Step 5 If you changed information in the IP Address, User Name, or Password fields, make the corresponding change in the router by using the configuration application of the router.

Step 6 Click **Save** to save your changes.

To exit without saving changes, click **Cancel**.

Step 7 If you deactivated the router, click **Activate** to reactivate it.

After you change information for an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the changes. If you want to cause Cisco IPICS to recognize the changes immediately, see the "Managing the RMS Configuration" section on page 2-70.

Note You can change the default time that Cisco IPICS takes to recognize an RMS by entering a new value in the RMS Polling Frequency field in the Administration > Options window. For more information, see the "Managing Cisco IPICS Options" section on page 2-91.

Deactivating or Activating an RMS

When you deactivate an RMS, it goes into the Deactivated state and becomes unavailable for use by Cisco IPICS until you activate it. You should deactivate an RMS when you make certain changes to it, as described in the "Editing or Viewing RMS Details" section on page 2-59.

Note If you deactivate an RMS that has one or more voice ports in use by Cisco IPICS, or if one or more VTGs are active, the RMS goes into the Stopping state. You cannot deactivate an RMS if any VTGs are active. A router that is in the stopping state cannot provide additional support for PMC SIP connections or additional channels that are participants in active VTGs. Existing connections and channels that are supported by the RMS are not affected. The RMS becomes deactivated when Cisco IPICS no longer uses any of its voice ports. To deactivate a VTG, see the "Changing the Status of a VTG Template" section on page 4-19.

When you activate an RMS component, it becomes available for use by Cisco IPICS.

To deactivate or activate an RMS, perform the following procedure:

Procedure

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

Step 2 In the RMS Name column, click the link of the RMS that you want to deactivate.

Step 3 Click **Deactivate** to deactivate an active RMS, or click **Activate** to activate a deactivated RMS.

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

Adding an RMS

When you add an RMS, you make it available to Cisco IPICS. Before you add an RMS, make sure that these conditions are met:

- The router must exist on the Cisco IPICS network and it must be configured as described in Appendix A, "Configuring the Cisco IPICS RMS Component"
- At least one location must be defined, as described in the "Managing Locations" section on page 2-38

To add a new RMS in Cisco IPICS, perform the following procedure:

Procedure

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

Step 2 Click **Add**.

The **Add** New Router Media Service window displays.

Step 3 In the Add New Router Media Service area, enter the following information:

Note For detailed descriptions of the RMS fields, see Table 2-15.

a. In the IP Address field, enter the IP address of the loopback interface. The IP address of the loopback interface must be configured to support SIP calls.

b. In the User Name field, enter the user name that is required to log in to the RMS.

c. In the Password field, enter the password that is required to log in to the RMS.

d. From the Location drop-down list box, choose a location that is defined by the IP address that you entered for the router.

   See the "Managing Locations" section on page 2-38 for more detailed information about locations.

e. Click **Save**.

   If you do not want to add this RMS, click **Cancel**.

   When you click **Save**, Cisco IPICS determines whether it can access the RMS. This process can take up to one minute. If the RMS is accessible, Cisco IPICS displays the Router Details area for the RMS. If the router is not accessible, a message informs you of the possible reason.

   The Router Details area displays the following information for the router that you added:

   - Location—This field specifies the location that is defined for this RMS
   - Status—This field displays unconfigured because you have not yet saved the changes that you made.
   - IP Address—This field specifies the IP address that you entered for this router.
   - Host Name—This field specifies the host name that you configured on the router.
   - User Name—This field specifies the user name that you entered for this router.
   - Password—This field specifies the password that you entered for this router.
   - Type—This field specifies the model number of this router

- Controllers—This field specifies the T1 connections that the router has available for loopback.

Step 4 In the Name field, enter a name for the RMS if you want to change the name that displays in the list or routers in the Manager Routers window.

By default, the name that displays is the router host name. You might find it useful to give the RMS a descriptive name. A name that you enter is for Cisco IPICS use only, it does not change the router host name.

Step 5 In the adjacent Loopbacks drop-down lists, create a loopback by choosing two controllers that are physically connected on the router; then click **Add**.

Repeat this step as needed to create additional loopbacks.

Step 6 Configure digital signal 0 (DS0s) for each loopback as described in the "Viewing and Configuring Loopbacks" section on page 2-66.

Step 7 Click **Save** to save the configuration for this RMS.

If you do not want to add this RMS, click **Cancel**.

After you add an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the addition. If you want to cause Cisco IPICS to recognize the addition immediately, see the "Managing the RMS Configuration" section on page 2-70.

Viewing and Configuring Loopbacks

Each loopback that you create in Cisco IPICS appears in a list near the bottom of the Edit Router Details area. You can perform the following tasks related to loopbacks:

- Viewing Detailed Information about a Loopback, page 2-67
- Enabling DS0s in a Loopback, page 2-67
- Disabling DS0s in a Loopback, page 2-68
- Removing a Loopback, page 2-69

Viewing Detailed Information about a Loopback

You view loopback information in the **Loopbacks** tab of the RMS window. You can access this tab by navigating to the Configuration > RMS window and clicking the **Loopbacks** tab.

For more information about the RMS window, see the "Understanding the RMS Window" section on page 2-57.

To see detailed information about a loopback, click the left arrow next to its name. To collapse an expanded view of a loopback, click the down arrow next to its name.

To see detailed information about all loopbacks, click **Expand All**. To collapse detailed information about all loopbacks, click **Collapse All**.

An expanded view of a loopback provides this information for each time slot in the loopback:

- Number—DS0 in the loopback
- State—One of the following:
  - Enabled—DS0 can be used by Cisco IPICS
  - Disabled—DS0 cannot be used by Cisco IPICS
- DS0 Status—One of the following:
  - In Use—DS0 is being used to add a channel to a VTG, add a VTG to a VTG, or add a SIP connection for a channel for a user
  - Available—DS0 can be used by Cisco IPICS
  - Reserved—DS0 is reserved for non-Cisco IPICS use
  - Errors—DS0 is misconfigured
- DS0 Source and DS0 Destination—Connections that the loopback is making. Port Source can be a channel or a VTG. Port Destination can be a channel, a VTG, or a user.

Enabling DS0s in a Loopback

After you create a loopback, you must enable the DS0s that can be used by Cisco IPICS. You can enable DS0s in one loopback at a time, or in several loopbacks at a time.

To enable DS0s in a loopback, perform the following procedure:

Procedure

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

Step 2 Click the **Loopbacks** tab.

Step 3 Expand each loopback in which you want to enable DS0s by clicking the right arrow next to its name or by clicking **Expand All**.

Step 4 Check the check box next to each DS0 that you want to enable.

If you want to enable all DS0s in a loopback, check the check box next to Number at the top of the list of DS0s for that loopback.

If you want to uncheck check boxes, take one of these actions:

- Uncheck specific check boxes, or uncheck the check box next to Number at the top of the list of DS0s to clears all check boxes for that loopback.
- Click **Clear** to clear all check boxes for all loopbacks.

Step 5 Click **Enable DS0s**.

The state for the DS0 displays **Enabled** in green text.

Step 6 Click **Save**.

If you do not want to enable the DS0 or DS0s, click **Cancel**.

Disabling DS0s in a Loopback

If you disable a DS0 in a loopback, it cannot be used by Cisco IPICS. You can disable DS0s in one loopback at a time, or in several loopbacks at a time.

To disable DS0s in a loopback, perform the following procedure:

Procedure

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

Step 2 Click the **Loopbacks** tab.

Step 3 Expand each loopback in which you want to disable DS0s by clicking the left arrow next to its name or by clicking **Expand All**.

Step 4 Check the check box next to each DS0 that you want to disable.

If you want to disable all DS0s in a loopback, check the check box next to Number at the top of the list of DS0s for that loopback.

If you want to uncheck check boxes, take one of these actions:

- Uncheck specific check boxes, or uncheck the check box next to Number at the top of the list of DS0s to clears all check boxes for that loopback.
- Click **Clear** to clear all check boxes for all loopbacks.

Step 5 Click **Disable DS0s**.

The state for the DS0 displays **Disabled** in red text.

Step 6 Click **Save**.

If you do not want to disable the DS0 or DS0s, click **Cancel**.

Removing a Loopback

To remove a loopback, click **Remove** next to its name; and then click **Save**.

If you decide not to remove the loopback, click **Add** next to its name or click **Cancel** instead of clicking **Save**.

Deleting an RMS

Deleting an RMS removes all of its resources from Cisco IPICS and makes the RMS unavailable to Cisco IPICS.

You cannot delete an RMS if any of its DS0s are in use by Cisco IPICS.

To delete an RMS, perform the following procedure:

Procedure

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

Step 2 Check the check box next to the RMS that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this RMS, click **Cancel**.

Managing the RMS Configuration

You can manage the RMS configuration by navigating to the Configuration > RMS window.

Merging RMS configuration updates Cisco IPICS with the following router information:

- Host name
- Router type
- Controllers

Merge the RMS configuration if you add or remove controllers on the router or if you change its host name, and you want Cisco IPICS to recognize the change.

Updating the configuration of an RMS applies the RMS configuration that is specified in Cisco IPICS to the RMS. This procedure can be useful in the following situations:

- You have changed information for an RMS as described in the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-59 and you do not want to wait for Cisco IPICS to recognize the changes, which can take up to 10 minutes (by default).
- You have added an RMS as described in the "Adding an RMS" section on page 2-64 and you do not want to wait for Cisco IPICS to recognize the addition, which can take up to 10 minutes (by default).
- You restarted an RMS and are experiencing voice connectivity or voice quality issues. Updating the configuration of the RMS can help to eliminate the router configuration as the source of the problem.
- The RMS has restarted but Cisco IPICS has not yet updated the router configuration with the configuration that is specified in Cisco IPICS.

An RMS that shuts down returns to its default configuration when it restarts. Within 10 minutes—by default—after it restarts, Cisco IPICS compares the current RMS configuration with the RMS configuration in the Cisco IPICS database. If there is a discrepancy, Cisco IPICS refreshes the RMS configuration to match the configuration in the database.

Note Manually updating the configuration for an RMS disconnects all users who are connected to the RMS through a SIP connection and may interrupt any active VTG participant that is hosted on that RMS.

To manage the RMS configuration, perform the following procedure:

Procedure

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

Step 2 To manage the RMS configuration, check the check box to the left of the RMS Name of the RMS.

Step 3 From the Configuration drop-down list box, take any of the following actions:

- To merge the RMS configuration, choose **Merge**.
- To update the RMS configuration, choose **Update**.
- To view the RMS configuration, choose **Show**.

  The configuration output displays in a separate window showing the configuration of the voice-ports and dial-peers for this RMS.

Cisco IPICS displays changes in the Edit Router Details area.

Tip You can manage the RMS configuration for all of the RMS components that are configured in Cisco IPICS by checking the check box at the top of the RMS list, and choosing **Merge, Update,** or **Show** from the Configuration drop-down list box.

Managing Licenses

The Cisco IPICS license determines the number of concurrent land mobile radio (LMR) ports, multicast ports, PMC users, IP phone users, dial users, and ops views that are available for your system. The total number of LMR and multicast ports, PMC, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased.

If your requirements exceed the limits of your current license, you can obtain additional licenses. For detailed information about licenses and how to obtain them, refer to the *Cisco IPICS Server Installation and Upgrade Guide*.

Note Before you can upgrade from a previous Cisco IPICS release to Cisco IPICS, release 2.0(1), you must purchase a Cisco IPICS, release 2.0(1) license.

As a Cisco IPICS system administrator, you can obtain and upload new license files, after you have obtained them, to the Cisco IPICS server so that the new licenses take effect. For instructions, see the "Uploading a License File" section on page 2-78.

You perform the license management tasks in the Administration > License Management window. For more information about this window, including how to access it, see the "Understanding the License Management Window" section on page 2-72.

Understanding the License Management Window

The License Management window provides information about the licenses that you configure for your Cisco IPICS installation. It also allows you to upload new licenses to the Cisco IPICS server after obtaining the licenses. See the "Uploading a License File" section on page 2-78 for information about uploading licenses.

To access the License Management window, navigate to Administration >License Management window in the Cisco IPICS Administration Console.

In this window, the **Summary** tab provides a summary of information about the licenses you have obtained for Cisco IPICS. This tab displays license feature names, the total number of ports, current port usage, and available ports. See Table 2-16 for a description of the licenses that can display in this tab.

The **Usage Per Ops View** tab provides license information per ops view. This tab displays types of licenses, the ops view, and current license usage information. See Table 2-17 for a description of the licenses, per ops view, that can display in this tab and the criteria that Cisco IPICS uses to determine license consumption for ports, PMC, IP phone, policy engine, and ops view usage.

Note The data that displays in the License Management window shows the usage at the time that the license window was last accessed. To view the most current license information, refresh your browser window. Make sure to refresh 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, then the update does not succeed and Cisco IPICS displays an error. If you receive an error, refresh your browser window and retry the operation.

Table 2-16 Summary Tab Fields in the License Management Window

Field	Description
Feature Name	
Concurrent LMR Ports	An enabled channel uses an LMR port license. After a channel is disabled, the server releases the LMR license and makes it available for use. Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location. If a channel has two multicast addresses that are assigned to the channel, then the single channel uses two licenses. If one of the multicast addresses is removed, then the system releases one of the licenses so that the port will then only use one license.

Table 2-16 Summary Tab Fields in the License Management Window

Field	Description
Concurrent Multicast Ports	An activated VTG uses a multicast port license. After a VTG is deactivated, the server releases the multicast license and makes it available for use. **Note** Be aware that an inactive VTG (VTG template) uses a license when a policy triggers (activates) that VTG; therefore, if the number of licenses has been exceeded, the policy will not be able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.
Concurrent PMC Users	A PMC user uses 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 uses multiple licenses (one for each PMC session). **Note** If you use all of the available PMC licenses, Cisco IPICS interrupts PMC user access to the system. Make sure that you are aware of the current status of PMC licenses, and that you purchase and install additional licenses immediately if you use all of the available PMC licenses.
Concurrent IP Phone Users	An IP phone user uses a license each time that a user logs in to Cisco IPICS from the phone. If you use all of the IP phone licenses, then no more IP phone users can dial in.

Table 2-16 Summary Tab Fields in the License Management Window

Field	Description
Concurrent Dial Users	Each time that the policy engine performs a dial-in or dial-out action, one license is used. If you use all of the dial user licenses, the policy engine cannot perform additional dial-in or dial-out actions. **Note** To enable dial-in/dial-out functionality in Cisco IPICS, you must have a policy engine base license. After you have purchased the policy engine base license, you will be able to access the policy engine-related windows and to perform dial-in/dial-out functions in Cisco IPICS. If you do not have a policy engine base license, the dial-in/dial-out functionality is disabled and you will not be able to access the policy engine windows.
Cisco IPICS Ops View	Cisco IPICS uses one license for each ops view that you configure. The number of ops views that are available for use displays in the License Summary pane. **Note** To create additional ops views, you must purchase and install a Cisco IPICS license that includes additional ops view ports.
Cisco IPICS Base Server License	License usage does not apply to this field. This field displays whether you have a base license for Cisco IPICS.

Table 2-16 Summary Tab Fields in the License Management Window

Field	Description
Policy Engine Base License	License usage does not apply to this field. This field displays whether Cisco IPICS policy engine is enabled. When the policy engine is enabled, the Summary tab displays **Licensed**. When the policy engine is not enabled, the Summary tab displays **Not Licensed**.

Note Dial ports can be used for dial-in or dial-out connections. For dial ports that are allocated among the ops view, the dial ports are used by dial-in, according to the pre-assigned dial-in phone number, that is configured in each ops view, that is dialed. For dial-out, the dial ports are used from the ops view, to which the user to be dialed, belongs. See Chapter 6, "Configuring and Managing Cisco IPICS Operational Views" for more information about ops views.

The **Usage Per Ops View** tab provides license information per ops view. This tab displays the types of licenses, the ops view, current license usage, and the allocated ports. See Table 2-17 for a description of the information in this tab.

Table 2-17 Usage Per Ops View Tab in the License Management Window

Field	Description
License Type	
PMC Ports	Ops View—Ops view to which this license belongs Current Usage—Number of PMC ports that are in use for this ops view Allocated Ports—Number of PMC ports that have been allocated to this ops view

Table 2-17 Usage Per Ops View Tab in the License Management Window

Field	Description
LMR Ports	Ops View—Ops view to which this license belongs Current Usage—Number of LMR ports that are in use for this ops view Allocated Ports—Number of LMR ports that have been allocated to this ops view
IP phone Ports	Ops View—Ops view to which this license belongs Current Usage—Number of IP phone ports in use for this ops view Allocated Ports—Number of IP phone ports that have been allocated to this ops view
Multicast Ports	Ops view—Ops view to which this license belongs Current Usage—Number of multicast ports that are in use for this ops view Allocated Ports—Number of multicast ports that have been allocated to this ops view
Dial Ports	Ops View—Ops view to which this license belongs Current Usage—Number of dial ports that are in use for this ops view Allocated Ports—Number of dial ports that have been allocated to this ops view

Understanding Time-bound License Behavior

Time-bound, or evaluation, licenses differ from permanent licenses by the inclusion of a predefined expiration date. For more detailed information and guidelines about time-bound licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide*.

About 30 days before a time-bound license is to expire, Cisco IPICS displays a warning message to alert you. You can dismiss this warning by clicking the **Dismiss** button.

When a license feature expires, the relevant functionality of that license becomes disabled. If the license is an uncounted license, the feature will be disabled; however, if the license is a counted license, the number of ports that correspond to that license type is reduced by the count of the expired license feature. In this case, Cisco IPICS reloads all of the license features when it detects that one or more license features has expired. Expired license features display in the license detail area as flagged items.

Uploading a License File

After you obtain a new Cisco IPICS license file, you must upload it to the Cisco IPICS server before it becomes effective. This procedure copies a license file from the server location where you stored it to the Cisco IPICS server.

Note After you upload the license file, Cisco IPICS places the file in the following directory:
/opt/cisco/ipics/tomcat/versions/5.5.9/webapps/license/

To upload a license file, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Administration > License Management**.

Step 2 In the License File field, enter the path name and file name of the license file to upload to the Cisco IPICS server.

To locate this file in a Choose File window, click **Browse**.

Note If you do not know the path name and file name of the license file, you can click Browse and navigate to the file in the Choose File window.

Step 3 Click **Upload** to upload the file to the Cisco IPICS database.

Step 4 Click **Apply** for the new license to become effective.

Cisco IPICS associates the license file with the server and restarts the license manager.

Note There may be a delay of a few minutes before you can access the Cisco IPICS Administration Console after you click the **Apply** button.

For more information about Cisco IPICS licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide*.

Viewing Active Users

As a Cisco IPICS system administrator, you can view the activity for users who are logged in to the system via PMC and IP phone, and users who are participating in a VTG, by accessing the Administration > Active Users window. This window contains information about each type of user who is logged in to the system, such as the identification of the user, the location of the user, and ops views to which the user belongs. Using this window, you can also manually force logged-in and dialed-in users to log out of Cisco IPICS, if necessary.

To access the Active Users window, navigate to Administration > Active Users.

To view active users and the associated information for each user, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Administration > Active Users**.

Step 2 From the View drop-down list box, choose one of following types of users that you want to view:

- **Logged-in Users**—Users who are logged in to Cisco IPICS
- **PMC Users**—Users who are connected to Cisco IPICS via the PMC
- **IP Phone Users**—Users who are connected to Cisco IPICS via an IP phone

- **Dialed-in Users**—Users who are connected to Cisco IPICS by using the dial-in/invite feature

A window displays a list of the type of users that you chose. See Table 2-18 for a description of the fields in the Active Users window.

Note You can specify the number of rows of active users that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Table 2-18 Active Users Window Fields

Field	Description
Logged-in Users	
User	Name or user ID of user who is logged in to the Cisco IPICS system
Date	Date that the user logged in to the Cisco IPICS system
PMC Users	
User	Name or user ID of the active PMC user
PMC ID	Identification of the PMC for the session
Version	PMC version information that the user is using
Address	IP address of the PMC client machine
Location	Location of the user
Belongs To	Ops view to which the active PMC user belongs
Last Activity	Date and time of the last PMC activity of the PMC user

Table 2-18 Active Users Window Fields (continued)

Field	Description
Status	Indicates the status of a PMC The Status column can contain a status of either Logged-in or Logging-out. The Logging-out status means that the PMC has not yet contacted the server to finalize the PMC session. All resources, including licenses and RMS resources, are deallocated immediately when a user is disabled, or when a PMC session is logged out by using the **Logout** button in the PMC tab in the Active Users window. The PMC session is retained until the server can provide detailed information to the PMC about the conditions of the logout. The server removes logging-out sessions in the following conditions: • The PMC contacts the server. • The server periodically checks (every 60 seconds by default) for sessions which have been active for 10 minutes and removes them in the event of a PMC crash or if the PMC is in offline mode. • At the startup of the Cisco IPICS server.
IP Phone Users	
User	Name or user ID of the active IP phone user
Digit ID	Digit identification number of the active IP phone user
Location	Location of the active IP phone user
Active	Indicates whether the IP phone user is currently active
Remote	Indicates whether the IP phone user is dialed in using a remote connection
Dialed-in Users	

Table 2-18 Active Users Window Fields (continued)

Field	Description
User	Name or user ID of the active dialed-in user
Dial Number	Number that the user dialed when dialing in to Cisco IPICS
Digit ID	Digit identification of the active dialed-in user
Type	Type of talk group This field is empty if the user is dialed in but has not joined any talk group. Type can indicate one of the following resources: • Channel • VTG
Talk Group	Name of the talk group (channel or VTG) that the user has joined This field is empty if the user is dialed in but has not joined any talk group.
Status	Status of the dialed-in user and can be one of the following statuses: • Not Joined—The user is dialed in but has not joined a channel or VTG • Listening—The user is dialed in and has joined a channel or VTG and is listening to that channel or VTG • Talking—The user is dialed in, has joined a channel or VTG, and is currently talking (pressing the PTT button) on that channel or VTG

Step 3 To manually disconnect a logged-in, PMC, or dialed-in user from Cisco IPICS, take any of the following actions:

- To log out a logged-in user, click the **Logged-in** tab.

  - Check the check box to the left of each logged-in user that you want to log out and click **Logout**.

- To log out a PMC user, click the **PMC** tab.
  - Check the check box to the left of each PMC user that you want to log out and click **Logout**.

  When you log out a PMC user, the session is ended and the action cleans up all the PMC resources and marks the session accordingly. If the PMC is not running, the cleanup action completes.

  If the PMC is running and connected to the server, the PMC gets the logout update from the server and logs out accordingly, redisplaying the Login dialog.

  If the PMC is running in offline mode, the PMC continues to run. If the PMC uses multicast communications, there are no effects on the channel. If the PMC uses SIP-based communications, the SIP channels become disconnected.

- To log out a dialed-in user, click the **Dialed-in** tab.
  - Check the check box to the left of each dialed-in user that you want to log out and click **Logout**.

Tip You can log out all users in each tab by checking the check box at the top of each user list and then click **Logout**.

Step 4 To refresh the window of any tab, click the **Refresh** button at the bottom of the list.

Managing Activity Logs

The Cisco IPICS logs store a variety of information about activities relating to VTGs, such as the ops view for each channel, user, and VTG, the creator of log entries, and the time that log activities occurred. You can review this information at any time. Log activity information is also used for historical reporting.

In Cisco IPICS, an activity gets logged once and the log entry remains indefinitely. When entities such as users, locations, channels, and VTGs, get deleted from Cisco IPICS, the corresponding log entries do not get deleted from the activity log table to provide a historical record if needed.

You search for and download activity logs in the Activity Log Management window. This window contains a **Logs** tab and an **Archives** tab. See the "Understanding the Activity Log Management Window" section on page 2-84 for more information about the Activity Log Management window.

Cisco IPICS tracks and logs the date and time that certain types of activities occur. For detailed information about the activity types that are logged in Cisco IPICS, and how to specify what activity types get logged per ops view, see the "Managing Activity Log Options Per Ops View" section on page 2-89.

You can choose how to view activity logs:

- By ops view—Ops views to which the resource belongs
- By channel—Users and VTGs that used that PTT channel
- By user—PTT channels and VTGs in which that user was involved
- By VTG—Users and PTT channels that were participants in that VTG

To view and download activity logs. See the "Viewing and Downloading Activity Logs" section on page 2-85 for more information.

Understanding the Activity Log Management Window

The Activity Log Management window displays each channel, user, or VTG that is configured in Cisco IPICS, depending on the information that you choose to view. It also allows you to perform the activity logs management functions.

The Activity Log Management window contains two tabs, in which you can manage activity log information: the **Logs** tab and the **Archives** tab.

In the **Logs** tab, you can choose to view logs by ops view and resource type (such as channel, user, and VTG), and search for particular logs based on a date range. If you are assigned the system administrator and/or ops view administrator role, you can also apply the date range filter to minimize the logs that get returned from the system. After filtering the activity log resource list by ops view and resource type, you can then choose one of the resources from a single list. For more information about using the search filters, see Chapter 1, "Using Search Windows."

Note Users who are assigned the ops view administrator role can monitor only the activity logs of the ops view to which that user belongs. If a particular ops view is disabled, then all the activity logging is done by using the SYSTEM default ops view. The system administrator is allowed to monitor logs of all the ops views. For more information about Cisco IPICS roles, see the "Cisco IPICS Roles" section on page 1-6.

For information about viewing and downloading Cisco IPICS activity logs, see the "Viewing and Downloading Activity Logs" section on page 2-85.

In the **Archives** tab, you can download activity log files that have been archived according to the threshold limits that are configured in the Administration > Options window. For more information about managing Cisco IPICS options, see the "Managing Cisco IPICS Options" section on page 2-91. For information about downloading archived activity logs, see the "Downloading Archived Activity Logs" section on page 2-88.

To open the Activity Logs Management window, navigate to Administration > **Activity Log Management**.

Viewing and Downloading Activity Logs

To perform detailed analysis of activities, you can view and download activity logs. You can view activity logs for any channel, user, or VTG, based on ops views and resource type. You view and download activity logs in the Activity Log Management window.

When you download activity logs, Cisco IPICS takes these actions:

- Creates an .xml file that contains all activity logs in the period, ops view, and resource type that you designate
- Downloads the .xml file to the location that you specify on the computer from which you are accessing the Administration Console.

The file includes information about the related log entries for the search criteria that you specify (such as ops view, resource type, and date range).

To view and download activity logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Administration > Activity Log Management**.

Step 2 From the drop-down list box in the **Logs** tab, choose the ops view for the activity logs that you want to view and/or download.

Step 3 From the Resource Type drop-down list box, choose the resource type for the activity logs that you want to view and/or download.

Step 4 To view and/or download only the activity logs for a specific resource, enter the name of the resource of the activity logs in the Resource Name field.

Step 5 From the Sort By drop-down list box, choose one of the following options:

- **Date-and-Time**—This option sorts the logs by the date and time of the logs.
- **Initiator-User-ID**—This option sorts the logs by the user who initiated the log entry.
- **Affected-Source-Resource**—This option sorts by the name of the affected resource.
- **Affected-Target-Resource**—This option sorts by the name of the affected target resource.

Step 6 In the From field, specify the beginning date and time of the of the activity logs that you want to view and/or download.

Step 7 In the To field, specify the ending date and time of the activity logs that you want to view and/or download.

Step 8 Click **Go**.

The activity logs display according to the criteria that you choose.

Note You can specify the number of rows of activity logs that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Step 9 To clear your search criteria, click the **Clear Filter** button.

Step 10 To download the logs to your PC, click **Download Activity Logs**.

Step 11 To open the file immediately, click **Open**. To save the file to your PC, click **Save**.

Note The activity log file is in .xml format.

Step 12 To view the activity logs in Microsoft Excel, save the file to a desired location and perform one of the following actions:

Note The following examples were performed by using Microsoft Office Excel 2003.

- Open the Microsoft Excel application and from the File drop-down menu click **Open**.
  - Navigate to the .xml file, highlight the file and click **Open**.
  - In the Open XML dialog box, click the **As an XML List** radio button.

    Microsoft Excel creates a schema that is based on the .xml file source data.
- Navigate to the location where you saved the .xml file, select the file and right-click it.
  - Choose **Open With** and then **Choose Program**.
  - Choose **Microsoft Excel** in the Open With dialog box.

Note If the Excel application does not display in the list of programs, click **Browse** and locate the application.

  - Click **OK**.
  - From the Open XML dialog box, click the **As a read-only workbook** radio button.

Step 13 To view or download archived activity logs, perform the steps in the "Downloading Archived Activity Logs" section on page 2-88.

Downloading Archived Activity Logs

You can download archived activity logs. Cisco IPICS archives the activity logs based on the thresholds that you assigned in the Administration > Options window. For more information about the Options window, see the "Managing Cisco IPICS Options" section on page 2-91.

To download archived activity logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Administration > Activity Log Management**.

Step 2 Click the **Archives** tab.

Table 2-19 shows the fields in the Archive Status pane.

Table 2-19 Archive WIndow Fields

Field	Description
Archive Time—*Display only*	Time when the activity log files were archived in Cisco IPICS
Archive Status—*Display only*	Indicates whether log files were archived successfully
Archive Count—*Display only*	Number of log entries that were archived during the last archive
Archived Files drop-down list box	The file names of the archived files
Download button	Click this button to download archived Cisco IPICS activity logs

Step 3 From the Archived Files drop-down list box, choose the archived activity log file that you want to download.

Note If no log files have been archived, the Archived Files drop-down list box and the Download button are disabled and display as dimmed.

Step 4 Click **Download**.

Step 5 To open this file immediately, click **Open**. To save the file to your PC, click **Save**.

Note Because Microsoft Excel does not support multi-root .xml documents, you can add the text "<activity_logs>" to the beginning and "</activity_logs>" to the end of the downloaded archived activity log file before opening the file. Adding the text changes the file to have only one root element.

If the name of the downloaded archived activity log file is "ipics_activity.xml.<1-24>", rename the file to "ipics_Activity<1-24>.xml" making sure that the .xml extension appears at the end of the file name, before opening in Microsoft Excel. Renaming the file ensures that Excel recognizes the file as an .xml file.

Managing Activity Log Options Per Ops View

You can specify the activities that you want Cisco IPICS to log, by ops view, in the Activity Log Options window. For example, if you want Cisco IPICS to only log when a VTG gets activated in a particular ops view, and no other activities, you would choose the Resource Creation and Deletion activity type for that ops view.

Table 2-20 describes the types of activities that can be logged in by ops views.

Table 2-20 Activity Log Types By Ops View

Activity Type	Description
Cisco Unified IP Phone Activities	Logs are created whenever Cisco Unified IP Phone activities occur in Cisco IPICS.
Dial-in Activities	Logs are created whenever dial-in activities occur in Cisco IPICS.

Table 2-20 Activity Log Types By Ops View (continued)

Activity Type	Description
Licensable Feature Activities	Logs are created whenever feature activities occur, for features that have been licensed in Cisco IPICS.
PMC Activities	Logs are created whenever PMC activities occur in Cisco IPICS.
Resource Association Activities	Logs are created whenever resources are associated in Cisco IPICS.
Resource Creation and Deletion Activities	Logs are created whenever resources, such as VTGs, users, and channels are created or deleted from Cisco IPICS.
System Activities	Logs are created whenever system activities, such as voice resource activities, occur in Cisco IPICS.
Virtual Talk Group Activities	Logs are created whenever VTG activities occur in Cisco IPICS.

You can access the Activity Log Options window by navigating to **Administration > Activity Log Options**.

To manage activity logs per ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Administration > Activity Log Options**.

Step 2 From the Ops View drop-down list box, choose the ops view for which you want to specify the activities to be logged.

Note All the activity types that are available to be logged in Cisco IPICS are listed in the Unselected Activity Types area. In order to specify particular activity types that you want to be logged in Cisco IPICS, for this ops view, you must move them to the Selected Activity Types list. If you do not move any activity types to the Selected Activity Types list, all activity types are logged in this ops view. If you move an activity type to the Unselected Activity Types list, the previously-logged activities of that type are not deleted from the system but they are prevented from being logged in the future.

Step 3 To select the activity types that you want to log in Cisco IPICS for an ops view, take any of the following actions:

- To move an activity type from one list to the other, click the activity type to highlight it and then click > or <. Or, double-click the activity type.
- To move several activity types from one list to the other at one time, Shift+click or Ctrl+click to select the activity types and then click > or <.
- To move all activity types from one list to the other at one time, click >> or <<.

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

If you do not want to save your changes, click **Cancel**.

Managing Cisco IPICS Options

Cisco IPICS provides you with the ability to adjust system preferences and turn on or off certain options in the Options window. Cisco IPICS allows you to restore default settings at any time.

Information in the Options window is contained in the following information tabs:

- **General** tab—Choose this tab to set RMS and activity log options.
- **Passwords** tab—Choose this tab to set the password options for users.
- **PMC** tab—Choose this tab to set PMC configuration options.

Cisco IPICS detects changes that are made to the system options and immediately makes the adjustments for those changes. You do not have to take any further action for the changes to take effect.

You can access the Options window by navigating to **Administration > Options**.

You can use the options in the Options window in the following ways:

- You can customize the Cisco IPICS option settings by editing the fields in the General, Passwords, and PMC tabs.

  Note Ensure that you click **Save** after each change that you make to the settings.

- To restore all settings to the default values, click **Restore Defaults**.

Table 2-21, Table 2-22, and Table 2-23 describe the fields in the Options window.

Table 2-21 General Tab in the Options Window

Setting	Description	Default Setting
Disable RMS Comparator (in the RMS pane)	The RMS comparator is the mechanism that checks the responsiveness of the RMS and if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. Because the RMS comparator can interject delays, you can disable it by checking this check box. **Note** If you connect via a high latency, low bandwidth connection, such as a satellite link, you should check this check box.	This check box is unchecked by default. If the Disable RMS Comparator check box is selected, the RMS Polling Frequency field displays as dimmed.
RMS Polling Frequency	The RMS comparator functionality includes a polling mechanism that regularly checks whether the server can reach all of the RMS components that are listed in the RMS window. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 1-32767	The default interval between checks specifies 10 minutes.

Table 2-21 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Activity Logs (in the Activity Logs pane)	This setting the maximum amount of database space that may be used by Cisco IPICS activity logs. For more information, see Chapter 10, "Understanding Cisco IPICS Serviceability and Diagnostic Information." This setting specifies a value in megabytes (MB). To change the default, double-click the current value and enter a new value. Valid values: 1-250	The default maximum space for activity logs specifies 50 MB.
Activity Log Retention Period	This setting specifies the number of days that Cisco IPICS retains activity log entries. When this number has been reached, the logs get written to a rolling archive log. The archive log files are preserved until they get overwritten when the number of rolling files reaches the maximum number of archive files limit that is set by the system. Valid values: 1-365	The default setting specifies 90 days.

Table 2-22 Passwords Tab in the Options Window

Setting	Description	Default Setting
Minimum Password Length (in the User Passwords pane)	This setting specifies the minimum number of characters that a user can enter when creating or changing the Cisco IPICS password in the **Home > My Profile** window. See the "Managing Your User Profile" section on page 5-2. Use the drop-down list box to choose a new setting. The minimum length can range from 4 to 80 characters. To ensure a strong password, you must create a password that is at least eight characters long, and includes 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: @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ? Valid values: 4-20	The default setting specifies 8 characters.
Minimum Digit Password Length	This setting specifies the minimum number of numeric characters that a user can enter when creating or changing the digit password in the My Profile window, in the Home drawer of the Administration Console. Use the drop-down list to choose a new setting. The minimum length can range from 4 to 10 characters. Valid values: 4-10	The default setting specifies 4 characters.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Lower Case Letter Count	This setting specifies the minimum number of lower case letters that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is set in the Minimum Password Length field. Valid values: 0-76	The default setting specifies 1 character.
Minimum Upper Case Letter Count	This setting specifies the minimum number of upper case letters that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is specified in the Minimum Password Length field. Valid values: 0-76	The default setting specifies 1 character.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Numeric Character Count	This setting specifies the minimum numeric character that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is specified in the Minimum Digit Password Length field. Valid values: 0-76	The default setting specifies 1 character.
Minimum Special Character Count	This setting specifies the minimum special character that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. Valid values: 0-76	The default setting specifies 1 character.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password History Count	This setting specifies the number of passwords that Cisco IPICS will mark as previously used, and that the user will not be able to use again. For example, if the Password History Count is set to 5, then the user will not be able to use any of the passwords that they have used for the previous five times. **Note** This field does not apply to the ipics or ipicsadmin user IDs. Valid values: 0-999	The default setting specifies 5 previous passwords.
Apply User Password Expiration (in Password Expiration pane)	This check box specifies whether Cisco IPICS applies the value that is specified in the Password Expiration field. If this check box is unchecked, then there will be no user password or digit expiration applied. Valid values: true or false	This check box is unchecked by default. If this check box is not selected, the Password Expiration and Password Expiration Notification fields display as dimmed.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration	This setting specifies the number of days in which the Cisco IPICS login password and the digit password will expire. For example, if the value is 180 days, then the password will expire after 180 days from the date that the password was created. **Note** If the value is specified as 0, the password never expires and the message Never Expired displays in the Password Expiration Date field, in the My Profile window for the user. **Tip** After a Cisco IPICS migration occurs, you may want to require all users to update their login passwords for enhanced password security. To force a login password update after a migration, configure the Password Expiration Days setting to 1; then once that one day has passed you can change the setting back to 180 days, or whatever setting you want to specify. This action will force users who log in to Cisco IPICS during that day (after the migration) to change their login passwords. Valid values: 1-999	The default setting specifies 180 days.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration Notification	This setting specifies the number of days before the password expires that the user receives a warning. For example, if the specified number of days is set to 3, the user receives the warning 3 days before password expiration. **Note** This field does not apply to the ipics or ipicsadmin user IDs. **Tip** If the number in this field is specified as 0, the current password expires on the actual password expiration date, and the user will be forced to create a new password at the next Cisco IPICS login. Valid values: 0-999	The default setting specifies 3 days.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Apply User Account Lockout (in the User Account Lockout pane)	This check box specifies whether Cisco IPICS applies the value that is specified in the Maximum Invalid Login Attempts Allowed field. When this check box is checked and a user exceeds the number of invalid login attempts that is specified, the user account is locked and the user can no longer log in to Cisco IPICS until the account is unlocked. For information about how to unlock an account that has been locked, see Chapter 3, "Performing Cisco IPICS Operator Tasks." **Note** This field does not apply to the ipics or ipicsadmin user IDs. If this check box is unchecked, there will be no account lockout applied. Valid values: true or false	This check box is unchecked by default. If this check box is not selected, the Maximum Invalid Login Attempts Allowed and the Failed Password Attempt Expiration fields display as dimmed.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Invalid Login Attempts Allowed	This setting specifies the maximum number of times a user can attempt to log in to Cisco IPICS with invalid login information (user name/password) before the user account gets locked out. The failed login attempts are consecutive. Valid values: 1-999 **Note** The user password invalid attempt count is a separate entity from the digit password invalid attempt count; however, if either password invalid attempt is exceeded, the user account will be locked. When the user account is unlocked, both invalid attempt counts will be reset to 0. When a user gets locked out of Cisco IPICS, a message displays stating that the user ID has been locked and that the user should contact the system administrator or operator for assistance. To unlock a user account, see Chapter 3, "Performing Cisco IPICS Operator Tasks." You can also re-enable a user account by using the enableuser tool. The enableuser tool clears the value that is specified in the Maximum Invalid Login Attempts Allowed field and unlocks the user account. To re-enable a user ID using the enableuser tool, refer to the *Cisco IPICS Troubleshooting Guide, Release 2.0(1)*.	The default setting specifies 5 attempts.

Table 2-22 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Failed Password Attempt Expiration	This setting specifies the number of hours that Cisco IPICS resets the Maximum Invalid Login Attempts Allowed field back to 0 once a user has reached the maximum invalid login attempts. Valid values: 1-999	The default setting specifies 8 hours.

Table 2-23 PMC Tab in the Options Window

Setting	Description	Default Setting
PMC Update Poll (in the Configuration pane)	This setting specifies the frequency that the PMC uses to poll the server for updates. For more information, refer to the *Cisco IPICS PMC Installation and User Guide*. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 3-3600	The default polling interval specifies 5 seconds.
Disable PMC Activity Log Upload (in the PMC Activity Logs pane)	When you check this check box, the PMC does not upload logs to the server. **Note** If you connect via a high latency (high delay), low bandwidth connection, such as a satellite link, you should check this check box. Valid values: true or false	This check box is unchecked by default. If this check box is checked the PMC Log Upload Frequency field and the PMC Send Logs on Rollover fields/check box display as dimmed.

Table 2-23 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Log Upload Frequency (PMC to server)	When a PMC client has activity logs ready to upload to the Cisco IPICS server, the PMC application places the logs in a queue. At regular intervals, the PMC client checks the queue and uploads to the server any logs that are waiting to be uploaded. Log files are copied to the **$TOMCAT_HOME/webapps/ipics_server/pmclogs** directory, and are based on user ID and PMC ID. Log files that are not successfully uploaded get put back in to the queue and are uploaded at a later time. This setting specifies the interval between these checks. For more information, refer to the *Cisco IPICS PMC Installation and User Guide*. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. **Note** Cisco IPICS archives or deletes PMC log files that have been uploaded to the server, such as debug logs, by using an archive utility. This utility runs once a day and checks for log files that are older than 14 days old and deletes them. If the total file size of the files is over 5GB, the oldest files are deleted until the total size drops below 5GB. For detailed information about PMC log files, see "Managing an End Device from the PMC Tab" section on page 3-19. Valid values: 60-32767	The default upload frequency specifies 600 seconds (10 minutes).

Table 2-23 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Send Logs on Rollover	Cisco IPICS defines the PMC UserInterface.log, Authentication.log, and ChannelStatistics.log log files based on a maximum size of 1MB. When any one of these log files reaches this predefined limit, the system creates a new log file. When you enable this option, the Cisco IPICS server retrieves the log files from the PMC based on file size rollover and renames the uploaded log file to reflect an archive copy. If you do not enable this option, the PMC deletes the log files when they reach their maximum size limit. Be aware of the following caveats: • The DebugLog.txt file does not have a size limit of 1MB, and is only uploaded to the server on request or when the PMC is started if this check box is checked (set to true). If this check box is unchecked, the DebugLog.txt file is not uploaded. • The ChannelActivity.log file is uploaded to the server every 10 minutes (or the interval that you configure in the PMC Log Upload Frequency field). Valid values: true or false	The PMC uploads files on rollover (the check box is checked).

Table 2-23 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Activity Log Update	The Cisco IPICS server gathers activity logs from the PMC client machines and updates the database with this information at regular intervals. In the Cisco IPICS database, this data is parsed, organized, and made available for queries from the Activity Log window of the Administration Console. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 30-32767	The default update frequency specifies 600 seconds (10 minutes).

Managing PMC Versions

The Cisco IPICS server maintains a repository of one or more versions of the PMC. PMC updates can be assembled into upgrade packages that you can upload to the Cisco IPICS server.

These updates of the PMC application add features and resolve issues. Users can upgrade their PMC clients at their convenience by downloading the current version of the PMC utility, as described in the "Downloading the PMC" section on page 5-19.

Note You must perform the PMC configuration procedures that are in this section before users can download and install a PMC on their PC clients.

When you initially install Cisco IPICS, a PMC package is included with the server. You must configure the PMC download configuration and generate the PMC Installer in order for that version to be available for download to PMC users.

When a new version of the PMC becomes available, you upload the new PMC package to the Cisco IPICS server making it available for the PMC users to download to their PMC clients. PMC packages are contained in .zip files and can include alert tones and skins.

Each PMC client polls the Cisco IPICS server regularly. As part of this process, the PMC client determines whether there is a new version of a PMC upgrade package to which it can or must update. You configure the recommended PMC versions to designate the PMC version that is available for this update, and to designate whether an update is required or recommended. For more information about configuring the PMC versions, see the "Changing the State of PMC Versions" section on page 2-110.

As a Cisco IPICS system administrator, you can perform the following PMC version management tasks:

- Uploading PMC Versions to the Cisco IPICS Server, page 2-109
- Changing the State of PMC Versions, page 2-110
- Deleting PMC Versions, page 2-112

You perform the PMC version update tasks in the PMC Versions window. For more information about this window, including how to access it, see the "Understanding the PMC Versions Window" section on page 2-107.

Understanding the PMC Versions Window

The PMC Versions window allows you to specify information about PMC versions to use for automatic updates. It also enables you to upload to the Cisco IPICS server the new PMC versions that are used for these updates.

The PMC Versions window lists information about each of the PMC versions that have been uploaded to the Cisco IPICS server.

To display the PMC Versions window, navigate to PMC **Management > PMC Versions**.

Table 2-24 describes the items in the PMC Versions window.

Table 2-24 Item in the PMC Versions Window

Item	Description	Reference
Upgrade Package field	This field contains the PMC version to be uploaded to the Cisco IPICS server.	See the "Uploading PMC Versions to the Cisco IPICS Server" section on page 2-109
Browse button	Click this button to browse to the location that contains the PMC version upgrade package that you can upload to the Cisco IPICS server.	
Upload button	Click this button to upload a new PMC version to the Cisco IPICS server.	
Name field	This field allows you to assign a unique identification to the PMC version upgrade package.	
Version field	This field specifies a unique version number that is assigned to the PMC version upgrade package.	
State field	This field specifies the priority (state) that is assigned to the upgrade package.	See the "Changing the State of PMC Versions" section on page 2-110
Delete button	Click this button to delete a PMC version from the Cisco IPICS server.	See the "Deleting PMC Versions" section on page 2-112

Table 2-24 Item in the PMC Versions Window (continued)

Item	Description	Reference
Drop-down list box for PMC version states	Choose from this list box to configure the state for the PMC versions.	See the "Changing the State of PMC Versions" section on page 2-110
Change State button	Click this button to change the state of the PMC version.	

Uploading PMC Versions to the Cisco IPICS Server

When you upload a new PMC version, the upgrade package file is copied from the stored location on your PC to the Cisco IPICS server.

To upload a PMC upgrade version to the Cisco IPICS server, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > PMC Versions**.

Step 2 To locate the PMC version upgrade package, that you obtained from Cisco, click **Browse**.

Step 3 In the Choose File window, browse to the PMC version that you want to upload and click **Open**.

The file that you choose displays in the Upgrade Package field.

Step 4 Click **Upload**.

Cisco IPICS uploads the file from your PC to the Cisco IPICS server. The PMC version displays in the PMC Versions list.

Note All new PMC versions are saved, by default, in a non-operational state. This means that the PMC users cannot download the version until you change the state. See the "Changing the State of PMC Versions" section on page 2-110 for more information.

Changing the State of PMC Versions

The PMC Versions window enables you to designate the PMC versions that are used for an automatic update by changing the state of the versions. When you specify a PMC version for the automatic update, be aware of this information:

- If you want to force PMC clients to update as soon as possible, choose **Recommended** from the drop-down list box. When you choose this state, the next time that a PMC client polls the server, it compares the PMC version that it is running with the recommended PMC version. If the PMC client does not match the recommended or operational versions, then it automatically downloads the PMC version that is specified in the drop-down list box, automatically updates to that version, and then automatically restarts.
- To force updates immediately, choose **Not Supported** from the drop-down list box. When you choose this state, PMC users who are running this version are forced to restart and download a newer version.

Caution Forcing a PMC automatic update shuts down and then restarts a PMC without warning a user, regardless of the purpose for which the PMC is being used. For this reason, it is recommended that you force an update only when it is absolutely necessary.

- You must upload a PMC version to the Cisco IPICS server before it becomes available in any of the fields in the PMC Versions window.

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

To change the state of PMC versions for automatic updates, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > PMC Versions**.

Step 2 Check the check box next to the PMC version that you want to change.

Step 3 From the drop-down list box, choose any of the following states:

- **Recommended**—This version represents the recommended software version that should be run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform the PMC user. The server then sends this version to the PMC and the PMC installs it after the PMC user responds positively to the message prompt or if other installed versions are not supported.
- **Staged**—This version represents the software version that the PMC downloads according to the discretion of the administrator. The server sends this version to the PMC for download but the PMC does not install it until the administrator changes the state of this version to recommended or operational. At that time, the PMC may install the new version after the PMC user responds positively to the message prompt or if other installed versions are not installed.

  By using the Staged version, the PMC can download the version without installing it. The PMC may download this version but does not install it until the server configuration has been updated to reflect this version as recommended or operational.
- **Operational**—This version represents a version of PMC software that is operational. This version is supported for use with the server but there may be a later version that is also supported.

Note The server always extends priority to the PMC versions that it marks as recommended.

- **Not Supported**—This version represents an unsupported PMC software version. The server does not send this version to the PMC so that the PMC users cannot choose an unsupported version from the drop-down list box in the location dialog box.

Note The server forces an upgrade on any PMC that has installed an unsupported version of software.

Step 4 Click the **Change State** button.

Deleting PMC Versions

To delete PMC versions, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > PMC Versions**.

Step 2 Check the check box of the PMC version that you want to delete.

Step 3 Click **Delete**.

A message displays asking if you want to delete the selected version.

Step 4 Click **OK** to delete the PMC version.

This version of the PMC is completely removed from the server.

If you do not want to delete the PMC version, click **Cancel**.

Managing PMC Alert Tones

PMC tone broadcast wave (.wav) files contain alerting tones, hereafter referred to as *alert tones*, that can be broadcast to a variety of Cisco IPICS users at the same time. Cisco IPICS stores alert tones in a set on the server. The alert tone set is packaged in a .zip file that you can upload to the server, and that PMC users can then download on to their client machines.

An alert tone set is associated with an ops view; therefore, each PMC user can see only one tone set based on the ops view association. For more information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

Note The PMC alert tone feature requires the use of compatible alerting tone files. These files must be .wav files that are encoded in Pulse Code modulation (PCM), which is a sampling technique that digitizes analog signals. These .wav files must be encoded in PCM format with 8 bits monaural samples at 8000 Hz sampling rate, for a total of 64 kbps. While higher and lower bit rates may seem to work, Cisco IPICS does not support the use of any other encoding or bit rates, as they may produce inferior sound quality. (Any file that is used with the G.729 codec may sound inferior due to its encoding algorithms; for more information, refer to the *Cisco IPICS PMC Installation and User Guide*.) In addition, all alerting tones should be encoded to a nominal value of -20 decibels relative to one milliwatt (dBm) and begin and end with zero deflection to eliminate or minimize "popping" or "clicking" sounds.

As a Cisco IPICS system administrator, you can perform the following alert tone management functions:

- Creating a PMC Alert Tone Set, page 2-113
- Adding PMC Alert Tone Sets, page 2-115
- Viewing or Editing PMC Alert Tone Sets, page 2-117
- Associating an Alert Tone Set to an Ops View, page 2-117
- Deleting PMC Alert Tones, page 2-118

Creating a PMC Alert Tone Set

To provide the alert tones that get downloaded to the PMC, you must first create a PMC alert tone set and upload it to the Cisco IPICS server. To create the tone set, perform the following procedure:

Procedure

Step 1 From any PC on which the Cisco IPICS PMC is installed, navigate to the following directory:

[C:\Program Files\Cisco Systems\Cisco IPICS\PMC\Components]

Step 2 Create a new empty directory and extract the sample alert tone set zip file, and all its contents, in to the new directory.

Step 3 Add any desired sound files in .wav format to this directory.

Note These files should be normalized to -2 db and should be encoded by using 8 bit PCM at 8000 Hz.

Step 4 Open the sample alert tone .xml file by using Notepad.

Note The order in which the .wav files appear in the .xml file determine the order in which the alert tones display on the PMC.

Step 5 In Notepad, add new alert tones or delete existing alert tones by following the example below:

```
<file item="1" name="stop.wav" displayName="STOP" type="tone"
priority="required" />
<file item="2" name="message.wav" displayName="Message" type="tone"
priority="required" />
<file item="3" name="siren.wav" displayName="Siren" type="tone"
priority="required" />
<file item="4" name="alert.wav" displayName="Alert" type="tone"
priority="required" />
<file item="5" name="urgent.wav" displayName="URGENT" type="tone"
priority="required" />
```

where:

"*name*" is the .wav file to be played, and "*displayName*" is the text that displays on the PMC.

Note The PMC displays a maximum of 8 characters for the display name.

Step 6 Save the example tone set .xml file and rename the .xml file to an appropriate file name.

Note You must save the .xml file in UTF-8 format. If you are using Notepad, choose UTF-8 from the Encoding drop-down menu in the Save As dialog box.

Step 7 Delete any files from the directory that you do not want.

Step 8 Using file explorer, navigate to the directory that contains the .xml and .wav files and select all of the .wav files and the .xml file.

Tip You can select all of the files by clicking **Ctrl+A**.

Step 9 Right-click the selected files and choose **Send To > Compressed Folder**.

Tip You can also use WinZip or a similar utility to compress the files.

Step 10 To enable the PMC user to press a button on the PMC to stop an alert tone from playing, for displayName enter the name "*STOP*" but give the name an invalid file name, such as "*stopplayout.wav*," then edit the alert tone file with this information, as if it were a real alert tone.

Step 11 You can now upload the compressed PMC alert tone set to the Cisco IPICS server. See the "Associating an Alert Tone Set to an Ops View" section on page 2-117 for information about how to upload a tone set.

Note You can use Windows Sound Recorder to save .wav files in the required format.

Adding PMC Alert Tone Sets

To add a new PMC alert tone set, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Alert Tones**.

Step 2 Click **Add**.

A blank alert tone detail window displays.

Step 3 To locate and upload the alert tone set that you want to add, click **Browse**.

Tip The Stop alert tone should be uploaded to the Cisco IPICS server. This alert tone will allow users to press the Stop alert tone to stop an alert tone that is currently playing. You should ensure that the Stop alert tone is included in an alert tone set that you upload to the Cisco IPICS server. If your tone set does not contain a .wav file called Stop, you can use an alert tone that is named something similar, such as Silence. See the "Creating a PMC Alert Tone Set" section on page 2-113 for information about how to create an alert tone set.

Step 4 In the Set Name field, enter a name for the alert tone set.

Step 5 In the Description field, enter a description for the alert tone set.

Step 6 Click the **Browse** button to upload the alert tone set.

Step 7 Click **Save**.

The tone set gets uploaded to the server and is available for use by PMC users.

The alert tone set name, file size, and MD5 summary information of the new alert tone set also displays.

If you do not want to save your changes, click **Cancel**.

Step 8 To associate an alert tone set to an ops view, click the Ops View tab and follow the steps in the "Associating an Alert Tone Set to an Ops View" section on page 2-117.

Viewing or Editing PMC Alert Tone Sets

To view or edit the PMC alert tone sets that are available for use in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Alert Tones**.

Step 2 Click the link in the Name column for the alert tone set that you want to view or edit.

An alert tones detail window displays current information about the tone set that you chose.

Step 3 To download the alert tone set without making any changes, click the **Download** button.

Step 4 To edit the information for the alert tone set, take any of the following actions:

- In the Name field, enter a new name for the alert tone set.
- In the Description field, enter a new description for the tone set.
- Click the **Browse** button to upload and overwrite the existing tone set.

Step 5 Click **Save**.

If you do not want to save your changes, click **Cancel**.

Step 6 To associate an alert tone set to an ops view, click the Ops View tab and follow the steps in the "Associating an Alert Tone Set to an Ops View" section on page 2-117.

Associating an Alert Tone Set to an Ops View

You can associate an alert tone set to an ops view while you are adding a new alert tone set, or you can associate an ops view to an existing tone set. Associating an alert tone set to an ops view ensures that PMC users can see only the tone set that is associated with the ops view to which they belong.

To associate an alert tone set to an ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Alert Tones**.

Step 2 In the Name column, click the alert tone set link that you want to associate with an ops view.

Step 3 Click the **Ops Views** tab.

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it and then click > or <. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click > or <.
- To move all ops views from one list to the other at one time, click >> or <<.

Step 5 Click **Save** to save the ops view that you want to associate to the alert tone set in the Associated Ops Views list.

PMC users can now only be able to see the alert tone set that is in the ops view to which they belong.

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

Deleting PMC Alert Tones

To delete PMC tones, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Alert Tones**.

Step 2 Check the check box to the left of the name of the tone that you want to delete.

Step 3 Click **Delete**.

The alert tone that you deleted is no longer available for use by the PMC users.

Note If you want to delete all of the existing alert tones, check the check box at the top of the alert tones list and click **Delete**.

Managing PMC Skins

Cisco IPICS supports several different skins that PMC users can use on their PMC. Skins are files, that you create and manage, that are packaged in sets (zip files) that can be downloaded to a PMC, and that form the appearance of the PMC. Once the skin sets are downloaded, PMC users can unpack them and choose from the individual skins, that were contained in the package, to use on their PMCs.

Skins are customizable in Cisco IPICS and are available in various options, including 4, 6, and 18-channel mouse skins and 4 and 8 channel touch screen skins. You control whether PMC users can download only selected PMC skins, or customizable skins.

Cisco IPICS supports only 18 channels to be viewed at a time, and several different skins from which PMC users can choose for the PMC. For more information about using the PMC, refer to the *Cisco IPICS PMC Installation and User Guide*.

Cisco IPICS enables you to upload and manage skin sets that are available to the PMC users. The information about the skin sets, contained in the Skins window, includes the name of the skin set, files size, and the MD5 summary of each skin set. You can use the MD5 summary field to determine whether skin sets get properly uploaded to the server.

Note The MD5 value should never be empty after the skin set has been uploaded to the server. It will only display as blank prior to adding the skin set because the server must process the file before producing the MD5 value.

You can access all skin sets that are currently available on the server by navigating to the PMC Management drawer in the Cisco IPICS Administration Console and clicking the **Skins** link.

You can view and edit existing skin sets, as well as add and delete skin sets, as described in the following procedures:

- Adding PMC Skins, page 2-120
- Viewing or Editing PMC Skins, page 2-120
- Deleting PMC Skins, page 2-121

Adding PMC Skins

To add a new PMC skin set, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Skins**.

Step 2 Click **Add**.

A blank New Skin detail window displays.

Step 3 To locate and upload the skin set that you want to add, click **Browse**.

Step 4 In the Skin Name field, enter a name for the skin set.

Step 5 In the Description field, enter a description for the skin set.

Step 6 Click the **Browse** button to upload the skin set.

Step 7 Click **Save**.

The skin set gets uploaded to the server and is available for download by PMC users.

The skin name, file size, and MD5 summary information of the new skin set also displays.

If you do not want to save your changes, click **Cancel**.

Viewing or Editing PMC Skins

To view or edit the PMC skins that are available for use in Cisco IPICS, perform the following procedure.

Note To add a new skin set, see the "Adding PMC Skins" section on page 2-120.

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Skins**.

Step 2 In the Skin Name column, click the link for the skin set that you want to view or edit.

A skin detail window displays current information about the skin set that you chose.

Step 3 To download the skin set without making any changes, click the skin name link.

Step 4 To edit the information for the skin set, take any of the following actions:

- In the Skin Name field, enter a new name for the skin.
- In the Description field, enter a new description for the skin.
- Click the **Browse** button to upload and overwrite the existing skin.

Step 5 Click **Save**.

If you do not want to save your changes, click **Cancel**.

Deleting PMC Skins

To delete PMC skins, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > Skins**.

Step 2 Check the check box to the left of the Skin Name of the skin set that you want to delete.

Step 3 Click **Delete**.

The skin set that you deleted is no longer available for use by the PMC users.

Note If you want to delete all of the existing skins, check the check box at the top of the skins list and click **Delete**.

Managing the PMC Installer

Before PMC users can download new PMC versions to their clients, you must configure the PMC Installer.

The PMC Installer installs the PMC on to PMC client machines. The PMC package downloads to a PMC client when a PMC user clicks the **Download PMC** link in the Home drawer, as described in the "Downloading the PMC" section on page 5-19.

As a Cisco IPICS system administrator, you can upload a new PMC package, as well as generate the PMC Installer as described in the "Generating the PMC Installer" section on page 2-123.

You perform these tasks in the PMC Installer window. For more information about this window, including how to access it, see thee "Using the PMC Installer Window" section on page 2-122.

Using the PMC Installer Window

The PMC Installer window contains configuration information that is necessary in order to generate a PMC installer.

To display the PMC Installer window, navigate to the PMC Management drawer in the Cisco IPICS Administration Console and click the **PMC Installer** link.

The Installer Status field displays the date and time that a pmcsetup.exe file was last generated, and displays the IP address defined by the bundled pmc.ini file.

Generating the PMC Installer

Generating a PMC Installer installs a new PMC version package, and makes it available for download from the **Download PMC** link in the Home drawer, as described in the "Downloading the PMC" section on page 5-19.

To configure additional PMC options, see the "Managing Cisco IPICS Options" section on page 2-91.

To configure a PMC and generate a PMC Installer, perform the following procedure from the PC on which you stored the PMC version package:

Procedure

Step 1 From the Administration Console, navigate to **PMC Management > PMC Installer**.

Step 2 To choose the IP address that is listed for Server Address, click the radio button next to the IP address that displays.

This address is the IP address that the PMC will use to contact the server. The IP address or hostname of the connected NIC hardware should display as a choice.

Step 3 To configure a different IP address for the PMC, click the **Other** radio button and enter the IP address that you want the PMC to use.

Note If you choose another IP address instead of the configured IP address, that IP address should be tested in the network domain that will be supported with that server. This is in case the PMC cannot connect to the server due to NAT or firewall restrictions.

Step 4 In the HTTP Port field, enter the port number that will be used for non-secure HTTP communication between the PMC and the server.

Step 5 In the HTTPS Port field, enter the port number that will be used for secure HTTPS communication between the PMC and the server.

Note Cisco recommends that you use the default HTTP and HTTPS ports that are listed in the PMC Installer Configuration area. The IP address, HTTP port, and HTTPS port fields affect only the PMC installer and do not have an immediate effect on PMC clients that have already been installed on user PCs. If you need to change these values, then Cisco recommends that you notify all users that they need to download and reinstall the PMC using the new pmcsetup.exe that is generated after you save the changes to these values.

Step 6 In the PMC Version To Be Used For The PMC Installer drop-down list box, choose the version number of the PMC that you want the users to download.

The drop-down list box should be populated with the version numbers of the pmcinst.exe files that have been uploaded to the Cisco IPICS server. See the "Managing PMC Versions" section on page 2-106 for more information.

Note There is only one PMC installer and all PMC users who use that installer will automatically receive a complete application of that PMC version.

Step 7 Click **Save**.

PMC users can now download a new version of the PMC application, as described in the "Downloading the PMC" section on page 5-19.

If you do not want to save your changes, click **Cancel**.

CHAPTER 3

Performing Cisco IPICS Operator Tasks

The Cisco IPICS operator is responsible for setting up and managing Cisco IPICS users and user groups, granting users access to Cisco IPICS and to the PMC, and assigning user channels, roles, and operational views (ops views).

A user can participate in an active VTG and communicate with other VTG participants. A user group is a logical grouping of users. A user group can be added to a VTG, which provides a Cisco IPICS dispatcher with an efficient method of adding several users to a VTG one at a time.

You perform Cisco IPICS operator activities from the User Management drawer in the Cisco IPICS Administration Console. To access this drawer, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-11, then choose the **User Management** drawer in the Server tab. You must be assigned the operator role to access the User Management drawer.

Note

- Some of the explanations and procedures in this chapter refer to information that displays or to tasks that you can perform only if ops views is enabled. For more information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views.".
- Several procedures in this chapter describe how to view or update information for a user from the User Management drawer. Users can also perform many of these procedures for their personal information from the Home drawer. For more information, see Chapter 5, "Performing Cisco IPICS User Tasks."

The following sections describe the operator activities that you can perform from the Cisco IPICS Administration Console:

- Managing Users, page 3-2
- Managing User Groups, page 3-41

Managing Users

A Cisco IPICS user can perform the following activities:

- Access the My Profile window in the Cisco IPICS Administration Console and perform the tasks that are available in that window
- Access channels with which they are associated
- Participate in VTGs to which they are assigned
- Use direct two-way channels to communicate through the PMC over a SIP channel with other associated users with which they are associated
- Communicate through the PMC with associated dial-in users
- Download the PMC installer

This section describes the following user management activities:

- Understanding the Users Window, page 3-3
- Adding a User, page 3-6
- Managing User Information, page 3-9
- Associating Resources with a User, page 3-28
- Managing Ops Views for a User, page 3-34
- Managing Prompts for a User, page 3-36
- Viewing Information about VTGs in which a User is a Participant, page 3-36
- Managing User Status, page 3-37

Understanding the Users Window

The Users window lists information about users that you have added in Cisco IPICS and provides the ability to perform several user management functions. The bottom area of this window displays a list of Cisco IPICS users and general information for each user. By default, this area displays all users, but you can choose to display only those users that match search criteria that you specify in the top area of the window.

To display the Users window, access the User Management drawer and click **Users**.

Table 3-1 describes the items in the Users window.

Table 3-1 Items in the Users Window

Item	Description	Reference
Filters		
User Name field First Name field Last Name field	Provides the ability to display only those users whose user name, first name, or last name begins with the character string that you enter (characters are not case-sensitive)	See the "Using Search Windows" section on page 1-13
Location drop-down list Role drop-down list Ops View drop-down list	Provides the ability to display only those users whose location, role, or associated ops view match the information that you choose	
Go button (in Users area)	Displays users according to the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of users	
User Information		
User Name field	User name assigned to the user	See the "Adding a User" section on page 3-6

Table 3-1 Items in the Users Window (continued)

Item	Description	Reference
Last Name field	Last name of the user	See the "Managing General Information for a User" section on page 3-9
First Name field	First name of the user	
Ops View field	Ops view to which the user belongs	See the "Managing Ops Views for a User" section on page 3-34
End Device Status field	Can display these icons: —Audio of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk or listen in a channel or VTG —Microphone of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk in a channel or VTG	See the "Changing User Status" section on page 3-38 and the "Managing an End Device from the User Management Window" section on page 3-15
Status field	Indicates whether a user is enabled or disabled	See the "Changing User Status" section on page 3-38
Prompt	Indicates whether a spoken name prompt is recorded for the user	See the "Managing Prompts for a User" section on page 3-36
Password Expiration field	Indicates when the password of the user expires	See the "Managing Cisco IPICS Options" section on page 2-91
Account Status field	Shows if a user account is locked or available	See the "Locking or Unlocking a User Account" section on page 3-38
Add button	Provides the ability to add a new Cisco IPICS user	See the "Adding a User" section on page 3-6
Copy button	Provides the ability to copy information from an existing user when you add a new user	
Delete button	Provides the ability to you delete a user	See the "Deleting a User" section on page 3-41

Table 3-1 Items in the Users Window (continued)

Item	Description	Reference
Change Status drop-down list	Provides the ability to enable or disable a user and lock or unlock a user account	See the "Changing User Status" section on page 3-38 and the "Locking or Unlocking a User Account" section on page 3-38
End Device drop-down list	Provides the ability to perform several activities for the PMC, Cisco Unified IP Phone, and dial-in phone of a user	See the "Managing an End Device from the User Management Window" section on page 3-15
Associations button	Displays the Associations window for a user	See these sections: • Associating PTT Channels with a User, page 3-28 • Associating Users with a User to Configure the Direct Two-Way Channel Feature, page 3-30 • Associating Phones with a User to Configure the Direct Dial Feature, page 3-31 • Associating Policies with a User, page 3-32 • Viewing Information about VTGs in which a User is a Participant, page 3-36
Display Controls		
Rows per page drop-down list	Specifies how many rows of users are included in a users list page	See the "Navigating Item Lists" section on page 1-15
Page field	Displays users on a specific page	
|< (First page) button	Displays the first page of the users list	
< (Previous page) button	Displays the previous page of the users list	
> (Next page) button	Displays the next page of the users list	
>| (Last page) button	Displays the last page of the users list	

Adding a User

When you add a user to Cisco IPICS, you assign a user ID to that user and configure several other options for the user.

If you add a user who has the same channel assignments, roles, and other information as that of an existing user, you might find it convenient to start by copying the information of the existing user. When you copy such information, Cisco IPICS opens a New Users window and enters all information that is stored for the existing user, except the user ID, password, digit ID, and digit password (PIN).

Before you add a user, you must configure locations as described in the "Managing Locations" section on page 2-38.

To add a new user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 From the Users area in the Managing Users window, take either of these actions:

- To add a user starting with a blank New User window, click **Add**.
- To add a user starting with a New User window that includes information based on an existing user, check the check box next to the existing user, and then click **Copy**.

Note The **Copy** button is dimmed if you do not check an existing user or if you check more than one existing user.

The New User window displays. If you clicked **Copy**, this window includes information from the existing user, except for the user ID and password.

Step 3 In the New User window, take these actions:

a. In the User Name field, enter a unique identification name for this user.

The User ID can include alphanumeric characters, numbers, underscores (_), and periods (.).

A User ID is not case-sensitive. If a User ID contains alphabetic characters, a user can enter the characters in upper case or lower case when logging in to Cisco IPICS.

b. In the First Name field, enter the First name of the user.

Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (').

c. In the Last Name field, enter Last name of the user.

Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (').

d. In the Password and the Confirm Password fields, enter the password that the user enters when logging in to Cisco IPICS or the PMC. (The actual characters in the password are represented by asterisks (*)).

You specify requirements for passwords, including length and character requirements, in the **Server** tab **> Administration > Options** window.

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

Passwords are case-sensitive. A user must enter a password exactly as it is configured.

e. (Optional) In the Description field, enter a description of, or notes that relate to, the user for your reference.

f. From the Belongs To drop-down list in the Ops Views area, choose the ops view to which the user group belongs.

Step 4 Perform the tasks that are described in Table 3-2, as needed.

You do not need to perform all of these tasks now. You can enter or update much of this information later.

Table 3-2 Tasks for Adding a Cisco IPICS User

Task	Reference
In the Address tab, enter the physical address and the e-mail address for the user.	See the "Managing Address Information for a User" section on page 3-11.
In the General tab, assign one or more Cisco IPICS roles to the user.	See the "Managing Roles for a User" section on page 3-12.
In the General tab, choose the ops view to which this user belongs, and specify the ops views that can access this user.	See the "Managing Ops Views for a User" section on page 3-34.
In the Dial Login tab, enter login information, if the user will access Cisco IPICS from a Cisco Unified IP Phone.	See the "Managing Dial Login Information for a User" section on page 3-13.
In the PMC tab, designate how a user communicates through the PMC, choose whether PMC log files are on or off, and specify debug levels for PMC log files.	See the "Managing an End Device from the PMC Tab" section on page 3-19.
In the Communications tab, specify how a user is contacted when a Cisco IPICS policy engine (hereafter referred to as policy engine) notification action executes or when a Cisco IPICS dispatcher initiates a policy engine dial-out to the user.	See the "Managing Communications Preferences for a User" section on page 3-23.
Associate ops views with the user.	See the "Managing Ops Views for a User" section on page 3-34.

Step 5 Click **Save** to add the user.

If you do not want to add the user, click **Cancel**.

Managing User Information

Cisco IPICS provides the ability for the operator to manage a variety of user information, as described in the following sections:

- Managing General Information for a User, page 3-9
- Managing Address Information for a User, page 3-11
- Managing Roles for a User, page 3-12
- Managing Dial Login Information for a User, page 3-13
- Managing an End Device for a User, page 3-15
- Managing Communications Preferences for a User, page 3-23

Managing General Information for a User

General information for a user includes the name, Cisco IPICS login credentials, and default location of the user.

You can add, view, or update general information for any user. To do so, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 In the User Name column, click the link for the user whose information you want to view or update.

Step 3 Click the **General Information** tab and view or enter the information that is described in Table 3-3.

Table 3-3 General Information

Field	Description
User Name	*Display only.* User name assigned when the user was created.
First Name	First name of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Last Name	Last name of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Password	Password that the user enters when logging in to Cisco IPICS or the PMC. (The actual characters in the password are represented by asterisks (*)). You specify requirements for passwords, including length and character requirements, in the **Server** tab **> Administration > Options** window. Valid characters: alphanumeric characters and these special characters: @ [\ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?.
Confirm Password	Confirmation of the entry in the password field.
Description	Description of, or notes that relate to, the user for your reference.
Password Expiration Date	*Display only.* Indicates when the password of the user expires.

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

If you do not want to save your changes, click **Cancel**.

Managing Address Information for a User

Address information for a user includes the physical address and e-mail address of the user.

You can add, view, or update address information for any user. To do so, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 In the User Name column, click the link for the user whose information you want to view or update.

Step 3 Click the **Address Information** tab and view or enter the information that is described in Table 3-4.

Table 3-4 Address Information

Field	Description
Address	Street address of the user. Valid characters: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :
Address (cont)	Additional street address information. Valid characters: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :
City	City of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
State/Province	State or province of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Country	Country of the user. Valid characters: alphanumeric characters, space, and period (.).

Table 3-4 Address Information (continued)

Field	Description
Zip/Postal Code	Zip code or postal code of the user. Valid characters: alphanumeric characters, space, and period (.).
E-mail	E-mail address of the user. Valid characters: alphanumeric characters, underscore (_), period (.), and at sign (@).

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

If you do not want to save your changes, click **Cancel**.

Managing Roles for a User

Roles determine the Cisco IPICS features that a user can access and the functions that a user can perform. All users are assigned the user role by default. In addition, you can assign one or more of the following roles to a user:

- Dispatcher—Responsible for setting up system policies and setting up VTG templates, activating VTGs to begin conferences, and adding or removing participants in VTG templates and active VTGs. Also monitors active VTGs, and creates and manages policies.
- Operator—Responsible for setting up and managing users, granting access to Cisco IPICS and the PMC, and assigning user channels, roles and ops views.
- Ops view administrator—Manages and monitors the activity logs that are filtered by ops views.
- System administrator—Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. Also creates ops views, manages Cisco IPICS licenses and PMC versions, creates and manages policies, and monitors the status of the system and its users via the activity log files and dashboard.
- All—Equivalent to assigning each of the other roles individually.

To add, view, or change roles for a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **General Information** tab.

Step 4 Choose the desired role from the drop-down list in the Roles area.

When you do so, a new Role field displays, which allows you to assign another role. Repeat this step to assign additional roles.

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

If you do not want to save your changes, click **Cancel**.

Managing Dial Login Information for a User

Dial login information consists of the login credentials that a user enters in the following situations:

- When logging in to the Cisco IPICS service from a Cisco Unified IP Phone. This service allows a Cisco Unified IP Phone user to communicate on PTT channels and participate in channels and VTGs.

  For related information, see Appendix B, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

- When logging in to the policy engine telephony user interface (TUI) from a touch-tone telephone. The TUI allows a phone user to interact with the policy engine.

  For related information, see the "Using the Policy Engine Telephony User Interface" section on page 7-27.

To add, view, or change dial login information for a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Dial Login** tab view or update the information that is described in Table 3-5.

Table 3-5 Dial Login Information

Field	Description
Digit ID	Numeric ID that the user enters when accessing the Cisco IPICS service from a Cisco Unified IP Phone when accessing the TUI. Valid characters: numeric characters.
Digit Password (PIN)	Password that the user enters when accessing the Cisco IPICS service from a Cisco Unified IP Phone or PIN that the user enters when accessing the TUI. (The actual characters in the password are represented by asterisks (*)) You specify requirements for passwords, including length and character requirements, in the **Server tab > Administration > Options** window. Valid characters: numeric characters.
Confirm Digit Password	Confirmation of the entry in the Digit Password (PIN) field.
Default Location	Location from which a phone connects to Cisco IPICS. For additional information about locations, see the "Managing Locations" section on page 2-38.

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

If you do not want to save your changes, click **Cancel**.

Managing an End Device for a User

And end-device can be a PMC, Cisco Unified IP Phone, or dial-in phone. As a Cisco IPICS operator, managing an end device of a user involves the following activities:

- Managing an End Device from the User Management Window, page 3-15—Provides the ability to mute or unmute an end device, disable or enable an end device, and obtain PMC log files
- Managing an End Device from the PMC Tab, page 3-19—Provides the ability to obtain log files, turn log files on or off, set log levels, and designate whether a user can listen or speak in a VTG
- Managing the PMC from the Associations Tab, page 3-21—Provides the ability to control a variety of options for each channel that is associated with a user

Managing an End Device from the User Management Window

From the User Management window, you can perform the following activities for the PMC, Cisco Unified IP Phone, or dial-in phone of a user:

- Mute or unmute the PMC, Cisco Unified IP Phone, or dial-in phone
- Disable or enable the PMC, Cisco Unified IP Phone, or dial-in phone
- Obtain a variety of log files for use in troubleshooting

You can perform these activities for a single user, or for several users at one time.

To manage the end device of a user or users from the User Management window, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Check the check box next to each user whose end device you want to manage.

Step 3 From the End Device drop-down list at the bottom of the window, choose the desired option.

Table 3-6 describes these options.

Table 3-6 PMC Drop-Down List Options

Option	Explanation	Notes
Set Listen Only	Disables the transmission of audio from a PMC, Cisco Unified IP Phone, and dial-in phone, which restricts a user to listening only	Affects any PMC or Cisco Unified IP Phone that a user logs in to, and affects any phone with which the user dials in to the TUI. You can also control whether a user can listen or talk from an end device as described in the "Managing an End Device from the PMC Tab" section on page 3-19 and the "Managing the PMC from the Associations Tab" section on page 3-21.
Unset Listen Only	Enables the transmission of audio from a PMC, Cisco Unified IP Phone, and dial-in phone	

Table 3-6 PMC Drop-Down List Options (continued)

Option	Explanation	Notes
Disable Audio	Disables the microphone and speaker on a PMC or a Cisco Unified IP Phone that is logged into the Cisco IPICS service, which prevents a user from listening and talking	Affects any PMC or Cisco Unified IP Phone that a user logs in to. Does not affect a phone from which a user dials in to the TUI.
Enable Audio	Enables the microphone and speaker on a PMC or a Cisco Unified IP Phone that is logged into the Cisco IPICS service, which allows a user to listen and talk	

Table 3-6 PMC Drop-Down List Options (continued)

Option	Explanation	Notes
Get Authentication Logs	Obtains the PMC authentication log file	If the user is logged into a PMC, copies the specified log file from that PMC to the following location on the Cisco IPICS server: /root/tomcat/current/webapps/ipics_server/pmclogs/<*user_name*>/<*PMC_ID*>/<*folder*> where: • *user_name* is the unique user name assigned to the user • *PMC_ID* is the ID that the system generates for the PMC installation • *folder* the name of the log file type: Authentication, Channel Statistics, User Interface, or Debug Log file naming uses this convention: <*year*>.<*month*>.<*day*>.<*hour(24)*>.<*minute*>.<*second*>.<*millisecond*>.log where *year*, *month*, *day*, *hour(24)*, *minute*, *second*, and *millisecond* identify the date and time that the file was created. If the user is not logged into the PMC, the request for a log file is ignored. When you request a log file, the PMC client closes the file, renames it, and starts a new file. After the renamed file uploads to the Cisco IPICS server, it is deleted from the PMC client. **Note** A log may be empty if logging is not turned on. For descriptions of these log files, refer to the "Using the PMC Application Logs" chapter in *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*. For related information about log files, see the "Managing Cisco IPICS Options" section on page 2-91.
Get Channel Statistics Logs	Obtains the PMC channel statistics log file	
Get User Interface Logs	Obtains the PMC user interface log file	
Get Debug Logs	Obtains the PMC debug log file	

Managing an End Device from the PMC Tab

From the User Management: Users > *Username* > PMC tab, you can perform the following activities for the end device of a user:

- Designate how a user communicates in VTGs
- Obtain PMC log files
- Turn PMC log files on or off and set log levels

To manage the end device of a user from the User Management: Users > *Username* > PMC tab, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **PMC** tab.

Step 4 To designate how a user communicates in VTGs, check the appropriate check boxes in the PMC Info area:

- Disable Audio—Disables the microphone and speaker on a PMC or a Cisco Unified IP Phone that is logged into the Cisco IPICS service. Does not affect a phone from which a user dials in to the TUI.
- Listen Only—Disables the transmission of audio from a PMC, Cisco Unified IP Phone, and dial-in phone, which restricts a user to listening only.
- Allow Latch—User can use the latching feature on a PMC or Cisco Unified IP Phone.
- Advanced PMC Permissions (Multi-select, Tones, DTMF, All Talk)—User can use the Multi-select, Alert Tones, Dual-Tone Multi-Frequency (DTMF), and All Talk features on a PMC.

Step 5 To turn on or set log levels for the PMC log files, take the desired actions:

- Choose whether the following PMC log files are on or off by making a selection from the corresponding drop-down list:
  - Authentication
  - User Interface
  - Channel Statistics
- Choose the debug level for the following PMC log files by making a selection from the corresponding drop-down list:
  - Debug Signaling
  - Debug User Interface
  - Debug Media

Note Do not turn on a PMC log file unless you need it. If you turn on a log file, set it to the lowest debug level that provides the information that you need. Log files can consume significant disk space, and the higher the debug level, the more disk space that is used.

Step 6 To obtain a log file from the PMC, choose one of the following options from the Get Logs from PMC drop-down list, and then click **Get Logs from PMC**:

- **Authentication**—Obtains the PMC authentication log file
- **Channels Statistics**—Obtains the PMC channel statistics log file
- **User Interface**—Obtains the PMC user interface log file
- **Debug**—Obtains the PMC debug log file

If the user is logged into a PMC, clicking **Get Logs from PMC** copies the specified log file from that PMC to the following location on the Cisco IPICS server:

/root/tomcat/current/webapps/ipics_server/pmclogs/<*user_name*>/<*PMC_ID*>/<*folder*>

where:

- *user_name* is the unique user name that is assigned to the user
- *PMC_ID* is the ID that the system generates for the PMC installation

- *folder* is the name of the log file type: Authentication, Channel Statistics, User Interface, or Debug

Log file naming uses this convention:

<*year*>.<*month*>.<*day*>.<*hour(24)*>.<*minute*>.<*second*>.<*millisecond*>.log

where *year*, *month*, *day*, *hour(24)*, *minute*, *second*, and *millisecond* identify the date and time that the file was created.

If the user is not logged into the PMC, the request for a log file is ignored.

When you request a log file, the PMC client closes the file, renames it, and starts a new file. After the renamed file uploads to the Cisco IPICS server, it is deleted from the PMC client.

Note A log file may be empty if logging is not turned on.

For descriptions of the PMC log files, refer to the "Using the PMC Application Logs" chapter in *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*. For related information about log files, see the "Managing Cisco IPICS Options" section on page 2-91.

Step 7 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Managing the PMC from the Associations Tab

From the User Management: Users > *Username* > Associations tab, you can perform the following activities for the PMC, Cisco Unified IP Phone, or dial-in phone of a user:

- Enable or disable the latching feature on a PMC or Cisco Unified IP Phone
- Enable or disable Listen Only on a PMC, Cisco Unified IP Phone, or dial-in phone
- Enable or disable Voice Activation Detection (VAD) on a PMC

You can perform these activities for any or all channels with which the user is associated.

To manage the PMC of a user from the User Management: Users > *Username* > Associations tab, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Associations** button at the bottom of the window.

Step 4 Make sure that the **Channels** tab is selected.

This table displays the channels that are associated with this user. The status field shows whether the channel is enabled or disabled. The Associations Attributes fields display settings for various end device parameters.

Step 5 Check the check box next to each channel for which you want to change the end device status.

Step 6 From the Change PMC Status drop-down list, choose the desired option.

Table 3-7 describes these options.

Table 3-7 PMC Drop-Down List Options

Option	Explanation
Allow Latch	Allows the user to use the latching feature on a PMC or Cisco Unified IP Phone.
Disallow Latch	Prevents the user from using the latching feature on a PMC or Cisco Unified IP Phone.
Set Listen Only	Disables the transmission of audio from a PMC, Cisco Unified IP Phone, or dial-in phone, which restricts a user to listening only.
Unset Listen Only	Enables the transmission of audio from a PMC, Cisco Unified IP Phone, or dial-in phone.

Table 3-7 PMC Drop-Down List Options (continued)

Option	Explanation
Enable Audio	Enables the microphone and speaker on a PMC or a Cisco Unified IP Phone that is logged into the Cisco IPICS service, which allows a user to listen and talk. Does not affect a phone from which a user dials in to the TUI.
Disable Audio	Disables the microphone and speaker on a PMC or Cisco Unified IP Phone that is logged into the Cisco IPICS service, which prevents a user from listening and talking. Does not affect a phone from which a user dials in to the TUI.

Note The options that you choose are applied immediately. You do not need to click **Save** to save changes, and clicking **Cancel** does not cancel changes.

Managing Communications Preferences for a User

Communications preferences specify how the policy engine contacts a user when a policy with which the user is associated executes or when a Cisco IPICS dispatcher initiates a policy engine dial-out call to the user. For more information about the policy engine and messages that users receive when they are contacted, see Chapter 7, "Using the Cisco IPICS Policy Engine" and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

When you specify communication preferences, you can provide the following information:

- Notification Preferences—Any combination of one or more e-mail, Short Message Service (SMS), or pager addresses
- Dial Preferences—One or more telephone numbers

This section includes these topics:

- Viewing, Adding, Editing, or Deleting Communications Preferences, page 3-24
- Changing the Order of Dial Preferences, page 3-27

Viewing, Adding, Editing, or Deleting Communications Preferences

When a policy with which a user is associated executes, the policy engine handles communications preferences for the user as follows:

- Notification Preferences—Policy engine contacts each e-mail, Short Message Service (SMS), or pager address that is specified
- Dial Preferences—If the policy engine is configured to dial, it calls each number in sequence until it reaches a user who enters a valid ID and PIN to confirm receipt of the call

To view, add, edit, or delete notification preferences and dial preferences for a user perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Communications** tab.

This tab displays the following information:

- Type (under Notification Preferences)—Method by which the user is notified:
  - Email—Notification is sent to an e-mail address
  - Pager—Notification is sent to a pager through an e-mail gateway
  - SMS—Notification is sent to an SMS through an e-mail gateway
- Number/Address (under Notification Preferences)—E-mail address for the corresponding notification type
- Type (under Dial Preferences)—Description of the location to be dialed, such as Business, Car, or Home

- Dial Number (under Dial Preferences)—Telephone number of the corresponding location type

Step 4 To add, edit, or delete notification preferences, take the appropriate actions under the Notification Preferences list:

- To add a notification preference:
  a. Click **Add**.
  b. From the drop-down list, choose a method by which the user receives notifications (e-mail, pager, or SMS).
  c. In the field next to the drop-down list, enter the e-mail address for the corresponding notification method.

     For the SMS and Pager methods, the e-mail address is for a gateway through which the message will be sent to the device.
  d. Click **Done**.
  e. Repeat these steps as needed to add more notification preferences.
- To edit a notification preference:
  a. Check the check box next to the notification preference that you want to edit.
  b. Click **Edit**.
  c. From the drop-down list, choose a method by which the user receives notifications.
  d. In the field next to the drop-down list, enter the enter the e-mail address for the corresponding notification method.
  e. Click **Update**.
- To delete a notification preference:
  a. Check the check box next to the notification preference or preferences that you want to delete.
  b. Click **Delete**.

Step 5 To add, edit, or delete dial preferences, take the appropriate actions under the Dial Preferences list:

- To add a dial preference:
  a. Click **Add**.
  b. From the drop-down list, choose a description for the dial preference.
  c. In the field next to the drop-down list, enter the telephone number for the corresponding dial preference.

     The first character must be a digit or a plus sign (+).

     This character can be followed by zero or more of these characters: digits, upper case or lower case letters, space, : . , - ( ) # *.

     One or more digits must be included next.

     The number may end with a digit or with one or more pound signs (#) or asterisks (*).
  d. Click **Done**.
  e. Repeat these steps as needed to add more dial preferences.
- To edit a dial preference:
  a. Check the check box next to the notification preference that you want to edit.

     You can use the Up Arrow and Down Arrow buttons to move a check to an adjacent check box.
  b. Click **Edit**.
  c. From the drop-down list, choose a description for the dial preference.
  d. In the field next to the drop-down list, enter the enter the telephone number for the corresponding dial preference.

     This field can contain numerals, dashes (-), and spaces. If the telephone number includes an extension, precede the extension with an uppercase or lowercase X.
  e. Click **Update**.
- To delete a dial preference:

a. Check the check box next to the dial preference or preferences that you want to delete.

   You can use the Up Arrow and Down Arrow buttons to move a check to an adjacent check box.

b. Click **Delete**.

Step 6 Check the **Dial after sending notifications** check box if you want the policy engine to attempt to call a user on the numbers in the Dial Preference list when a policy with which the user is associated executes.

If you check this check box, the policy engine attempts to call the user even if you do not specify a notification preference.

Step 7 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Changing the Order of Dial Preferences

If you check the **Dial after sending notifications** when you configure communications preferences, the policy engine attempts to call a user on the numbers in the Dial Preference list when a policy with which the user is associated executes. The policy engine calls each number on the list in sequence until it reaches a user who enters a valid ID and PIN to confirm receipt of the call.

To change the order of numbers to call in the dial preferences list, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Click the link in the User Name column for the user.

Step 3 Click the **Communications** tab.

Step 4 Check the check box next to the dial preference type that you want to move to a different position in the list.

Step 5 Click the **Up Arrow** button to move the dial preference up in the list or click the **Down Arrow** button to move it down in the list.

Step 6 Repeat Step 4 and Step 5 as needed to move other dial preferences.

Step 7 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Associating Resources with a User

When you associate a Cisco IPICS resource with a user, you provide the user with access to various features and functions that relate to the resource. You can perform the following association activities:

- Associating PTT Channels with a User, page 3-28
- Associating Users with a User to Configure the Direct Two-Way Channel Feature, page 3-30
- Associating Phones with a User to Configure the Direct Dial Feature, page 3-31
- Associating Policies with a User, page 3-32

Associating PTT Channels with a User

Associating PTT channels with a user has the following effects:

- Causes the channels to appear as channels on the PMC of the user
- Causes the channels to appear on a Cisco Unified IP Phone when the user accesses the Cisco IPIC phone service
- Causes the channels to be available to the user through the policy engine telephony user interface

You can also associate PTT channels with a user in the Channels window. See the "Associating Users to PTT Channels" section on page 2-24 for more information.

To associate PTT channels with a user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions to display the Associations window for the user with whom you want to associate channels:

- Click the link for the user in the User Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name, then click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list is dimmed if you do not check a user or if you check more than one user.

Step 3 In the Associations window, make sure that the **Channels** tab is selected.

This tab shows a list of the channels that are associated with the user, the status of each channel, and information about attributes for devices that use the channel.

Step 4 Click **Add**.

The Search Results window appears.

Step 5 In the Search Results window, locate one or more channels with which to associate with this user by optionally specifying search criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-13.

Step 6 In the Search Results window, check the check box next to each channel that you want to associate with this user and then click **OK**.

The channels that you choose appear in the list of associated channels.

If you want to remove any channel from this list, click the check box next to the channel, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

Associating Users with a User to Configure the Direct Two-Way Channel Feature

Two users who are associated with each other can communicate with each other by using direct two-way channels on their PMC clients. In this way, two online PMC users can communicate with each other even if they are not associated with a channel or are not participants in a VTG.

Associating one user (User A) with another user (User B) has the following effects:

- User B is automatically associated with User A
- The user name of User A appears as a channel on the PMC of user B
- The user name of User B appears as a channel on the PMC of user A

To associate a user with other users, perform the following procedure:

Procedure

Step 1 Take either of these actions to display the Associations window for the user with whom you want to associate users:

- Click the link for the user in the User Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User name, then click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list is dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Users** tab.

This tab shows the user name, last name, first name, and status (enabled or disabled) of each user that is associated with the user that you selected.

Step 3 Click **Add**.

The Search Results window appears.

Step 4 In the Search Results window, locate one or more users with which to associate with this user by optionally specifying search criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-13.

Step 5 Check the check box next to each user that you want to associate with this user and then click **OK**.

The users that you choose appear in the list of associated users.

If you want to remove any user from this list, click the check box next to the user, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

Associating Phones with a User to Configure the Direct Dial Feature

When you associate phones with a user, the user can communicate directly with those phones by using the policy engine direct dial feature.

For information about configuring direct dial, see the "Managing the Direct Dial Feature" section on page 8-37.

To associate phones with a user, perform the following procedure:

Procedure

Step 1 Take either of these actions to display the Associations window for the user with whom you want to associate phones:

- Click the link for the user in the User Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name, then click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list is dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Phones** tab.

This tab shows the dial destination and label of each phone that is associated with this user.

Step 3 Click **Edit**.

The Phone Associations window displays. This window shows the following information:

- Available Phones—Direct dial numbers that can be associated with this user
- Associated Phones—Phones that are associated with the user or that will be associated with the user after you click **Save**

Step 4 Take any of these actions:

- To move a phone from one list to the other, click the phone to highlight it and then click **>** or **<**. Or, double-click the phone.
- To move several phones from one list to the other at one time, Shift+click or Ctrl+click to select the phones and then click **>** or **<**.
- To move all phones from one list to the other at one time, click **>>** or **<<**.

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

If you do not want to save your changes, click **Cancel**.

Associating Policies with a User

When you associate policies with a user, the user can perform the following activities:

- Activate the policy from the Policies window, as described in the "Activating a Policy Manually" section on page 7-21.
- Activate the policy by calling the policy engine. For related information, see the "Using the Policy Engine Telephony User Interface" section on page 7-27.
- Use the 1 through 9 keys on a telephone as *hot keys* to quickly activate a policy that is associated with the corresponding key.

To associate policies with a user, perform the following procedure.

Note You can also associate policies with a user as described in the "Associating Users with a Policy" section on page 7-19.

Procedure

Step 1 Take either of these actions to display the Associations window for the user with whom you want to associate policies:

- Click the link for the user in the User Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name, then click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list is dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Policies** tab.

This tab shows the name and type of each policy that is associated with the user.

Step 3 Click **Edit**.

The Policy Associations window displays. This window shows the following information:

- Available Policies list—Policies that can be associated with this user
- Associated Policies list—Policies that are associated with the user or that will be associated with the user after you click **Save**

Step 4 Take any of these actions:

- To move a policy from the one list to the other, click the policy to highlight it and then click **>** or **<**. Or, double-click the policy.
- To move several policies from one list to the other at one time, Shift+click or Ctrl+click to select the policies and then click **>** or **<**.
- To move all policies from one list to the other at one time, click **>>** or **<<**.

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

If you do not want to save your changes, click **Cancel**.

A user can access any of the first nine policies in the list of policies by pressing the corresponding key on a touch tone telephone. The first policy corresponds to the 1 key on a telephone, and the ninth policy corresponds to the 9 key on a telephone.

To change the position of a policy, check the check box next to it, then use the up arrow button or the down arrow button to move it up or down in the list.

Managing Ops Views for a User

Managing ops views for a user involves these activities:

- Choosing an Ops View to Which a User Belongs, page 3-34
- Associating Ops Views with a User, page 3-35

Choosing an Ops View to Which a User Belongs

A user can belong to one ops view. To specify this ops view, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 In the User Name column, click the link for the user with which you want to associate an ops view.

Step 3 Choose the **General** tab.

Step 4 Choose the ops view to which the user group belongs from the Belongs To drop-down list in the Ops Views area.

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

If you do not want to save your changes, click **Cancel**.

Associating Ops Views with a User

You can specify one or more ops views that can access a particular user.

To see a the ops views that can access a user, from the User Management drawer in the Cisco IPICS Administration Console, click **Users**, choose the **General** tab, and look at the Accessible To list in the Ops Views area.

To specify the ops views that can access a particular user, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions to associate ops views with a user:

- Click the link for the user in the User Name column, click the **General** tab, and then click **Edit** in the Ops View area.
- Check the check box to the left of the User Name of the user, then choose **Ops Views** from the Associate drop-down list at the bottom right of the Users window.

Note The **Associate** button is dimmed if you do not check a user or if you check more than one user.

The Ops View to User Association window displays. This window shows the following information:

- Available Ops Views—Ops views that have been configured in Cisco IPICS and that can be associated with the user
- Associated Ops Views—Ops views that are associated with the user or that will be associated with the user after you click **Save**

Step 3 Take any of these actions:

- To move an ops view from the one list to the other, click the ops view to highlight it and then click > or <. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click > or <.
- To move all ops views from one list to the other at one time, click >> or <<.

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

If you do not want to save your changes, click **Cancel**.

Managing Prompts for a User

If you are using the policy engine, a user can have an associated spoken name prompt. This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface.

The prompt field in the Users window indicates whether a spoken name prompt is recorded. You can record and manage the spoken name prompt for a user by clicking the **Not Recorded** or the **Recorded** link for the user in the prompt column.

When you click a link in the Prompt column, the Spoken Names window displays. If you clicked **Not Recorded**, the system provides the ability to record the prompt for the first time. If you clicked **Recorded**, the system provides the ability to rerecord the prompt. For instructions about how to record or rerecord a prompt, see the "Recording a Spoken Name Prompt" section on page 8-25.

Viewing Information about VTGs in which a User is a Participant

You can view a list of VTGs in which a user is a participant, and you can view the status of those VTGs. A user becomes a participant of a VTG in the following ways:

- A Cisco IPICS dispatcher adds the user to a VTG
- A Cisco IPICS dispatcher adds a user group that includes the user to the VTG

For related information, see Chapter 4, "Performing Cisco IPICS Dispatcher Tasks."

To view a list of VTGs in which a user is a participant, perform the following procedure:

Procedure

Step 1 Take either of these actions to display the Associations window for the user for whom you want to view associated VTGs:

- Click the link for the user in the User Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the User Name, then click the **Associations** button at the bottom of the Users window

Note The Associate drop-down list is dimmed if you do not check a user or if you check more than one user.

Step 2 In the Associations window, click the **Virtual Talk Groups** tab.

This tab shows the VTGs that are associated with the user and the status of each VTG.

Managing User Status

Managing the status of a user can involve specifying whether a user can access Cisco IPIC or removing a user from the system. For detailed information about managing user status, see the following sections:

- Changing User Status, page 3-38
- Locking or Unlocking a User Account, page 3-38
- Recovering a Deleted System Administrator User, page 3-40
- Deleting a User, page 3-41

Changing User Status

A user can have either of these statuses:

- Enabled—User can log in to Cisco IPICS from an end device (PMC, Cisco Unified IP Phone, and dial-in phone).
- Disabled—User cannot log in to Cisco IPICS from any end device. (PMC, Cisco Unified IP Phone, and dial-in phone)

  If you disable a user who is currently logged in to Cisco IPICS, that login session is automatically terminated.

You can change the status of a single user or you can change the status of several users at one time.

To determine the current status of a user, access the User Management drawer, click **Users**, and look at the information in the Status column for the user.

To change the status of a user or users, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions:

- Click the link for the user in the User Name column to display the User Management window for the user, and click **Enable** or **Disable**.

  The **Enable** or **Disable** button appears at the bottom left of the user management window. The name of the button depends on the current status of the user.
- Check the check box next to each user whose status you want to change, then choose the desired action (**Enable Users** or **Disable Users**) from the Change Status drop-down list.

Locking or Unlocking a User Account

A user whose account is locked cannot log into the Cisco IPICS system. Existing logins continue to work until the user logs out of the system.

A user account can be locked in the following ways:

- By the user exceeding the designated number of invalid login attempts when the Cisco IPICS administrator has configured user lockout. For more information, see Chapter 2, "Performing Cisco IPICS System Administrator Tasks.".
- When a Cisco IPICS operator locks the user account as described in this section.

A Cisco IPICS operator must unlock a locked user account before the user can log into Cisco IPICS.

Note Only the operator or All roles can unlock a user account as described in this section. If there is no user with these roles available to access Cisco IPICS (because, for example, they are locked themselves), you can use the enableuser command to unlock a user account. For more information about the enableuser command, refer to *Cisco IPICS Troubleshooting Guide*.

To lock or unlock a user account, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of these actions:

- Click the link for the user in the User Name column to display the User Management window for the user, and click **Lock** or **Unlock**.

  The **Lock** or **Unlock** button appears at the bottom of the user management window. The name of the button depends on the current status of the user account.
- Check the check box next to each user whose status you want to change, then choose the desired action (**Lock Account** or **Unlock Account**) from the Change Status drop-down list.

Recovering a Deleted System Administrator User

You can recover deleted system administrators by logging in as an operator and creating a new system administrator user ID.

Note You must have operator privileges to recover a deleted system administrator user ID.

To recover the system administrator role, perform the following procedure:

Procedure

Step 1 Log in to the server by using the operator user name and password.

Step 2 From the User Management drawer in the Administration Console, click **Users**.

Step 3 Click **Add**.

Step 4 In the required fields, which are indicated by an asterisk, enter the user information.

Step 5 From the Roles drop-down list box, choose **System Administrator** or **All** for the user role.

The new user appears in the SYSTEM ops view and can perform administrative tasks.

For more detailed information about adding a new user, see the "Adding a User" section on page 3-6.

Deleting a User

If a user is no longer needed, you can delete it from Cisco IPICS. You can delete a single user or you can delete several users at one time.

If you delete a user who is logged in to Cisco IPCS or who has active connections to Cisco IPICS (for example, a user who is associated with an active VTG), Cisco IPICS disables the user and then removes the user.

To delete a user or users, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Check the check box next to each user that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the user or users, click **Cancel**.

Managing User Groups

A user group is a logical grouping of users. When a Cisco IPICS dispatcher adds a user group to a VTG, all users in that group become participants in the VTG.

This section describes the following user group management activities:

- Understanding the User Groups Window, page 3-42
- Adding a User Group, page 3-43
- Adding Members to a User Group, page 3-45
- Managing Ops Views for a User Group, page 3-46
- Changing the Name of a User Group, page 3-49

- Viewing Information about VTGs in Which a User Group is a Participant, page 3-49
- Deleting a User Group, page 3-50

Understanding the User Groups Window

The User Groups window lists information about each of the user groups that you have added in Cisco IPICS. It also provides the ability to perform several user group management functions.

To display the User Groups window, access the User Management drawer and click **User Groups**.

Table 3-8 describes items in the User Groups window.

Table 3-8 Items in the User Groups Window

Items	Description	Reference
Filters		
Name field	Provides the ability to display only those users whose user name, first name, or last name begins with the character string that you enter (characters are not case-sensitive)	See the "Using Search Windows" section on page 1-13
Ops View drop-down list	Provides the ability to display only those users who are associated with ops views that match the information that you choose	
Go button (in Users area)	Displays users according to the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of users	
User Group Information		
User Group Name field	Name assigned to the user group	See the "Adding a User Group" section on page 3-43
Ops View field	Ops view to which the user group belongs	See the "Managing Ops Views for a User Group" section on page 3-46

Table 3-8 Items in the User Groups Window

Items	Description	Reference
Add button	Provides the ability to add a new user group	See the "Adding a User Group" section on page 3-43
Copy button	Provides the ability to copy information from an existing user group when you add a new user group	
Delete button	Provides the ability to delete a user group	See the "Deleting a User Group" section on page 3-50
Associations button	Displays the Associations window for a user group	See the "Viewing Information about VTGs in Which a User Group is a Participant" section on page 3-49
Display Controls		
Rows per page drop-down list	Specifies how many rows of users are included in a users list page	See the "Navigating Item Lists" section on page 1-15
Page field	Displays users on a specific page	
|< (First page) button	Displays the first page of the users list	
< (Previous page) button	Displays the previous page of the users list	
> (Next page) button	Displays the next page of the users list	
>| (Last page) button	Displays the last page of the users list	

Adding a User Group

Adding a user group makes it available to Cisco IPICS.

If you add a user group that belongs to the same ops view or that has the same members as an existing user group, you may find it convenient to start by copying the information of the existing user group. When you copy such information, Cisco IPICS opens a New User Group area, and enters information that is stored for the existing user group, except the user group name.

You may find it useful to create and name user groups according to location (for example, South Side users) or function (for example, Translators).

To add a new user group, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the Manage Users: User Groups area, take either of these actions:

- To add a user starting with a blank New User window, click **Add**.
- To add a user group starting with a New User window that includes information based on an existing user group, check the check box next to the existing user group and then click **Copy**.

Note The **Copy** button is dimmed if you do not check an existing user group or if you check more than one existing user groups.

The New User Group area displays. If you clicked **Copy**, this window includes information from the existing user group, except for the user group name.

Step 3 In the User Group Name field, enter a name for this user group.

The name can include alphanumeric characters, spaces, and any of these special characters: . , – ‘ # ( ) / :_.

In the Description field, enter a description for the user group.

Step 4 From the Ops View drop-down list, choose the ops view to which this user group belongs.

Step 5 Perform the tasks that are described in Table 3-9, as needed.

You do not need to perform all of these tasks now. You can enter or update any of this information later.

Table 3-9 Tasks for Adding a Cisco IPICS User

Task	Reference
In the General tab, specify the ops views that can access this user group	See the "Managing Ops Views for a User Group" section on page 3-46
After you save the user group, in the Members tab, specify users that are members of this user group	See the "Adding Members to a User Group" section on page 3-45.

Step 6 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Adding Members to a User Group

A user who you add to a user group becomes a *member* of that user group. A user group can have an unlimited number of members, and a user can be a member of an unlimited number of user groups.

Note You cannot add a user to a user group that is a participant in an active VTG. You must remove the user group from the VTG before you add a user to it.

To add members to a user group, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the User Group Name column, click the link for the user group to which you want to add members.

Step 3 Choose the **Members** tab.

This tab displays the following information for each member of this user group:

- User Name—User name assigned to the user
- Last Name—Last name of the user
- First Name—First name of the user
- End Device Status—Can display these icons:
  - —Audio of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk or listen in a channel or VTG
  - —Microphone of the PMC, Cisco Unified IP Phone, and dial-in phone of the user is disabled, so user cannot talk in a channel or VTG
- Status—Indicates whether a user is enabled or disabled
- Account Status—Shows if a user account is locked or available

Moving a user from the Group Members list to the Available Users list removes that user from the user group.

The Search Results window appears.

Step 4 In the Search Results window, locate one or more users to add to this user group by optionally specifying filter criteria and then clicking **Go**.

For instructions about using the search results window, see the "Using Search Windows" section on page 1-13.

Step 5 In the Search Results window, check the check box next to each user that you want to add to this user group and then click **OK**.

The users that you choose appear in the list of members.

If you want to remove any user from this list, click the check box next to the user, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

Managing Ops Views for a User Group

Managing ops views for a user group involves these activities:

- Choosing an Ops View to which a User Group Belongs, page 3-47
- Associating Ops Views with a User Group, page 3-47

Choosing an Ops View to which a User Group Belongs

A user group can belong to one ops view. To specify this ops view, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the User Group Name column, click the link for the user group with which you want to associate an ops view.

Step 3 Choose the **General** tab.

Step 4 Choose the ops view to which the user group belongs from the Belongs To drop-down list in the Ops Views area.

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

If you do not want to save your changes, click **Cancel**.

Associating Ops Views with a User Group

You can specify one or more ops views that can access a particular user group.

To see a the ops views that can access a user group, from the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**, click the link for the user group, and look at the Accessible To list in the Ops Views area.

To choose the ops views that can access a particular user group, perform this procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 Take either of these actions to associate ops views with a user group:

- In the User Group Name column, click the link for the user group, click the **General** tab, and then click **Edit** in the Ops View area.
- Check the check box to the left of the User Group Name of the user group, then click **Associate Ops Views** at the bottom right of the User Groups window.

Note The **Associate Ops Views** button is dimmed if you do not check a user group or if you check more than one user group.

The Ops View to User Association window displays. This window shows the following information:

- Available Ops Views—Ops views that have been configured in Cisco IPICS and that can be associated with the user group
- Associated Channels list—Ops views that are associated with the user group or that will be associated with the user group after you click **Save**

Step 3 Take any of these actions:

- To move an ops view from the one list to the other, click the ops view to highlight it and then click **>** or **<**. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, Shift+click or Ctrl+click to select the ops views and then click **>** or **<**.
- To move all ops views from one list to the other at one time, click **>>** or **<<**.

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

If you do not want to save your changes, click **Cancel**.

Changing the Name of a User Group

You can change the name of a user group at any time. To do so, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 In the User Group Name column, click the link for the user group whose name you want to change.

Step 3 Choose the **General** tab.

Step 4 In the User Group Name field, enter a new name for this user group.

The name can include alphanumeric characters, spaces, and any of these special characters: . , – ‘ # ( ) / :_.

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

If you do not want to save your changes, click **Cancel**.

Viewing Information about VTGs in Which a User Group is a Participant

You can view a list of VTGs in which a user group is a participant, and you can view the status each VTG. A user group becomes a participant in a VTG when a Cisco IPICS dispatcher adds the user group to a VTG.

For related information, see Chapter 4, “Performing Cisco IPICS Dispatcher Tasks.”

To view a list of VTGs in which a user group is a participant, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 Take either of these actions:

- In the User Group Name column, click the link for the user group, and then click **Associations** at the bottom of the Users window.
- Check the check box to the left of the User Group Name of the user group, and then click **Associations** at the bottom of the User Groups window.

The following information displays for each VTG in which the user is participating:

- VTG Name—Name of the VTG
- Status—Whether the VTG is active or inactive

Deleting a User Group

You can delete a user group when you no longer need it to organize users. You can delete a single user group or you can delete several user groups at one time.

Note You cannot delete a user group that is a participant in an active VTG or that is a member of a VTG template. You must remove the user group from the VTG before you delete it.

To delete a user group, perform the following procedure:

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **User Groups**.

Step 2 Check the check box next to each user group that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the user group or groups, click **Cancel**.

Performing Cisco IPICS Dispatcher Tasks

A Cisco IPICS dispatcher is responsible for setting up virtual talk group (VTG) templates, activating VTGs to begin conferences, and adding or removing members or participants in VTG templates and active VTGs. A dispatcher also monitors active VTGs, notifies participants about active VTGs, and can mute and unmute PMC users as necessary.

In addition, a dispatcher manages policies, each of which activates a VTG template at a particular time and then deactivates it after a designated interval. Policy management activities are performed in the Policy Engine tab of the Cisco IPICS Administration Console. For more information about the policy engine, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine," and Chapter 7, "Using the Cisco IPICS Policy Engine."

Note Only a dispatcher or an operator who belongs to a certain ops view should create, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are associated with that ops view. This situation can cause inconsistencies when users view policies. For more information, see Chapter 7, "Using the Cisco IPICS Policy Engine," and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

You perform the Cisco IPICS dispatcher activities from the VTG Management window in the Administration Console. To access this window, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-11. Navigate to **VTG Management > Virtual Talk Groups**.

Note You must be assigned the dispatcher role to access the Dispatcher window.

Note Cisco IPICS allows more than one dispatcher to log in to the system at a time. This situation requires coordination between dispatchers because the users, channels, or groups that are committed to a VTG by one dispatcher may be required by another. The Cisco IPICS operational views, also referred to as *ops views*, feature provides a way to handle this situation. With this feature, a dispatcher sees only the VTG participants that have been assigned to a particular ops view. For more information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

Managing VTGs

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

You can stage a VTG by creating a VTG template, which is an inactive VTG. You use a VTG template to arrange participants that can communicate when you activate the VTG template. You can create as many VTG templates as necessary and activate any of them when needed.

After you activate the VTG, you can easily manage it by adding and removing users, PTT channels, and other VTGs, notifying and dialing out to VTG participants, and by muting and unmuting PMC users.

This chapter describes information about how to manage VTGs and includes the following sections:

- Understanding Virtual Talk Groups Window Icons, page 4-6
- Managing VTG Templates, page 4-7

- Managing Active VTGs, page 4-17
- Using the Search Utility, page 4-34

You perform the VTG management tasks in the **VTG Management > Virtual Talk Groups** window. For more information about this window, including how to access it, see the "Understanding the Virtual Talk Groups Window" section on page 4-3 and the "Understanding Virtual Talk Groups Window Icons" section on page 4-6.

For related information, see the "Best Practices for Managing VTGs" section on page 4-37.

Understanding the Virtual Talk Groups Window

As a Cisco IPICS dispatcher, you perform dispatcher tasks in the Virtual Talk Groups window. The Virtual Talk Groups window lists information about each of the VTG templates that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS VTGs and general information for each VTG. By default, this area displays all VTGs, but you can choose to display only VTGs that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of VTGs that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Table 4-1 describes the items in the Virtual Talk Groups window.

Table 4-1 Items in the Virtual Talk Groups Window

Item	Description	Reference
Filter		
VTG Name field	This field enables search for only the VTG names that begin with the character string that you enter (characters are not case-sensitive).	To limit the display of VTGs or to display a certain VTG, enter the desired filter criteria in the filter field and then click **Go**.
Go button	Click this button to display VTGs by the search criteria that you choose.	
Clear Filter button	Click this button to remove filter selections and display an empty list of VTGs.	
VTG Information		
VTG Name field	This field specifies a unique identification name that is assigned to the VTG template.	See the "Managing VTG Templates" section on page 4-7
Status field	This field indicates whether a VTG is active or inactive.	See the "Managing Active VTGs" section on page 4-17

Table 4-1 Items in the Virtual Talk Groups Window

Item	Description	Reference
Prompt field	This field indicates whether a spoken name is recorded for the VTG template. This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface. You can record the spoken name prompt for a user by clicking the **Not Recorded** or the **Recorded** link in the Prompt column. When you click a link in the Prompt column, the Spoken Names window displays.	See the "Managing Prompts" section on page 8-10
Add button	Click this button to add a new Cisco IPICS VTG template.	See the "Adding a New VTG Template" section on page 4-10 and the "Modifying a VTG Template" section on page 4-14
Delete button	Click this button to delete a VTG template.	See the "Deleting a VTG Template" section on page 4-16
Change Status drop-down list box	Choose from this drop-down list box to activate or deactivate a VTG template.	See the "Changing the Status of a VTG Template" section on page 4-19

The individual VTG windows contain information tabs:

- **General** tab—This tab allows you to manage information about the VTG template, such as VTG name, description, and VTG status.
- **PMC** tab—This tab allows you to set attributes for the PMC.

- **Participants** tab—This tab allows you to view available resources and current VTG participants, add and remove channels, users, and other VTGs from the VTG template, activate and deactivate the VTG, and execute various activities within the active VTG. Activities that you can execute include notifiying users, dialing out to specific VTG participants, and enabling/disabling PMC attributes.

To access the Virtual Talk Groups window, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-11, then navigate to **VTG Management > Virtual Talk Groups**.

Note You must be assigned the dispatcher role to access the Virtual Talk Groups window.

For more information about managing VTG templates and active VTGs, see the "Managing VTG Templates" section on page 4-7, and the "Managing Active VTGs" section on page 4-17.

For information about the icons in the Virtual Talk Groups window, see the "Understanding Virtual Talk Groups Window Icons" section on page 4-6.

Understanding Virtual Talk Groups Window Icons

Various icons in the Virtual Talk Groups window provide important information. Some icons in the Resources area display with an arrow to their left. You can use this arrow to expand the area to show more information about the resource, such as how many users are in a user group or PTT channels in a channel group.

When you disable users and channels in Cisco IPICS, they get disconnected from any active VTGs but still display in the Participants tab of the active VTG, with a blue X and/or text status to the right of the user or channel. You can modify any attribute on a user or channel while it is disabled.

Table 4-2 describes the icons that can display in the Virtual Talk Groups window.

Table 4-2 VTG Workspace Window Icons

Icon	Meaning
	User
	User group
	PTT channel
	PTT channel group
	VTG
	Unavailable VTG channel For more information, see the "Reactivating a VTG" section on page 4-32.

Managing VTG Templates

A VTG template lets you create various arrangements of members (users, PTT channels, and VTGs), without committing network resources or affecting VTGs that are in progress. A dispatcher can activate a VTG template at any time, which brings the VTG participants together into a live conference.

You can view information about any VTG template by clicking the VTG name that displays in the Virtual Talk Groups window. Information about the template displays in a separate window.

When you modify a VTG template, no changes occur in system resources or in the communication between participants until you activate the VTG template. When you make changes to an active VTG, the original template remains unchanged.

:The following sections describe information about managing VTG templates:

- Guidelines for Managing VTG Templates, page 4-8
- Adding a New VTG Template, page 4-10
- Modifying a VTG Template, page 4-14
- Deleting a VTG Template, page 4-16

You perform the VTG template management tasks in the Administration Console Virtual Talk Groups window. For more information about this window, including how to access it, see the "Understanding the Virtual Talk Groups Window" section on page 4-3.

Guidelines for Managing VTG Templates

When you are managing VTG templates, be sure to adhere to the following guidelines:

- A Cisco IPICS user can appear more than once in a list of VTG members. For example, the user could be added individually and as part of one or more user groups. When the VTG becomes active, Cisco IPICS recognizes such multiple appearances as a single user.
- If you drag a user or a PTT channel into a VTG from the Users or Channels lists and that user or PTT channel already exists in a group within the VTG, the channel or user name does not appear another time as an individual user or PTT channel. If you drag a user or PTT channel into a VTG individually and then add a group that contains the user or PTT channel, Cisco IPICS does display the user or PTT channel in the group and individually.
- Cisco IPICS allows you to create blank VTGs, which are VTGs with no participants. You can activate a blank VTG and then add participants to it.
- When adding VTGs to another VTG, each VTG that you add is called a sub-VTG. Activating the top-level VTG activates any sub-VTGs. Activating a sub-VTG does not activate the top-level VTG.
- You cannot make a VTG a participant of itself or create a VTG that would result in a loop of VTGs. For example, if you place VTG-A into VTG-B, you cannot place VTG-B into VTG-A.

  Similarly, if VTG-A contains the sub-VTG-D and VTG-C contains the sub-VTG-D, you cannot add VTG-C to VTG-A.

If you try to activate any channels or VTGs that, when activated, will cause an audio loop, Cisco IPICS detects this action and does not activate them. They display crossed out in the VTG list.

- Mixing secure and non-secure channels in the same VTG is not recommended because users on secure channels will be able to hear users on non-secure channels.
- When you click a specific VTG from the VTG Management > Virtual Talk Groups window, the Participants information displays, from which you can view all available VTG resources that are configured in Cisco IPICS. For more information, see the "Adding a New VTG Template" section on page 4-10.
- To add a PTT channel, drag the channel name that you want to add from the Channels Resources area to the Participants area.
- To add a PTT channel group, drag the channel group name that you want to add from the Channels Resources area to the Participants area.
- To add a user, drag the user name that you want to add from the Users Resources area to the Participants area.
- To add a user group, drag the user group name that you want to add from the Users Resources area to the Participants area.
- To add a VTG, drag the VTG name that you want to add from the Resources area to the Participants area. (Adding a VTG to another VTG creates a *conference of conferences*.)
- To add a channel, user, or VTG that you searched for, drag the resource from the Resources area to the Participants area.

Tip To expand a collapsed Channels, Channel Groups, Users, User Groups, or VTGs list, click the arrow to the left of the list.

After you complete the drag and drop operation and release the mouse button, the resource that you added to the VTG template displays in green until you click **Save** to commit the change. To remove an item that displays in green, drag it out of the Participants area and into the Resources area.

Tip Be aware that you must click **Save** before you click the **Activate VTG** button to save your changes to the VTG. If you click **Activate VTG** before you click **Save**, you lose your changes and you must reenter them.

Note Activation or deactivation of a VTG requires that the Cisco IPICS server communicate with the RMS. If a VTG is deactivated when the RMS is unavailable, the deactivation occurs in the Cisco IPICS database, but is not reflected in the RMS until the Cisco IPICS server resumes communications with the RMS.

- If you remove a PMC user from a VTG and that user monitors a PTT channel that remains in the VTG, that user can continue to participate in the VTG through the PTT channel.
- If a user or a channel appears in a VTG more than once and you remove a single listing of the user or the channel, Cisco IPICS removes all instances of the user or the channel from the VTG.
- If you drag a user out of a user group in the Participants area, you do not change the actual user group.
- Empty PTT groups or user groups are not allowed in a VTG. If a group is included in a VTG and you drag every member out of the group, Cisco IPICS removes the group from the VTG.

Adding a New VTG Template

When you add a VTG template, you specify the name of the VTG and, typically, designate the members who are participants in the VTG. You can activate the VTG template at any time after you save it.

Note Activation or deactivation of a VTG requires that the Cisco IPICS server communicate with the RMS. If a VTG is deactivated when the RMS is unavailable, the deactivation occurs in the Cisco IPICS database, but is not reflected in the RMS until the Cisco IPICS server resumes communications with the RMS.

To add a new VTG template, perform the following procedure:

Procedure

Step 1 Navigate to **VTG Management > Virtual Talk Groups**.

Step 2 Click **Add**.

Step 3 In the VTG Name field, enter a name for the VTG.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / : ,.

Step 4 In the Description field, enter a description for this VTG.

Step 5 You can view the status of the VTG in the Status field.

Step 6 To set the PMC attributes, click the **PMC** tab.

For information about how some attributes behave with associations, see the “Understanding Association Attribute Behaviors” section on page 2-21.

Step 7 From the RX Mute During PTT drop-down list box, choose one of the following values:

- **VTG**—When PTT is engaged, RX (receive transmission) is muted on VTGs.
- **None**—When PTT is engaged, no channels are muted.
- **All**—When PTT is engaged, RX is muted on all channels/VTGs.

Step 8 To enable Voice Activity Detection (VAD) on the PMC, enabled the VAD check box.

When VAD is enabled, the PMC only sends voice traffic when it detects voice activity.

When set to true (attribute check box is checked) on the channel/VTG, VAD is used by the PMC while communicating with the channel/VTG.

By default, this attribute is set to false (attribute check box is not checked).

Step 9 To enable latch, check the **Allow Latch** check box.

The latch functionality allows a Cisco IPICS user to lock in a PTT channel.

Note When Allow Latch is set to true (attribute check box is checked) on a channel/VTG, the user can use latch on any channel/VTG or user/VTG association.

By default, this attribute is set to true (attribute check box is checked).

Step 10 To enable Listen Only, check the **Listen Only** check box.

When set to true (attribute check box is checked), the user can listen only on a channel; transmission is not allowed. This attribute applies to the PMC, IP phones, and dialed-in users.

Note If a VTG contains only channels and no users, enabling Listen Only on the PMC has no effect. However if the VTG contains users, enabling Listen Only dims the PTT button on the PMC but the channels in the PMC are not set to Listen Only.

Step 11 To uniquely identify VTGs by a specific color that displays on the PMC, choose a color from the VTG color drop-down list box.

Step 12 To add participants to the VTG template, click the **Participants** tab.

Step 13 To view the available resources that are configured in Cisco IPICS and which can be added as participants in this VTG template, choose one of the following options from the View drop-down list box that displays in the Resources area:

Note If there are less than 100 users, channels, or VTGs configured in Cisco IPICS, those resources display in the drop-down list box. If there are more than 100 resources configured, you must use the Search utility to display them. For more information about the search functionality, see the "Using the Search Utility" section on page 4-34.

- **Channels**—Choose this option to view the available channels that are configured in Cisco IPICS.
- **Channel Groups**—Choose this option to view the available channel groups that are configured in Cisco IPICS.

Note When you choose **Channel Groups** from the drop-down list box, the Search button displays as dimmed and the search functionality becomes unavailable.

- **Users**—Lets you view the available users that are configured in Cisco IPICS.
- **User Groups**—Lets you view the available user groups that are configured in Cisco IPICS.

Note When you choose **User Groups** from the drop-down list box, the Search button displays as dimmed and the search functionality becomes unavailable.

- **Virtual Talk Groups**—Choose this option to view the available VTGs that are configured in Cisco IPICS.

Step 14 Add any number and any combination of these resources to the VTG template as described in the "Guidelines for Managing VTG Templates" section on page 4-8.

Tip To expand a collapsed Channels, Channel Groups, Users, User Groups, or VTGs list, click the arrow to the left of the list.

Note Be aware that you must click **Save** before you click the **Activate VTG** button to save your changes to the VTG. If you click **Activate VTG** before you click **Save**, you lose your changes and you must reenter them.

Step 15 Click **Save** to add the VTG template without exiting the current window.

If you do not want to save your changes, click **Cancel**.

Step 16 To activate the VTG from this window, click **Activate VTG**.

Modifying a VTG Template

When you modify a VTG template, you can change its name and add or remove participants.

Because a VTG template is not an active event, you can make any changes to the template without affecting any current communication between users.

To modify a VTG template, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **VTG Management > Virtual Talk Groups**.

Step 2 In the VTG Name column, click the name of the VTG that you want to modify.

Step 3 If you want to change the name of the VTG template, click the **General** tab and enter the new name in the **VTG Name** field.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / : ,.

Step 4 To set the PMC attributes, click the **PMC** tab.

For information about how some attributes behave with associations, see the “Understanding Association Attribute Behaviors” section on page 2-21.

Step 5 From the RX Mute During PTT drop-down list box, choose one of the following values:

- **VTG**—When PTT is engaged, RX (receive transmission) is muted on VTGs.
- **None**—When PTT is engaged, no channels are muted.
- **All**—When PTT is engaged, RX is muted on all channels/VTGs.

Step 6 To enable Voice Activity Detection (VAD) on the PMC, enabled the VAD check box.

When VAD is enabled, the PMC only sends voice traffic when it detects voice activity.

When set to true (attribute check box is checked) on the channel/VTG, VAD is used by the PMC while communicating with the channel/VTG.

By default, this attribute is set to false (attribute check box is not checked).

Step 7 To enable latch, check the **Allow Latch** check box.

The latch functionality allows a Cisco IPICS user to lock in a PTT channel.

Note When Allow Latch is set to true (attribute check box is checked) on a channel/VTG, the user can use latch on any channel/VTG or user/VTG association.

By default, this attribute is set to true (attribute check box is checked).

Step 8 To enable Listen Only, check the **Listen Only** check box.

When set to true (attribute check box is checked), the user can listen only on a channel; transmission is not allowed. This attribute applies to the PMC, IP phones, and dialed-in users.

Note If a VTG contains only channels and no users, enabling Listen Only on the PMC has no effect. However if the VTG contains users, enabling Listen Only dims the PTT button on the PMC but the channels in the PMC are not set to Listen Only.

Step 9 To uniquely identify VTGs by a specific color that displays on the PMC, choose a color from the VTG color drop-down list box.

Step 10 To view the available resources that are configured in Cisco IPICS and which can be added as participants in the VTG template, click the **Participants** tab.

Step 11 From the View drop-down list box in the Resources area, choose from the following criteria:

Note If there are less than 100 users, channels, or VTGs configured in Cisco IPICS, then those resources will display in the drop-down list box. If there are more than 100 resources configured, you must use the Search utility to display them. See the "Using the Search Utility" section on page 4-34 for more information.

- **Channels**—Choose this option to view the available channels and channel groups that are configured in Cisco IPICS.
- **Channel Groups**—Choose this option to view the available channel groups that are configured in Cisco IPICS.

- **Users**—Choose this option to view the available users that are configured in Cisco IPICS.
- **User Groups**—Choose this option to view the available user groups that are configured in Cisco IPICS.
- **Virtual Talk Groups**—Choose this option to view the available VTGs that are configured in Cisco IPICS.

Step 12 To add participants to the VTG template after choosing the view in Step 11, see the "Guidelines for Managing VTG Templates" section on page 4-8.

Tip To expand a collapsed Channels, Channel Groups, Users, User Groups, or VTGs list, click the arrow to the left of the list.

Step 13 Click **Save** to modify the VTG template without exiting the current window.

If you do not want to save your changes, click **Cancel**.

Note Be aware that you must click **Save** before you click the **Activate VTG** button to save your changes to the VTG. If you click **Activate VTG** before clicking **Save**, you lose your changes and you must reenter them.

Step 14 To activate a VTG template in this window, click **Activate VTG**.

Deleting a VTG Template

If a VTG template is no longer needed, you can delete it from Cisco IPICS. Deleting a VTG template has no effect on the participants within it.

You cannot delete a VTG template that is associated with an active VTG. To delete such a VTG template, you must first deactivate the active VTG. See the "Reactivating a VTG" section on page 4-32 or the "Using the Search Utility" section on page 4-34 for more information.

To delete one or more VTGs, perform the following procedure:

Procedure

Step 1 From the VTG Management drawer in the Cisco IPICS Administration Console, click **Virtual Talk Groups**.

Step 2 Check the check box next to each VTG template that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the VTG or VTGs, click **Cancel**.

Tip To simultaneously delete all the VTG templates that are configured in Cisco IPICS, check the check box at the top of the Virtual Talk Groups list; then click **Delete**.

Managing Active VTGs

:The following sections describe information about managing active VTGs:

- Guidelines for Managing Active VTGs, page 4-17
- Changing the Status of a VTG Template, page 4-19
- Adding Participants to and Removing Participants from an Active VTG, page 4-20
- Muting or Unmuting a PMC User in an Active VTG, page 4-23
- Notifying and Dialing Out to Participants, and Setting PMC Attributes in an Active VTG, page 4-29
- Reactivating a VTG, page 4-32

Guidelines for Managing Active VTGs

When you are managing active VTG templates, be sure to adhere to the following guidelines:

- When channels that are associated with an active VTG get disabled, the channel gets disconnected from the VTG but still displays with a blue X and/or text status next to it, in the Participants tab in the Virtual Talk Groups window for that particular active VTG.
- When a disabled user or channel gets deleted, it gets removed from the affected VTGs.
- When a user group or channel group gets deleted, the group and its members (channels and users) get removed from the affected VTGs.
- If a user gets removed from a user group, the change automatically propagates to any VTG to which the user group is associated and the user gets disconnected and removed from the affected VTGs. It is no longer visible in the user group list.
- When a disabled user gets enabled again, the user automatically connects to the affected VTGs. If the user is connected via a SIP-based connection, the appropriate RMS resources get allocated to support those connections.
- If a channel gets removed from a channel group, the change automatically propagates to any VTG to which the channel group is associated and the channel gets disconnected from the affected VTGs. It is no longer visible in the channel group list.
- When a disabled channel gets enabled again, the channel does not automatically connect in the affected VTGs. You must reactivate the affected VTGs for the channel to connect and join the VTGs.
- If a user gets added to a user group, or a channel gets added to a channel group, no action is taken in the affected VTGs. In order to update the VTG with the changes to the user group or channel group, you must drag the user group or channel group back into the VTG. The user or channel that was added to the user or channel group gets connected to the VTG when the changes are saved.
- Users and channels that are members of a user group or channel group can also be directly associated with VTGs. In this case, the state of the directly associated users and channels override the states of the member users and member channels. For example, if a channel is directly connected to a VTG and is also a member of a channel group, modifications to the channel group do not affect the connection status of the channel in the VTG.
- You cannot delete an active VTG. You must deactivate it first.

- A PTT channel can be a participant in one active VTG at a time. If you try to add a PTT channel that is in an active VTG to a another active VTG, or try to activate another VTG that has the PTT channel in it, Cisco IPICS shows the PTT channel as unavailable in the second VTG.
- If the Cisco IPICS server fails, all active VTGs continue without disruption; however, you can no longer make changes to the VTG or mute a user.
- When you are connected via a high latency, low bandwidth connection, allow 1.5 minutes for every three channel/VTG activations.

Changing the Status of a VTG Template

A VTG can have either of the following statuses:

- Activated—Participants in a VTG template can communicate with each other.
- Deactivated—Channels in a VTG are no longer connected and participants in a VTG template can no longer communicate with each other.

You can change the status of a single VTG template, or you can change the status of several VTG templates at one time.

Activating a VTG causes Cisco IPICS to commit the network resources required to enable the participants in a VTG template to communicate with each other.

Note Activation or deactivation of a VTG requires that the Cisco IPICS server communicate with the RMS. If a VTG is deactivated when the RMS is unavailable, the deactivation occurs in the Cisco IPICS database, but is not reflected in the RMS until the Cisco IPICS server resumes communications with the RMS.

A VTG template can also be activated by a policy. For more information, see the Chapter 7, “Using the Cisco IPICS Policy Engine.”

When you activate a VTG, it attempts to obtain a multicast address from the multicast pool. If it is successful, it attempts to acquire resources for each of its channels and sub-VTGs. (Channels go into the pending state during this process.) If the VTG successfully obtains a multicast address and some resources, it becomes active; otherwise, it does not activate.

Note When you activate a VTG, there may be a delay before users can communicate with each other, especially if the VTG contains many PTT channels, users, and other VTGs. The delay may range from a few seconds to more than one minute, depending on the number of participants in the VTG.

When you deactivate a VTG, the channels in the VTG are no longer connected to each other. You can deactivate a VTG at any time.

A VTG template can also be activated by a policy. For more information, see the Chapter 7, "Using the Cisco IPICS Policy Engine."

To determine the current status of VTG templates, access the VTG Management drawer, click **Virtual Talk Groups**, and look at the information in the Status column for the VTG templates.

To change the status of a VTG, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **VTG Management > Virtual Talk Groups**.

Step 2 Take either of the following actions:

- In the VTG Name column, click the VTG name to display the VTG
  - To activate or deactivate the VTG, click **Activate VTG** or **Deactivate VTG**; then click **Save**.

  The **Activate VTG** or **Deactivate VTG** button appears at the bottom of the VTG management window. The name of the button depends on the current status of the VTG template.
- Check the check box next to each VTG template that you want to change; then choose the desired action (**Activate** or **Deactivate**) from the Change Status drop-down list box.

Adding Participants to and Removing Participants from an Active VTG

You can add participants to or remove participants from an active VTG.

When you add participants to an active VTG, Cisco IPICS does not commit network resources to the VTG until you click **Save**. At that point, Cisco IPICS commits the necessary resources to enable the existing VTG participants to communicate with those that you added.

Changes that you make to an active VTG do not affect the VTG template and are not saved to the VTG template when you deactivate the VTG.

Note There typically is a delay of several seconds for changes to take effect after you save them. Therefore, a user who is added to an active VTG may not be able to hear or communicate immediately, and a user who is removed from an active VTG may be able to continue participating in the VTG for a short time.

A user who is added to an active VTG is affected as follows:

- A PMC user sees a new PTT channel button that represents the VTG
- A handheld radio user on an LMR network hears new voices on the radio channel
- A Cisco Unified IP Phone user sees a new selection in the Services > IPICS menu on the phone that represents the VTG

To add participants to or remove participants from an active VTG, perform the following procedure:

Procedure

Step 1 From the VTG Management drawer in the Cisco IPICS Administration Console, click **Virtual Talk Groups**.

Step 2 Click the link of the active VTG to which you want to add or remove participants.

Step 3 To add participants to, or remove from the active VTG template, click the **Participants** tab.

Step 4 To view the available resources that are configured in Cisco IPICS that can be added as participants in this active VTG, from the View drop-down list box in the Resources area, choose from the following criteria:

Note If there are less than 100 users, channels, or VTGs configured in Cisco IPICS, then those resources will display in the drop-down list box. If there are more than 100 resources configured, you must use the Search utility to display them. For more information about the search functionality, see the "Using the Search Utility" section on page 4-34.

- **Channels**—Choose this option to view the available channels and channel groups that are configured in Cisco IPICS.
- **Channel Groups**—Choose this option to view the available channel groups that are configured in Cisco IPICS.

Note When you choose **Channel Groups** from the drop-down list box, the Search button displays as dimmed and the search functionality becomes unavailable.

- **Users**—Choose this option to view the available users that are configured in Cisco IPICS.
- **User Groups**—Choose this option to view the available user groups that are configured in Cisco IPICS.

Note When you choose **User Groups** from the drop-down list box, the Search button displays as dimmed and the search functionality becomes unavailable.

- **Virtual Talk Groups**—Choose this option to view the available VTGs that are configured in Cisco IPICS.

Step 5 To add participants to the VTG template, after choosing the view in Step 4, see the "Guidelines for Managing VTG Templates" section on page 4-8.

Step 6 If you want to remove participants from the VTG, drag each participant outside of the Participants area.

After you complete the drag and drop operation and release the mouse button, the participant changes to red. It is permanently removed from the VTG after you click **Save**. The participant can continue participating in the VTG until you click **Save**.

Step 7 To finalize your modifications, click **Save**.

If you want to cancel your changes, click **Cancel**.

Muting or Unmuting a PMC User in an Active VTG

Cisco IPICS allows you to mute a PMC user in an active VTG or in all VTGs in which the user is a participant, and to unmute any muted user. This feature can be useful if a user is participating from a noisy location, or if you want to mute a user for any other reason.

You can choose how to mute a PMC user as follows:

- Allow the user to listen to the VTG but not to speak in it
- Do not allow the user to speak or listen to the VTG
- Allow the user to listen to any channel or VTG, but not to speak
- Do not allow the user to speak or listen to any channel or VTG

The mute feature affects PMC, IP phone, and dialed users. In the case of an IP phone user, if the user is already transmitting on a VTG or PTT channel, the microphone does not get muted during that transmission. In addition, because all the user transmissions in a PTT channel are mixed into a single signal, it is not possible to mute the microphone of a LMR user in a PTT channel.

Note Users, channels, and VTGs may have attributes that control their behavior. In some cases, resources may have the same behavior attributes so when you associate users to VTGs and modify the attributes for users, the system determines the resulting behavior by the attribute configuration for each associated resource. Cisco IPICS allows you to override the resulting behaviors for specific associations. When you modify user attributes that are part of an association, the resulting behavior depends on attribute settings for those users in the association. See the "Understanding Association Attribute Behaviors" section on page 2-21 for more information about modifying attributes that are part of an association.

To mute or unmute a user in an active VTG, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **VTG Management > Virtual Talk Groups**.

Step 2 Click the link of the active VTG that contains the user that you want to mute or unmute.

Step 3 Click the **Participants** tab.

Note If necessary, click the arrow next to a user group in the Active VTG Details area to expand the group so that you can see an individual user.

You can mute and unmute users in either the User Details window, or in the Virtual Talk Groups window of the active VTG.

Step 4 To mute a user in the User Details window, double-click the user who you want to mute from either the **Participants** area or the **Resources** area; then, take one of the following actions in the User Details window:

Note If you choose a user from the **Resources** area (users who are not participants of the active VTG), changes to the attributes in the User Details window result in the same behavior as when attributes are modified in the Users window, PMC tab, and have no effect on the VTG. If you choose users who are participants of the VTG, changing attributes in the User Details window result in the attributes taking on the values of the user-VTG association and only apply to the VTG. See the "Understanding Association Attribute Behaviors" section on page 2-21 for more information about association attributes.

- Check the **Listen Only** check box to allow the user to listen to the active VTG but not to speak, and then click **Save**.

  In the Virtual Talk Groups window of the active VTG, an icon displays next to the name of the user showing that the PMC microphone has been muted. This attribute applies to the PMC, IP phones, and dialed-in users.

- Check the **Disable Audio** check box to disallow the user from listening or speaking in the active VTG, and then click **Save**.

This setting disables the channel in this VTG. In the Virtual Talk Groups window of the active VTG, an icon displays next to the name of the user showing that the PMC speaker has been muted. This attribute applies to the PMC, IP phones, and dialed-in users.

Note Be aware that when you choose the Disable Audio feature from any location in the Cisco IPICS server, the audio on all end user devices (PMC, IP phones, dialed-in users), except for radios, is disabled.

Step 5 To mute a user in the Participants area of the Virtual Talk Groups window, check the check box next to the name of the user that you want to mute and then take any of the following actions:

- From the drop-down list box at the bottom of the Participants area, choose **Set Listen Only** to allow the user to listen to the active VTG but not to speak; then, click **Execute**.

  An icon displays next to the name of the user showing that the PMC microphone has been muted. This attribute applies to the PMC, IP phones, and dialed-in users.

- From the drop-down list box at the bottom of the Participants area, choose **Disable Audio** to disallow the user from listening or speaking in the active VTG, then, click **Execute**.

Note Be aware that when you choose the Disable Audio feature from any location in the Cisco IPICS server, the audio on all end user devices (PMC, IP phones, dialed-in users), except for radios, is disabled.

This setting disables the user in this VTG. An icon displays next to the name of the user showing that the PMC speaker has been muted.

Step 6 To unmute a user in the User Details window, double-click the user that you want to unmute, from either the **Participants** area or the **Resources** area, and take one of the following actions in the User Details window:

- Uncheck the **Listen Only** check box to allow the user to speak and to listen to the active VTG; then, click **Save**.

  The icon next to the user name disappears in the Virtual Talk Groups window. This attribute applies to the PMC, IP phones, and dialed-in users.

- Uncheck the **Disable Audio** check box to allow the user to speak and to listen to the active VTG; then, click **Save**.

  The user is enabled and the icon next to the user name disappears in the Virtual Talk Groups window.

- Click **Close** to exit the User Details window.

Step 7 To unmute a user in the Participants area of the Virtual Talk Groups window, check the check box of the user that you want to unmute and take any of the following actions:

- From the drop-down list box at the bottom of the Participants area, choose **Unset Listen Only** to allow the user to listen and to speak in the active VTG; then, click **Execute**.

  The icon next to the user name disappears.

- From the drop-down list box at the bottom of the Participants area, choose **Enable Audio** to allow the user to speak and to listen in the active VTG; then, **Execute**.

  This setting enables the user in this VTG and the icon next to the name of the user disappears.

For information about how to enable or disable the Latch feature in the User Details window, see the "Enabling or Disabling the Latch Feature in the User Details Window" section on page 4-26.

Enabling or Disabling the Latch Feature in the User Details Window

Cisco IPICS lets you enable or disable the latch feature for a PMC user in the User Details window. The latch feature can be useful if a user wants to lock in a channel or talk on multiple channels at the same time.

Changes to PMC attributes vary depending on the location from which you access the User Details window. For example, if you open the User Details window for a user who is a participant of an active VTG, changes to the attributes for that user result in different behaviors, according to the user-VTG association values. If you modify attributes for a user who is not a participant of an active VTG (a user in the **Resources** area of the Virtual Talk Groups window), only the user is affected and not the VTG.

Note Users, channels, and VTGs may have attributes that control their behavior. In some cases, resources may have the same behavior attributes. When you associate users to VTGs and modify the attributes for users, the system determines the resulting behavior by how the attributes are configured for each associated resource. Cisco IPICS allows you to override the resulting behaviors for specific associations. When you modify user attributes that are part of an association, the resulting behavior depends on the attribute settings for those users in the association. See the "Understanding Association Attribute Behaviors" section on page 2-21 for more information about modifying attributes that are part of an association.

To enable or disable the latch feature for a PMC user, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **VTG Management > Virtual Talk Groups**.

Step 2 Click the link of the active VTG that contains the user for whom you want to enable or disable the latch feature.

Step 3 Click the **Participants** tab.

Note If necessary, click the arrow next to a user group in the Active VTG Details area to expand the group so that you can see an individual user.

Step 4 To enable latch for a user in the User Details window, double-click the user for whom you want to enable latch from either the **Participants** area or the **Resources** area.

Note If you choose a user from the **Resources** area (users who are not participants of the active VTG), changes to the attributes in the User Details window result in the same behavior as when attributes are modified in the Users window, PMC tab, and have no effect on the VTG. If you choose users who are participants of the VTG, changing attributes in the User Details window results in the attributes taking on the values of the user-VTG association and only applies to the VTG. See the "Understanding Association Attribute Behaviors" section on page 2-21 for more information about association attributes.

Step 5 Check the **Allow Latch** check box.

Step 6 Click **Save**.

Step 7 To disable the latch feature for a PMC user in the User Details window, double-click the user for whom you want to disable latch, from either the **Participants** area or the **Resources** area.

Step 8 Uncheck the **Allow Latch** check box.

Step 9 Click **Save**.

Note When you modify user attributes that are part of an association, the resulting behavior depends on attribute settings for those users in the association. See the "Understanding Association Attribute Behaviors" section on page 2-21 for more information about modifying attributes that are part of an association.

Step 10 Click **Close** to exit the User Details window.

Note To enable or disable latch for a user in the **Participants** area of the Virtual Talk Groups window, see the "Notifying and Dialing Out to Participants, and Setting PMC Attributes in an Active VTG" section on page 4-29.

Notifying and Dialing Out to Participants, and Setting PMC Attributes in an Active VTG

You can initiate various actions in an active VTG, including notifying participants via e-mail, Short Message Service (SMS), or pager, dialing out to participants who are connected via the Public Switched Telephone Network (PSTN) or IP phone, and enabling and disabling PMC attributes for selected VTG participants.

When you activate a VTG template in Cisco IPICS, you can invite the participants to join the VTG. This invitation can be in the form of an e-mail that can be specified for e-mail message, SMS text message, or pager delivery. The notification can also be a phone call, depending on the communication preferences that have been set for the VTG participants.

When Cisco IPICS operators initially create users, they set up a user profile in which the users can enter and manage personal information, including communication preferences. The users have the option to enter and edit notification preferences that include their e-mail addresses and dial preferences that include an ordered list of phone numbers to be used when you initiate a dial-out to given users.

Note In the user profile, users can specify their SMS and pager contact information in the form of e-mail addresses. When a notification gets sent to these e-mail addresses (provided by their SMS/pager providers), a text message or page is sent.

When you initiate a notification action, the policy engine automatically sends the users an e-mail that is directed to their e-mail account, SMS, or pager, inviting them to join the VTG. The policy engine obtains the e-mail contact information from the notification preferences that were configured in their user profiles. See the Chapter 7, “Using the Cisco IPICS Policy Engine,” for more information about the policy engine.

Note If the Dial after sending notifications check box is checked in the Communications tab of the user profile, then Cisco IPICS will first send all e-mail notifications, and then attempt to place a call to the participants by using the dial preferences that were set in the user profile.

When you initiate a dial-out to selected participants, Cisco IPICS attempts to call the participants by using the numbers that are specified in their individual dial preferences and begins with the first number in the list. If the call is successful, Cisco IPICS connects the call to the active VTG and stops. If the call is unsuccessful, Cisco IPICS continues to place calls to numbers in the order that they appear in the dial preferences list until a call is successful or until all of the numbers in the list have been tried.

If the dial-out action successfully completes, the participant can log in to Cisco IPICS. When you refresh the active VTG window, a PSTN (telephone) icon displays for each successful dial-out participant. An error icon displays for those participants for whom the dial-out was unsuccessful.

Cisco IPICS displays the method by which the participants are connected, (for example, by PSTN or PMC) and also displays the call progress (connecting, connected, call failed) when you initiate a dial-out to participants who are connected via the PSTN.

Note The connection method and call progress indicators only update when you refresh the window.

You can also set and modify PMC attributes for selected VTG participants. You execute these actions in the VTG window of the active VTG.

To initiate actions in an active VTG, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **VTG Management > Virtual Talk Groups**.

Step 2 Click the link of the active VTG for which you want to initiate actions.

Note To activate a VTG template in Cisco IPICS, see the "Changing the Status of a VTG Template" section on page 4-19.

Step 3 From the View drop-down list box in the Participants tab, choose one of the following options:

- **All**—Choose this option to view all of the participants (channels, users, and other VTGs) in this VTG.
- **Channels**—Choose this option to view the channels who are participating in this VTG.
- **Users**—Choose this option to view the users who are participating in this VTG. The window displays an icon next to each participant to indicate how the user is connected (via PMC, phone, or channel) to the VTG.
- **Virtual Talk Groups**—Choose this option to view the other VTGs that are participating in the VTG.

Step 4 To choose the participants that you want to include in a particular action, check the check boxes next to the names of the participants.

Note For example, if you want to dial out to users who are connected via a phone to invite them to join this active VTG, check the check boxes next to the names of those users.

Step 5 From the drop-down list box, choose any of the following actions:

Note If you have limited call resources, you should choose the Notify Participants option rather than Dial Participants.

- **Notify Participants**—Choose this option to invite VTG participants, via e-mail, to join an active VTG. When you choose participants to be invited to this VTG, Cisco IPICS automatically notifies those participants in the form of an e-mail. Notification is sent via e-mail message, SMS text message, or page. Cisco IPICS obtains the e-mail addresses and delivery options from the communication preferences information that the users and/or Cisco IPICS operators entered in the user profiles.
- **Dial Participants**—Choose this option to dial out to selected participants to invite them to join an active VTG. When you choose participants to whom you want to dial out, the policy engine uses the dial preferences information (for example, phone numbers) that the users and/or Cisco IPICS operators have entered in their user profiles to determine the number(s) to be called and dials the participants.

- **Allow Latch**—Choose this option to enable the latch functionality, during this VTG, for selected participants. When you choose this action, participants that you choose will be able to lock in channels.
- **Disallow Latch**—Choose this option to disable the latch functionality, during this VTG, for selected participants. When you choose this action, the participants that you choose will not be able to lock channels.
- **Set Listen Only**—Choose this option to enable the Listen Only attribute, during this VTG, for selected participants. When you choose this action, participants that you choose in this VTG will only be able to listen (receive) and not to speak (transmit). This attribute applies to the PMC, IP phones, and dialed-in users.
- **Unset Listen Only**—Choose this option to disable the Listen Only attribute, during this VTG, for selected participants. When you choose this action, participants that you choose in this VTG will be able to speak (transmit).
- **Enable Audio**—Choose this option to enable audio, during this VTG, for selected participants. When you choose this action, participants that you choose in this VTG will have audio.
- **Disable Audio**—Choose this option to disable audio, during this VTG, for selected participants. When you choose this action, participants that you choose in this VTG will not have audio.

Note Be aware that when you choose the Disable Audio feature from any location in the Cisco IPICS server, the audio on all end user devices (PMC, IP phones, dialed-in users), except for radios, is disabled.

Step 6 Click **Execute**.

Cisco IPICS executes the specified action(s).

Reactivating a VTG

If all channels are not available for a VTG when you activate it, Cisco IPICS activates the channels that are available. A channel may be unavailable because there are insufficient router resources available for it or because it is in use by another active VTG.

An blue X displays to the right of an unavailable VTG channel in the Active VTG Details area. To see why the channel is unavailable, hold the mouse over the X and look at the tooltip that pops up.

When a VTG channel is unavailable, Cisco IPICS allows the VTG to continue operating without the channel, and lets you take the necessary action to obtain the unavailable channel and reactivate the VTG. When you reactivate a VTG, Cisco IPICS determines whether previously unavailable channels are available and adds them to the active VTG if they are. In this way, Cisco IPICS ensures that you do not have to disrupt a VTG if some channels are not available when you activate it.

To reactivate a VTG, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **VTG Management > Virtual Talk Groups**.

Step 2 In the VTG Name column, click the VTG that you want to activate.

Step 3 Make a note of which channels in the VTG are unavailable and why.

Cisco IPICS displays a blue X next to each unavailable channel in the Participants area. Hold the mouse cursor over the blue X to see why the channel is unavailable.

Step 4 If the channel is unavailable because of insufficient router resources, take these actions to free additional router resources:

- Remove channels from any VTG
- Disable users who have active SIP unicast connections

Note You can see how router resources are being used by looking at information about its loopbacks in the RMS window. For more information, see the "Viewing Detailed Information about a Loopback" section on page 2-67.

Step 5 If the channel is unavailable because it is in use by another VTG, take either of the following actions:

- Identify the active VTG to which this channel is associated by performing the following steps:

  - In the Configuration drawer, click **Channels**.
  - In the Channels list, click the channel name link.
  - Click the **Associations** tab.
  - From the View drop-down list box, choose **Virtual Talk Groups**.
  - Look at the active VTG that is listed in the Virtual Talk Groups list, and then navigate to **VTG Management > Virtual Talk Groups**.
  - Choose the active VTG that was listed in the Associations tab of the Channels window.
- Locate the additional VTG in which this channel is a participant by performing the following steps:
  - In the VTG Management drawer, click **Virtual Talk Groups** again.
  - Click the link of another active VTG in the Virtual Talk Groups list and see if the channel is a participant in that VTG.
  - Repeat as necessary until you locate the VTG in which the channel is a participant.

Step 6 Remove the channel from one of the active VTGs by dragging the channel out of the Participants area; then, clicking **Save**.

Note Make sure that the channel is not needed in this active VTG before you perform this step.

Step 7 In the VTG Management drawer, click the name of the original VTG in which the channel is shown as unavailable.

Step 8 If the VTG contains other unavailable resources, repeat Step 4 through Step 6.

Step 9 Click **Reactivate VTG**.

Using the Search Utility

You can search for a PTT Channel, user, or VTG by using the search utility. The search utility is located in the Virtual Talk Groups window of each individual VTG template.

When you complete a search, you can see the results display in the Resources area.

Note If there are less than 100 resource entries (VTGs, channels, users) in the system, the available resource lists in the VTG Participants tab are pre-populated. If the system has more than 100 resources, the resource list displays as blank and you must perform a search to populate it. Channel groups and user groups are always pre-populated.

To use the search utility to find a PTT channel, user, or VTG, perform the following procedure:

Procedure

Step 1 From the VTG Management drawer in the Cisco IPICS Administration Console, click **Virtual Talk Groups**.

Step 2 Click the link of the VTG on which you want to search for channels, users, or VTGs.

Step 3 Click the **Participants** tab, and then click the **Search** link that appears above the Resources area.

A separate search window displays.

Step 4 From the View drop-down list box, in the top left corner of this window, choose one of the following options:

- **By Channel**—Choose this option to search for channels.
- **By User**—Choose this option to search for users.
- **By VTG**—Choose this option to search for VTGs.

The Search window adjusts to display fields that apply to the item for which you want to search.

Step 5 Take one of the following actions:

- If you are searching for a PTT channel or a VTG, enter a text string for the channel in the Channel Name field, or enter a text string for the VTG in the VTG Name field.

A text string can be an entire channel name or VTG name, or it can be any consecutive characters in the name. For example, if you are searching for a VTG called Fire West, you could enter the text string "fire," and Cisco IPICS returns results based on the beginning character.

Text strings are not case sensitive.

Tip If you are searching for a channel, you can also search by the ops view of the channel by choosing an ops view from the Ops View drop-down list box.

Proceed to Step 6.

- If you are searching for a user, enter information in any or all of the following fields:
  - User Name, First Name, and Last Name—Enter text strings for the user for whom you are searching.

    Text strings are not case sensitive.
  - Location drop-down list box—Location of the user
  - Role drop-down list box—Cisco IPICS role of the user
  - Ops View drop-down list box—Ops view to which the user belongs

    For example, if you know only a portion of the user name, but you also know that the user a dispatcher in the West Side location, you can enter a character string in the User Name field and then choose Dispatcher and West Side from the Role and Location drop-down list boxes.

    Proceed to Step 6.

Step 6 Click **Go**. To clear your criteria, click **Clear Filter**.

The items that meet your search criteria display in the list at the bottom of the search window.

Note You can specify the number of rows of channels, users, or VTGs that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Step 7 To choose the resources that you want, check the check box to the left of each resource.

Step 8 Click **OK**.

The Search window closes and the search results display in the Resources area of the individual VTG window.

Best Practices for Managing VTGs

Cisco IPICS presents new opportunities for members of your organization to participate in conferences. Some of these members may be unfamiliar with the technology, conventions, and practices of PTT communication. For example, these users may have never used a PTT device or participated in a large conference with radio users.

Other PTT users may be surprised by the experience of participating in a Cisco IPICS-managed conference. For example, a handheld radio user may be familiar with the experience of conferring only with a small number of other handheld users on a certain LMR channel. When the LMR channel for that user is placed in a VTG, that user becomes part of a potentially much larger and more diverse conference.

Changes in a conference can occur suddenly for a conference participants, especially those participating with handheld radios. For example, at one moment, a user may be speaking with one or more radio users from the same department; then, when a dispatcher adds the LMR channel to a VTG, the user hears completely different voices.

The following guidelines can be helpful in assisting your new and experienced users with Cisco IPICS:

- Establish a dispatcher-only PTT channel and add this channel to every PMC and VTG. This channel allows the Cisco IPICS dispatcher to announce VTG changes to the participants, so that they can be made aware when users are added or removed from a VTG.
- Instruct new PMC users on the etiquette of PTT communication. For example:
  - In some network configurations, one or more users may not hear when another user breaks into a conversation

- Talk in short bursts
- If extensive conversation is required, consider an alternate method of communication

Performing Cisco IPICS User Tasks

Everyone who uses Cisco IPICS is assigned a user role. This role allows you to log into the Administration Console, view and update your user information, update your communication preferences so that you can use Cisco IPICS to communicate with other Cisco IPICS users, and download the Cisco IPICS PMC client application to your PC.

The user role may be your only role, or you may have one or more other roles (system administrator, ops view administrator, dispatcher, or operator).

This chapter contains the following sections:

- Logging in to Cisco IPICS, page 5-1
- Managing Your User Profile, page 5-2
- Managing User Associations, page 5-14
- Downloading the PMC, page 5-19

Logging in to Cisco IPICS

When you access Cisco IPICS via your browser, the first window that displays is the Cisco IPICS Login window.

To log in to Cisco IPICS, enter your user name in the User Name field, enter your password in the Password field; then click **Log In**.

Note Be aware that user names are case-insensitive; that is, you can enter upper case or lower case characters for your login user name. Cisco IPICS will automatically convert any upper case characters to lower case. However, passwords are case-sensitive, so make sure to enter them exactly as they are configured. For more information about your Cisco IPICS login password, see the "Managing Your User Profile" section on page 5-2.

After you log in, the Cisco IPICS Administration Console displays your user profile. If you have been assigned more than one user role, the additional drawers that can be accessed according to those roles, display in the left pane of the Administration Console. For more information about how an operator assigns user roles, see the "Managing Users" section on page 3-2.

To access your user profile, navigate to **My Profile** from the Home drawer. See the "Managing Your User Profile" section on page 5-2 for more information about the user profile.

To view and edit user associations, in the Home drawer, click the **My Associations** link. See the "Managing User Associations" section on page 5-14 for more information about managing user associations.

To download the PMC client application to your PC, click the **Download PMC** link from the Home drawer. See the "Downloading the PMC" section on page 5-19 for more information about downloading the PMC client application.

Managing Your User Profile

Your user profile, also referred to as *My Profile*, includes your name, password, default location, communication preference, and other optional personal information. Your user profile was initially set up by a Cisco IPICS operator, but you can change information, as needed.

Your user profile information is shown in the My Profile window, which displays after you log in to Cisco IPICS. The user profile personal information is contained in information tabs, labeled General, Address, Dial Login, PMC, Communications, and Policies. Managing your user profile involves reviewing and updating this information.

User and digit password requirements are configured by the system administrator or operator in the Cisco IPICS server.

To manage your user profile, perform the following procedure:

Procedure

Step 1 If the My Profile window is not already displayed, navigate to the Home drawer in the Cisco IPICS Administration Console and click **My Profile**.

Step 2 Review the information that is described in Table 5-1 and update this information, as needed, by choosing the appropriate information tab.

Fields that are designated as display only can be changed by a Cisco IPICS operator as described in the "Managing Users" section on page 3-2 and the "Managing User Groups" section on page 3-41.

Table 5-1 Edit My Profile Fields

Field	Description
General Tab	
User Name	*Display only.* This field specifies the user name assigned when your profile was created. **Note** User names are case-insensitive; that is, you can enter either upper case or lower case characters for your user name.
First Name	This field specifies your first name. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (')
Last Name	This field specifies your last name. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (')

Table 5-1 Edit My Profile Fields (continued)

Field	Description
Old Password	This field specifies the password that you enter when you log in to Cisco IPICS. For security, you should change your password periodically. You may be forced to change your password based on the configuration in the server. **Note** Be aware that passwords are case-sensitive and must be entered exactly as they were configured by the Cisco IPICS operator.
New Password	This field specifies the new password that you enter when you change your login password. Valid characters: alphanumeric characters and these special characters: @ [\ ] ^ _ ‘ ! “ # $ % & ' ( ) * , - . / : ; { < | = } > ~ ?
Confirm Password	This field specifies confirmation of the entry in the new password field.
Description	*Optional.* You can enter a description in this field.

Table 5-1 Edit My Profile Fields (continued)

Field	Description
Password Expiration Date	*Display only.* This field specifies the expiration date of your login password. This field is read-only and is based on the password expiration settings that the system administrator configures in the Cisco IPICS server. **Note** You will receive warning messages when your password is about to expire, and after it has expired; these messages display in the red error block in the My Profile window. If you do not change your password before your old password expires, you will only be able to log in to your user profile to change your password. You will not have access to any other windows in Cisco IPICS. If the Cisco IPICS system administrator changes the password requirements, your old passwords will not be affected until they expire. The new password rules apply the next time that you create a new password.
IPICS Status	*Display only.* This field indicates whether the user is enabled or disabled.
Roles	*Display only.* This field specifies the Cisco IPICS roles that have been assigned to you. "All" indicates that you have been assigned the privileges of all roles.
Account Status	*Display only.* This field specifies the status of the user account.
Belongs To	*Display only.* This field appears if operational views (ops views) is enabled and indicates the ops view to which you belong. For more information, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Address Tab	

Table 5-1 Edit My Profile Fields (continued)

Field	Description
Address	This field specifies your street address. Valid characters: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :.
Address (cont)	This field specifies additional street address information. Valid characters: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :
City	This field specifies your city. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’)
State/Province	This field specifies your state or province. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’)
Country	This field specifies your country. Valid characters: alphanumeric characters, space, and period (.)
Zip/Postal Code	This field specifies your zip or postal code. Valid characters: alphanumeric characters, space, and period (.)
E-mail	This field specifies your e-mail address. Valid characters: alphanumeric characters, underscore (_), period (.), and ampersand (@)
Dial Login Tab	
Digit ID	This field specifies the identifier that you enter when you access Cisco IPICS from a Cisco Unified IP Phone that has been configured for use with Cisco IPICS. Valid characters: numeric characters.

Table 5-1 Edit My Profile Fields (continued)

Field	Description
Old Digit Password	This field specifies the password that you enter when you initially access Cisco IPICS from a Cisco Unified IP Phone that has been configured for use with Cisco IPICS (the actual characters in the password are represented by asterisks (*)). By default, the password must contain at least 4 characters. Valid characters: numeric characters
Digit Password (PIN)	This field specifies the password that you enter when accessing the Cisco IPICS service from a Cisco Unified IP Phone or personal identification number (PIN) that you enter when accessing the TUI. (The actual characters in the password are represented by asterisks (*).) By default, the password must contain at least 4 characters. Valid characters: numeric characters
Confirm Digit Password	This field specifies confirmation of entry in the Digit Password field.

Table 5-1 Edit My Profile Fields (continued)

Field	Description
Default Location	This field specifies the location that displays, by default, on your PMC. Choose a location from the drop-down list box. **Note** To use IP phones with Cisco IPICS, you must assign a location that is the same as the dial login default location. The server assigns the configured default location to an IP phone user when the user logs in to Cisco IPICS. (In this case, there is no user selection for location.) IP phone users can access only the associated channels that are assigned to their default location, along with any assigned VTGs. If the configured default location is the ALL location, IP phone users can access only the channels that are assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location as the default location for the IP phone user.
PMC Tab	

Table 5-1 Edit My Profile Fields (continued)

Field	Description
PMC Info	*Display only.* This field indicates how you can communicate in VTGs or channels: • Disable Audio—You cannot transmit or receive communications on the channel • Listen Only—You are restricted to listening only on the channel; no transmission is allowed • Allow Latch—You can latch, or lock in, channels • Advanced PMC Permissions—Specifies whether you are enabled for the following features on the PMC: – Channel multiselect for voice and tone transmissions – Alert tones transmissions – DTMF tones transmissions – All Talk channel transmissions For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide*.
Communications Tab	
Notification Preferences	This field specifies any combination of one or more E-mail, Short Message Service (SMS), or pager address. To manage your notification preferences, see the "Managing Communications Preferences" section on page 5-10.
Dial Preferences	This field specifies one or more telephone numbers. To manage your dial preferences, see the "Managing Communications Preferences" section on page 5-10.

Step 3 Click **Save** to save any changes that you have made.

Managing Communications Preferences

Communications preferences specify how Cisco IPICS contacts you when a user-associated policy executes. These preferences are also used by Cisco IPICS when a dispatcher initiates a notification or dial out to you, in order to invite you to join an active VTG. For more information about notifications, see Chapter 7, "Using the Cisco IPICS Policy Engine."

When you specify communication preferences, you can provide the following information:

- Notification Preferences—Any combination of one or more E-mail, SMS, or pager address.
- Dial Preferences—One or more telephone numbers.

This section includes the following topics:

- Viewing, Adding, Editing, or Deleting Communications Preferences, page 5-10
- Specifying the Order of Dial Preferences, page 5-13

Viewing, Adding, Editing, or Deleting Communications Preferences

You can view, add, edit, or delete notification preferences and dial preferences in the user profile. To do so, perform the following procedure:

Procedure

Step 1 Access the Home drawer in the Cisco IPICS Administration Console and click **My Profile**.

Step 2 Click the **Communications** tab.

This tab displays the following information:

- Type (under Notification Preferences)—Method by which you get notified:
  - E-mail—Cisco IPICS sends notification to an e-mail address that you specify.
  - SMS—Cisco IPICS sends notification to an SMS through an e-mail gateway.

  - Pager—Cisco IPICS sends notification to a pager through an e-mail gateway.
- Number/Address (under Notification Preferences)—This field specifies the e-mail address for the corresponding notification type.
- Type (under Dial Preferences)—This field specifies the description of the location to be dialed, such as business, car, or home.
- Dial Number (under Dial Preferences)—This field specifies the telephone number of the corresponding location type.

Step 3 To add, edit, or delete notification preferences, take the appropriate actions under the Notification Preferences list:

- To add a notification preference, follow these steps:
  a. Click **Add**.
  b. From the drop-down list box, choose a method by which the user receives notifications (e-mail, SMS, or pager).
  c. In the field next to the drop-down list box, enter the e-mail address for the corresponding notification method.

     For the SMS and pager methods, specify the e-mail address of the gateway through which the message is sent to the device.
  d. Click **Done**.
  e. Repeat these steps, as needed, to add more notification preferences.
- To edit a notification preference, follow these steps:
  a. Check the check box next to the notification preference that you want to edit.
  b. Click **Edit**.
  c. From the drop-down list box, choose a method by which you want to receive notifications.
  d. In the field next to the drop-down list box, enter the e-mail address for the corresponding notification method.
  e. Click **Update**.
- To delete a notification preference, follow these steps:
  a. Check the check box next to the notification preference or preferences that you want to delete.

b. Click **Delete**.

Step 4 To add, edit, or delete dial preferences, take the appropriate actions under the Dial Preferences list:

- To add a dial preference, follow these steps:
  a. Click **Add**.
  b. From the drop-down list box, choose a description for the dial preference.
  c. In the field next to the drop-down list box, enter the telephone number for the corresponding dial preference.

     This field can contain numerals, dashes (-), and spaces. If the telephone number includes an extension, precede the extension with an uppercase or lowercase X.
  d. Click **Done**.
  e. Repeat these steps as needed to add more dial preferences.
- To edit a dial preference, follow these steps:
  a. Check the check box next to the dial preference that you want to edit.

     You can use the up arrow and down arrow to move a check to an adjacent check box.
  b. Click **Edit**.
  c. From the drop-down list box, choose a description for the dial preference.
  d. In the field next to the drop-down list box, enter the telephone number for the corresponding dial preference.

     This field can contain numerals, dashes (-), and spaces. If the telephone number includes an extension, precede the extension with an uppercase or lowercase X.
  e. Click **Update**.
- To delete a dial preference, follow these steps:
  a. Check the check box next to the dial preference or preferences that you want to delete.
  b. You can use the up arrow and down arrow buttons to move a check to an adjacent check box.
  c. Click **Delete**.

Step 5 Check the **Dial after sending notifications** check box if you want the policy engine to attempt to call you by using the numbers that are configured in the Dial Preferences list when an associated policy executes.

Note If the Dial after sending notifications check box is checked, Cisco IPICS will first send all e-mail notifications, and then attempt to place a call to the participants by using the dial preferences that were set in the user profile.

Step 6 Click **Save** to save your changes.

Specifying the Order of Dial Preferences

You can specify the order of the numbers that you add to your dial preferences. Cisco IPICS dials the numbers in the order that you specify, beginning with the first number in the list, until every number has been tried, or until one of the calls in answered. If the call is successful, Cisco IPICS connects the call and stops. If the call is unsuccessful, Cisco IPICS continues to place calls to the numbers, in the order that they appear in the preferences list, until a call is successful or until all of the numbers in the list have been tried (whichever comes first).

To specify the order of the dial preferences, perform the following procedure:

Procedure

Step 1 Access the Home drawer in the Cisco IPICS Administration Console and click **My Profile**.

Step 2 Click the **Communications** tab.

Step 3 Check the check box next to the dial preference type that you want to move to a different position in the list.

Step 4 Click the up arrow button to move the dial preference up in the list, or click the down arrow button to move it down in the list.

Step 5 Repeat Step 3 and Step 4 as needed to move other dial preferences.

Step 6 Click **Save** to save your changes.

Managing User Associations

In Cisco IPICS, you can be associated with other users, channels, VTGs, phones, and policies. You can view Cisco IPICS resources to which you have been associated in the My Associations window in the Administration Console.

The My Associations window contains information tabs that display the channels, users, phones, VTGs, and policies with which you are associated in Cisco IPICS. Table 5-2 describes information about the resources within each of these tabs.

Table 5-2 My Association Window Fields

Field	Description
Channels Tab	
Associated Channels	This tab specifies the channels to which you are associated. When you are associated with PTT channels, those channels appear as options on a PMC or a properly-configured Cisco Unified IP Phone. Channels are represented by the icon. To view the channels to which you are associated, choose **Channels** from the View drop-down list box. The following information displays about the channels to which you are associated: • Channel Name—This field specifies the name of the channel. • Status—This field indicates whether the channel is enabled or disabled. • Latchable—This field indicates whether the channel can be latched (locked). • Disable Audio—This field indicates whether audio is disabled. • Listen Only—This field indicates whether the Listen Only attribute is enabled.
Users Tab	

Table 5-2 My Association Window Fields (continued)

Field	Description
Associated Users	This tab specifies users to whom you are associated. When you are associated with other Cisco IPICS users, you can use your PMC to communicate with those users over a SIP channel. In this way, you can communicate with these users even if you are not associated with a channel or participants in a VTG. Users are represented by the icon. To view the users to whom you are associated, choose **Users** from the View drop-down list box. The following information displays about the users to whom you are associated: • User Name—This field specifies the user ID of the user. • Last Name—This field specifies the last name of the user. • First Name—This field specifies the first name of the user. • Status—This field indicates whether the user is enabled or disabled.
Phones Tab	

Table 5-2 My Association Window Fields (continued)

Field	Description
Associated Phones	This tab specifies the phones with which you are associated. When you are associated with phones, you can use your PMC to communicate with other users who are connected via a telephone. Phones are represented by the icon. The following information displays about the phones to which you are associated: • Dial Destination—This field specifies the phone number to call (the number of the associated phone). • Label—This field specifies the label that displays on the PMC (minimum of 15 characters).
Virtual Talk Groups Tab	
Virtual Talk Groups	This tab specifies the VTGs to which you are associated. When you are associated with VTGs, you can communicate with other participants of that VTG. VTGs are represented by the icon. To view the VTGs to which you are associated, choose **Virtual Talk Groups** from the View drop-down list box. The following information displays about the VTGs to which you are associated: • VTG Name—This field specifies the name of the VTG. • Status—This field indicates whether the VTG is active or inactive.

Table 5-2 My Association Window Fields (continued)

Field	Description
Policies Tab	
Associated Policies	This tab specifies the policies to which you are associated that you can activate by calling the policy engine. Policies are represented by the icon. The window displays the policy name in the Policy Name column. **Note** You can change the order in which the policies display by checking the check box next to a policy name and clicking the up and down arrows at the bottom of the policy list.

To view the resources with which you are assigned, see the "Viewing User Associations" section on page 5-18.

Viewing User Associations

To view your user associations, perform the steps in the following procedure:

Procedure

Step 1 Access the Home drawer in the Cisco IPICS Administration Console and click **My Associations**.

Step 2 To view your user associations, click any of the following information tabs:

- **Channels**
- **Users**
- **Phones**
- **Virtual Talk Groups**
- **Policies**

Note You can change the order in which the policies display by checking the check box next to a policy name and clicking the up and down arrows.

See Table 5-2 for a description of each of the association tabs.

Downloading the PMC

As a Cisco IPICS user, you can download the current version of the PMC to your PC. To do so, perform the following steps from the PC to which you want to download the PMC.

For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide*.

Procedure

Step 1 Access the Home drawer in the Cisco IPICS Administration Console and click **Download PMC**.

Cisco IPICS initiates the PMC download utility, which installs the PMC on your PC and creates a shortcut on your desktop.

Step 2 Follow the on-screen prompts to download and install the PMC.

Configuring and Managing Cisco IPICS Operational Views

This chapter describes the Cisco IPICS operational view functionality and it includes information about relevant terminology, caveats, and administration tasks.

This chapter includes the following sections:

- Managing Cisco IPICS Ops Views, page 6-1
- Understanding Ops Views Caveats, page 6-11
- Performing Ops Views Tasks, page 6-17

Managing Cisco IPICS Ops Views

Cisco IPICS provides the ability for you to organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other. In Cisco IPICS, these separate views are known as operational views, or ops views. While these views are maintained separately by the Cisco IPICS system administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

Note The use of ops views allows segmentation of resources that authorized Cisco IPICS users may see on the Cisco IPICS Administration Console. Ops views does not affect the way in which channels and VTGs display on the PMC or Cisco Unified IP Phone.

When you purchase a Cisco IPICS license, you receive a license with a specified number of ops views. In the License Management window, Cisco IPICS displays the total number of ops view ports, current usage, as well as individual port usage per ops view.

To see detailed information about license limits in the Ops Views configuration window, navigate to the Configuration drawer in the Cisco IPICS Administration Console and click **Ops Views**. See the "Understanding the Ops Views Window" section on page 6-3 for more information.

For more information about Cisco IPICS license information, see the "Understanding the License Management Window" section on page 2-72.

When you access the **Ops Views** window, the server displays the SYSTEM ops view by default. The SYSTEM ops view is the home base or system-wide view to which the Cisco IPICS administrators belong. When new ops views are created, ports are reallocated from the SYSTEM ops view to the new ops view, and any additional ops views that you create.

Note Cisco IPICS displays the number of available licenses and concurrent usage information in the License Management window. As a best practice, make sure that you update your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative 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.

For more information about managing licenses in Cisco IPICS, see the "Managing Licenses" section on page 2-72. For detailed information about how to obtain licenses in the release of Cisco IPICS, refer to the *Cisco IPICS Server Installation and Upgrade Guide Release 2.0(1)*.

This section describes the Cisco IPICS ops view management functions and includes the following topics:

- Understanding the Ops Views Window, page 6-3
- Creating New Ops Views, page 6-5
- Assigning Ops Views Resources, page 6-6
- The Benefits of Using Ops Views, page 6-6
- Understanding Ops Views Attributes, page 6-7
- Understanding Ops Views User Roles, page 6-9

Understanding the Ops Views Window

The Ops Views window lists information about each of the ops views that have been added in Cisco IPICS. It also lets you perform several ops views management functions.

To display the Ops Views window, navigate to **Configuration > Ops Views**.

Table 6-1 describes the items in the Ops Views window.

Table 6-1 Items in the Ops Views Window

Item	Description	Reference
Name field	Unique identification name that is assigned to the ops view	See the "Performing Ops Views Tasks" section on page 6-17
Dial Number field	Number that is configured in the ops view and which users dial to access CIsco IPICS from an IP phone	
LMR Ports Limit field	Maximum number of land mobile radio (LMR) license ports that are allocated to this ops view	
Multicast Ports Limit field	Maximum number of multicast license ports that are allocated to this ops view	
PMC Users Limit field	Maximum number of PMC users license ports that are allocated to this ops view	
IP Phones Limit field	Maximum number of IP phone license ports that are allocated to this ops view	
Dial Ports Limit field	Maximum number of dial ports that are allocated to this ops view	
Add button	Click this button to add an ops view	See the "Adding Ops Views" section on page 6-18

Table 6-1 Items in the Ops Views Window (continued)

Item	Description	Reference
Delete button	Click this button to delete an ops view	See the "Deleting Ops Views" section on page 6-32
Resources button	Click this button to view the resources that belong to or are accessible to the ops view	See the "Viewing Resources That Belong To and are Accessible To Ops Views" section on page 6-23

Creating New Ops Views

Only the system administrator can create new ops views on the server. The number of ops views that can be created depends on the number of ops view ports that the Cisco IPICS license provides. You can view the number of ops view ports that are in the system by accessing the License Management window in the Cisco IPICS Administration Console. For more information about ops view ports, see the "Understanding the License Management Window" section on page 2-72 to view ops view ports.

After a new ops view has been created, you can associate resources, such as channels, to the ops view. The operator creates an operator user who belongs to that ops view and who can manage the ops view resources that are visible within the specific ops view.

When a resource contains or is associated to another resource that belongs to the ops view of that user, the user has the ability to remove the associated resource from the other resource, but cannot modify it in any other way.

For example, a VTG that belongs to an ops view called A Team contains a channel that belongs to an ops view called B Team. A dispatcher, who belongs to the A Team ops view, has the ability to modify any resources in the VTG including adding or removing participants who are accessible to the A Team ops view. The dispatcher can also activate or deactivate the VTG.

A dispatcher, who belongs to the B Team ops view, has the ability to view the VTG and remove the channel from the VTG, but cannot modify any resources.

Note Although operators and dispatchers cannot create ops views, these users may assign resources and define the resources that are accessible to different ops views if they have the necessary permissions. Cisco recommends that each ops view contain at least one dispatcher and one operator to manage the resources that are visible to these roles.

For information about assigning the relevant Cisco IPICS resources to ops views, see the "Performing Ops Views Tasks" section on page 6-17.

Assigning Ops Views Resources

Table 6-2 shows the Cisco IPICS resources that you can associate or assign to different ops views and where you can find additional information about assigning ops view to resources.

Table 6-2 Cisco IPICS Ops View Resources

Resource	Where to Find More Information
Users	Managing Ops Views for a User, page 3-34
User groups	Managing Ops Views for a User Group, page 3-46
Channels	Associating Users to PTT Channels, page 2-24
Channel groups	Associating Ops Views to Channel Groups, page 2-36
VTGs	Managing VTGs, page 4-2 and Understanding VTG and Sub-VTG Caveats, page 6-13
Policies	Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine," and "Using the Cisco IPICS Policy Engine"

The Benefits of Using Ops Views

By allowing you to segment your resources, the use of ops views enables greater flexibility and enhanced manageability of Cisco IPICS resources. The ops views feature may provide the following organizational benefits:

- Enhanced management of Cisco IPICS resources, such as users, channels, and VTGs for dispatchers by allowing the creation of customized ops views that enable interoperability
- Increased security by limiting operator and dispatcher access to certain Cisco IPICS resources and isolating certain Cisco IPICS resources from the view of other users
- Extended functionality by allowing multiple virtual instances of Cisco IPICS on the server
- Simplified dispatcher and operator responsibilities by limiting access to only those resources that they need to manage
- Expanded levels of responsibility by authorizing specific operators or dispatchers for the SYSTEM ops view so that these users can manage resources for the entire system

User roles determine which users can do various ops view-related activities. The "Understanding Ops Views User Roles" section on page 6-9 explains the ops view user roles.

Understanding Ops Views Attributes

This section describes the following ops views attributes that Cisco IPICS supports:

Belongs To

- This attribute determines the ops view that the resource belongs to. In other words, the ops view that you specify for this attribute is the ops view that owns this resource.
- A resource belongs to only one ops view.
- For users, the Belongs To attribute determines the resources that users see when they log in to the Cisco IPICS system. A user can view only those resources that are accessible to the ops view to which they belong.
- A VTG belongs to the same ops view as the dispatcher who created the VTG. A dispatcher who belongs to a specific ops view will always have visibility to the VTGs that belong to that same ops view.

- A policy belongs to the same ops view as the dispatcher who created the policy. A dispatcher who belongs to a specific ops view will always have visibility to the policies that belong to that same ops view.

Note Only an operator or a dispatcher who belongs to a certain ops view should create, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are associated with that ops view. This situation can cause inconsistencies when users view policies. For more information, see Chapter 7, "Using the Cisco IPICS Policy Engine," and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

- When a user logs in to a PMC or a Cisco Unified IP Phone, that user uses a PMC or Cisco Unified IP Phone usage license. Cisco IPICS calculates this license usage against the license limit of the ops view that the user currently belongs to.
- When a dispatcher activates a VTG, or when an enabled policy activates a VTG, that VTG uses a concurrent multicast port license. Cisco IPICS calculates this license usage against the license limit of the ops view that the dispatcher belongs to. When an enabled policy activates a VTG, the ops view that the policy belongs to is charged the license usage for activation of that VTG.
- Cisco IPICS calculates license usage for a concurrent LMR port against the license limit of the ops view that a channel belongs to. This usage is calculated on a per-connection basis. For more information about license usage, see the "Managing Ops Views License Usage and Limits" section on page 6-26.

Accessible To

- This attribute specifies that the resource is accessible to, or visible to, the ops view(s) that Cisco IPICS displays in this field.
- Users have access only to the resources that are accessible to the ops view to which they belong.
- A resource can be accessible to an unlimited number of ops views.

- The SYSTEM ops view can always access all resources even if it does not explicitly appear in the list of accessible ops views.

Note

- When you configure a resource to belong to a specific ops view, Cisco IPICS automatically adds that resource as being accessible to the same ops view.
- When you reconfigure the belongs to field for a resource to a different ops view, Cisco IPICS adds the newly-configured ops view to the accessible to list for that resource. However, Cisco IPICS does not remove, from the list of accessible ops views, the ops view that was previously configured.

Understanding Ops Views User Roles

Some Cisco IPICS user roles expand to assume additional responsibilities. Table 6-3 describes the various Cisco IPICS ops view user roles and their associated responsibilities.

Note Operators and dispatchers who belong to an ops view can view the VTGs that also belong to that ops view. In addition, they can also view all resources that are accessible to that ops view. These users may not view any resources that do not belong to, or are not accessible to, that ops view.

Note An operator or a dispatcher who belongs to the SYSTEM ops view can view all resources in all ops views.

Table 6-3 Cisco IPICS Ops View User Roles

Cisco IPICS User Role	Responsibilities
System Administrator	• The system administrator can add and delete ops views and can also modify the attributes of ops views. • This system administrator can associate an ops view to a channel and a channel group. • As part of the SYSTEM ops view, the system enables full access to the system administrator (and all users who belong to the SYSTEM ops view); that is, these users can see all of the resources in all of the ops views that are configured on the system. • Only those users who belong to the SYSTEM ops view can be assigned the system administrator or all roles.
Operator	• Operators who belong to the SYSTEM ops view should create at least one operator per ops view (for all ops views except the SYSTEM ops view) and define each operator as belonging to a specific ops view. These definitions allow the operators who belong to specific ops view(s) to manage the resources for their individual ops view(s). • The operator can add, edit, and delete users and user groups and assign ops views to users and user groups. • The operator can assign each user or user group to any ops view as long as the operator belongs to the SYSTEM ops view. • The operator can only belong to one ops view. Unless the operator belongs to the SYSTEM ops view, this user is limited to only viewing and managing the resources that belong to the ops views that the operator belongs to or other ops views that are accessible to the operator.

Table 6-3 Cisco IPICS Ops View User Roles (continued)

Cisco IPICS User Role	Responsibilities
Dispatcher	• The dispatcher can belong to only one ops view. Unless the dispatcher belongs to the SYSTEM ops view, this user is limited to only viewing and managing the resources that are accessible to the ops views that the dispatcher belongs to. • The dispatcher manages VTGs but otherwise cannot make changes that affect ops views. • The dispatcher can share management of a VTG with another dispatcher, even if the dispatchers are in different ops views, if the VTG contains resources that are accessible to each of the ops views. • The dispatcher manages policies that belong to the same ops view as the dispatcher or are associated to VTGs that are accessible to the ops view that the dispatcher can access.
Ops View Administrator	The ops view administrator is allowed to access the following Cisco IPICS windows: • Activity Logs—Accessed by navigating to **Administration > Activity Log Management** (includes downloading activity logs) • Activity Log Options—Accessed by navigating to **Administration > Activity Log Options** • Policies—Accessed by navigating to **Policy Engine > Policy Management** (includes Associations window)

Understanding Ops Views Caveats

This section includes information about ops views caveats that apply to this release of Cisco IPICS. For specific information about the caveats that apply to VTGs and sub-VTGs, see the "Understanding VTG and Sub-VTG Caveats" section on page 6-13.

The following caveats pertain to the use of Cisco IPICS ops views:

- Users who do not belong to a specific ops view default to the SYSTEM ops view.
- As a Cisco IPICS operator, the system allows you to view and modify only those users who either belong to or are accessible to your ops view. As a Cisco IPICS dispatcher, the system allows you to view and modify only those VTGs that contain resources that either belong to or are accessible to your ops view. You can view only those users and channels that either belong to or are accessible to your ops view.
- VTGs and policies always belong to the ops view of the user who created the VTG or the policy.
- The dispatcher can see all of the resources in a VTG as long as one of the VTG resources is in the same ops view as the dispatcher or if the VTG belongs to the same ops view as the dispatcher. If the remaining resources are not in the same ops view, the system does not display these resources in the Users or Channels panes.
- The system displays only resources that either belong to or are accessible to your specific ops view.
- Members of channel and user groups do not inherit accessibility from the groups; therefore, the system displays all of these resources whether or not they are individually accessible to the specific ops view.
- When you search for a resource by using the search functionality in the Channels, Users, and VTGs panes, the system displays only the resources that are accessible to the specific ops view.
- The policies information that the system displays in the Ops Views window reflects the policies that belong to or are accessible to the specific ops view; that is, the policies that the system shows in this area are those policies that were created by someone who belongs to this ops view.
  - Cisco IPICS enables users who belong to the SYSTEM ops view to view all of the policies that are configured on the server.
  - You can view a policy if the policy contains a VTG and that VTG contains a resource that belongs to or is accessible to your ops view.
  - You cannot view a policy that controls a VTG if that VTG does not contain resources that belongs to or is accessible to your ops view.

Note Only an operator or a dispatcher who belongs to a certain ops view should create, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are associated with that ops view. This situation can cause inconsistencies when users view policies. For more information, see Chapter 7, "Using the Cisco IPICS Policy Engine," and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

Understanding VTG and Sub-VTG Caveats

The Cisco IPICS implementation of ops view access for VTGs enables resource sharing among multiple ops views. The ops view functionality allows any dispatcher, who has access to shared resources within a VTG that belongs to a different ops view, to fully access that VTG.

For example, if a resource, (user, channel, or VTG) from ops view 1 is within a VTG and the VTG was activated by dispatcher 2 who belongs to ops view 2, the VTG is accessible to ops view 2. However, dispatcher 1 who belongs to ops view 1 is also able to access that VTG because at least one of the VTG resources is accessible to ops view 1.

The following caveats pertain to VTGs and sub-VTGs when you use ops views:

- As a general rule, VTGs inherit accessibility from the resources that it contains. That is, VTGs belong to the same ops view as the dispatcher who created them.

  The following examples depict this rule:

  a. If a dispatcher who belongs to the SYSTEM ops view creates a VTG, that VTG or policy belongs to the SYSTEM ops view. The system displays this information in the ops view details pane only for the SYSTEM ops view (it does not display in other ops views).

  b. If VTG 1 contains only a single channel (channel 1) and that channel is accessible to ops view 1 and ops view 2, then VTG 1 is also accessible to ops view 1 and ops view 2.

     Table 6-4 shows an example of VTG ops view accessibility.

Table 6-4 VTG Ops View Accessibility

Resource	Contents	Accessibility
VTG 1	Contains a single channel (channel 1)	
Channel 1		Accessible to ops view 1 and ops view 2
VTG 1		Accessible to ops view 1 and ops view 2

- This same general rule applies to VTGs that contain other VTGs (also known as sub-VTGs), depending on their states (see the next bullet for more information about this dependency).

  For example, if VTG 1 contains only VTG 2 and VTG 2 is accessible to ops view 1, then VTG 1 is also accessible to ops view 1 (because VTG 1 contains VTG 2, which is accessible to ops view 1).

  Table 6-5 shows an example of sub-VTG ops view accessibility.

Table 6-5 Sub-VTG Ops View Accessibility

Resource (state)	Contents	Accessibility
VTG 1 (active)	Contains sub-VTG (VTG 2)	
VTG 2 (active)		Accessible to ops view 1
VTG 1		Accessible to ops view 1

- With sub-VTGs, there is a dependency on the active/inactive state of the sub-VTG for purposes of determining accessibility. That is, an active VTG can only inherit accessibility from an active sub-VTG and an inactive VTG can only inherit accessibility from an inactive sub-VTG.

  By using the previous example, this means that if VTG 1 is active and VTG 2 is inactive, then VTG 1 will not be accessible to ops view 1.

  Table 6-6 shows an example of active/inactive state dependency on sub-VTG ops view accessibility.

Table 6-6 Active/Inactive Sub-VTG Ops View Accessibility

Resource (state)	Contents	Accessibility
VTG 1 (active)	Contains sub-VTG (VTG 2)	
VTG 2 (inactive)		Accessible to ops view 1
VTG 1		Not accessible to ops view 1

- An ops view that can access a sub-VTG can also access the resources in the VTG that contains the sub-VTG.
- However, an ops view that can access a VTG that contains a sub-VTG may not be able to access that sub-VTG unless there is a resource in the sub-VTG that provides access to the ops view.

  Table 6-7 shows an example of how resources in sub-VTGs can affect ops view accessibility.

Table 6-7 Sub-VTG Resources for Ops View Accessibility

VTG 1	VTG 2
VTG 1 contains the following resources: • User 1, who is accessible to ops view 1 • VTG 2 (sub-VTG)	VTG 2 contains the following resource: • User 2, who is accessible to ops view 2
VTG 1 becomes accessible to the following ops views: • Ops view 1—VTG 1 inherits accessibility from User 1 • Ops view 2—VTG 1 inherits accessibility from VTG 2, which contains User 2	VTG 2 becomes accessible to the following ops view: • Ops view 2—VTG 2 inherits accessibility from User 2

Table 6-7 Sub-VTG Resources for Ops View Accessibility (continued)

Ops View 1 Dispatcher	Ops View 2 Dispatcher
The ops view 1 dispatcher can see the details for the following resources: • VTG 1—User 1, who is accessible to ops view 1, is in VTG 1 (The ops view 1 dispatcher has no access to the contents in VTG 2 because ops view 1 does not have access to ops view 2)	The ops view 2 dispatcher can see the details for the following resources: • VTG 2—User 2, who is accessible to ops view 2, is in VTG 2 • VTG 1—VTG 2 is a sub-VTG of VTG 1

  - The ops view 1 dispatcher can see the details for VTG 1 and can add or remove resources from VTG 1. Because a sub-VTG shows as a resource in a VTG, the ops view 1 dispatcher can also remove the sub-VTG (VTG 2) even though the ops view 1 dispatcher cannot see the details of VTG 2. (The ops view 1 dispatcher can see that VTG 2 is contained in VTG 1 and this dispatcher can make changes even though the contents of VTG 2 cannot be seen.)

- You can use sub-VTGs as a way to shield the participants in the sub-VTG from other resources who should not be able to see them.
- When you associate VTGs to policies, the system displays only the VTG templates that are accessible to the ops view.
- The VTG Workspace pane displays the VTGs that belong to the specific ops view or the VTGs that contain resources that are accessible to the specific ops view. The system displays all contents of a highlighted VTG in this workspace, but the Channels, Users, and VTGs panes display only the resources that are accessible to this specific ops view.

Understanding How Ops Views Affect VTGs

This section describes the affect that ops views have on VTGs. For information about additional caveats, see the "Understanding VTG and Sub-VTG Caveats" section on page 6-13.

VTGs do not require a dispatcher to associate ops views. Cisco IPICS automatically determines the ops views that can access each individual VTG based on the VTG contents and the VTG creator.

VTGs belong to the same ops view as the user who created the VTG. Therefore, you do not need to define the belongs to field for VTGs.

For example, if an operator who belongs to the SYSTEM ops view creates a VTG, that VTG belongs to the SYSTEM ops view. The system displays this VTG in the ops view details pane only for the SYSTEM ops view (it does not display this VTG information in any of the other ops views).

Note VTGs always belong to the ops view of the user who created the VTG.

VTG Caveats

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

- The Virtual Talk Groups window displays the VTGs that belong to a specific ops view and the VTGs that contain resources that are accessible to specific ops views.
- The system displays all contents of a highlighted VTG in this window.
- The exception pertains to members of a channel or user group, who the system displays whether or not they are individually accessible to the specific ops view.

Tip If a VTG unexpectedly becomes active or inactive, check for any policies that may be associated to the VTG. An operator in another ops view can create a policy that is associated to any VTG that the operator has access to.

Performing Ops Views Tasks

There are several tasks that must be performed to create and configure ops views for use on the server. You can also edit or remove ops views, as needed. This section describes these ops views-related tasks and the affect that ops views has on Cisco IPICS resources, such as VTGs and policies.

This section includes the following topics:

- Adding Ops Views, page 6-18
- Viewing Resources That Belong To and are Accessible To Ops Views, page 6-23
- Viewing Ops Views License Details, page 6-25
- Deleting Ops Views, page 6-32

Adding Ops Views

The system displays the ops views that the system administrator creates and allows Cisco IPICS resources, such as users, user groups, channels, channel groups, VTGs, and policies to be assigned to these ops views.

Note Some fields in the SYSTEM ops view cannot be changed.

To add an ops view, perform the following procedure:

Procedure

Step 1 From the Configuration drawer in the Cisco IPICS Administration Console, click **Ops Views**.

Note When you open the Ops Views window for the first time, the system displays the SYSTEM ops view as the default ops view.

Step 2 To add a new ops view, click **Add**.

Step 3 In the Name field, enter a name for the ops view. This entry is required.

Tip The name that you enter for the ops view should be descriptive to reflect the nature of its use.

Step 4 In the Description field, enter a description for the new ops view that you are adding.

The Description field is an optional field.

Step 5 From the General tab, in the **License Allocation** pane, enter applicable license information in the fields, as described in the Table 6-8.

Table 6-8 License Allocation Fields in the Ops View Window

Feature	Limit	Current Usage
LMR Ports	Number of LMR license ports that you allocate for this ops view. Enter the number of LMR ports in the Limit field.	*Display only*—These fields indicate the number of license ports for the feature that is currently in use.
Multicast Ports	Number of multicast license ports that you allocate for this ops view. Enter the number of multicast ports in the Limit field.	
PMC Users	Number of PMC users ports that you allocate for this ops view. Enter the number of PMC users ports in the Limit field.	
IP Phones	Number of IP phone ports that you allocate for this ops view. Enter the number of IP phone ports in the Limit field.	
Dial Ports	Total number of dial ports that you allocate for this ops view. These ports are used for both the dial-in/invite and notification features. Enter the number of dial ports in the Limit field.	

For more information about managing licenses for ops views, see the "Viewing Ops Views License Details" section on page 6-25.

Step 6 In the **Dial Information and Dial Port Resource Allocation** pane, enter applicable dial information in the fields, as described in the Table 6-9.

For information about how to allocate dial ports, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 6-29. For more detailed information about the dial-in/invite and notification features, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine," and Chapter 7, "Using the Cisco IPICS Policy Engine."

Note When you add dial numbers (DNs) for ops views in a Cisco IPICS deployment that includes the policy engine, and if the new DNs fall outside of existing route patterns that are assigned to a SIP trunk (in Cisco Unified CallManager) or outside of existing destination patterns that are assigned to a dial peer (in the Cisco IOS SIP Gateway), then you must update the SIP provider configuration to include the new DNs. For more information, see the "Configuring the SIP Provider" section on page 8-41.

Table 6-9 Dial Information and Dial Port Resource Allocation Fields in the Ops View Window

Field	Description
Dial Number	This field specifies the number that users, who belong to this ops view, will dial in to Cisco IPICS.
Email address of the sender	This field specifies the e-mail address that Cisco IPICS uses to send out notifications to users in the ops view. When users who belong to the ops view, receive an e-mail notification, this e-mail address is the address from which Cisco IPICS sends the e-mail message.

Table 6-9 Dial Information and Dial Port Resource Allocation Fields in the Ops View Window

Field	Description
Default language	This field specifies the language in which the notifications are sent, as well as the language that is used by the dial engine to determine which voice prompts to play to users who call in to Cisco IPICS. **Note** Only Latin-1 supported languages give callers the option to spell the name of the channel/VTG/policy when calling in to Cisco IPICS.
Dial ports reserved for dial-in/invite feature	This field specifies the number of dial ports that you allocate for exclusive use by the dial-in/invite feature for the ops view. Dial ports allocated here are used only by the dial-in/invite feature; they are not used by the notifications feature. The dial-pool number of ports that you configure in this window are typically allocated for dial-in users who typically engage in long conversations on VTGs or channels. The dial ports that Cisco IPICS uses for notifications are allocated from the ops view of the policy that includes the notification action (the ops view of the user who created the policy). **Note** The number of ports that you allocate in this window cannot exceed the number of dial users who may be allocated from the SYSTEM ops view.

Table 6-9 Dial Information and Dial Port Resource Allocation Fields in the Ops View Window

Field	Description
Dial ports reserved for notifications	This field specifies the number of dial ports that you allocate for exclusive use by the notifications feature for the ops view. Dial ports that you allocate in this window are not used by the dial-in/invite feature. The dial-pool number of ports that you configure in this window are allocated for blast notification. These sessions are typically short in duration and play out short messages and then exit. The dial ports that Cisco IPICS uses for the notifications feature are allocated from the ops view of the policy that includes the notification action (the ops view of the user who created the policy). **Note** The number of ports that you allocate in this window cannot exceed the number of dial ports that may be allocated from the SYSTEM ops view.
Dial ports reserved for dial-in/invite or notifications	*Display only*—This number represents the total number of dial ports that are available for both the dial-in/invite and notification features. Ports are allocated from the total number of licensed dial ports that are assigned to the ops view. This field displays the number of remaining dial ports after subtracting the ports that were configured for both the dial-in/invite and notification features. For information about how to configure dial ports, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 6-29.

Note Be aware that when you allocate the number of ports in your dial pool, this number should match the number of outbound/inbound ports that are available on the gateway. The available physical ports should match the total number of outbound and inbound calls. For more information about allocating dial ports, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 6-29.

For more information about the Cisco dial engine, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

Step 7 To save your changes, click **Save**.

A Resources button displays at the bottom of the window. You can now view the resources that are accessible to this ops view. See the "Viewing Resources That Belong To and are Accessible To Ops Views" section on page 6-23.

For information about assigning resources to ops views, see the "Assigning Ops Views Resources" section on page 6-6.

Viewing Resources That Belong To and are Accessible To Ops Views

When you have created an ops view in Cisco IPICS, resources can be assigned to the ops view. See the "Assigning Ops Views Resources" section on page 6-6 for more information about how resources are assigned to ops views.

To view resources that either belong to, or are accessible to ops views, perform the following procedure:

Procedure

Step 1 From the Configuration drawer in the Cisco IPICS Administration Console, click **Ops Views**.

Step 2 To view ops view resources, take either of these actions:

- In the Name column, click the link of the ops view for which you want to view resources, and then click the **Resources** button at the bottom of the window.

- Check the check box to the left of the ops view for which you want to view resources and then click the **Resources** button at the bottom of the window.

The Resources window displays.

Step 3 Take either of the following actions:

- To view resources that belong to this ops view, choose **Resources That Belong To This Ops View** from the View drop-down list box.
  - Proceed to Step 4.
- To view resources that are accessible to this ops view, and that could be assigned to it, choose **Resources That Are Accessible To This Ops View** from the View drop-down list box.
  - Proceed to Step 4.

The resource window that you choose displays, showing information tabs for each resource.

Step 4 To view the specific resources that either belong to or are accessible to this ops view, take any of the following actions:

- To view channels that belong to or are accessible to this ops view, click the **Channels** tab.

Tip You can specify the number of rows of channels that display per results page by choosing from the Rows per page drop-down list box at the top right of the window; then click **Go**. To navigate between the results pages, click the arrows at the bottom of the window.

The channels display, showing the channel name and status for each channel.

- To view channel groups that belong to or are accessible to this ops view, click the **Channel Groups** tab.

  The channel groups display, showing the channel group name, ops view, and channel count for each channel group.
- To view users who belong to or are accessible to this ops view, click the **Users** tab.

Tip You can specify the number of rows of users that display per results page by choosing from the Rows per page drop-down list box at the top right of the window; then click **Go**. To navigate between the results pages, click the arrows at the bottom of the window.

The users displays, showing the user name, last name, first name, and status of each user.

- To view the user groups that belong to or are accessible to this ops view, click the **User Groups** tab.

  The user groups display, showing the user group name and ops view for each user group.

- To view the VTGs that belong to or are accessible to this ops view, click the **VTGs** tab.

Tip You can specify the number of rows of VTGs that display per results page by choosing from the Rows per page drop-down list box at the top right of the window; then click **Go**. To navigate between the results pages, click the arrows at the bottom of the window.

The list of VTGs display, showing the VTG name and status of each VTG.

- To view the policies that belong to or are accessible to this ops view, click the **Policies** tab.

  The policies display, showing the policy name of each policy.

Viewing Ops Views License Details

This section includes information about how to view the details about each ops view and how to configure the licenses. It includes the following topics:

- Managing Ops Views License Usage and Limits, page 6-26
- Configuring Licenses for Ops Views Usage, page 6-28

To access the detailed information for each ops view, from the Configuration drawer of the Cisco IPICS Administration Console click the **Ops Views** link. In ops view configuration window, click the name of an ops view to highlight it. The system displays the details for the specific ops view.

The ops view window includes information about the number of available license limits for licensable features, which includes LMR ports, multicast ports, PMC users, IP phones, and dial ports, as well as dial information. This information displays in the **General** tab of the window.

The numbers in the License Allocation pane represent the number of users or ports that can use Cisco IPICS per the license configuration. For example, the number 50 indicates that 50 ports or users are licensed to use the system; the number 0 indicates that no ports or users are licensed to use the system.

For more information about the ops view configuration window, see the "Performing Ops Views Tasks" section on page 6-17.

Managing Ops Views License Usage and Limits

Cisco IPICS displays detailed license information for current usage and license limits for licensable features. To view this information, navigate to the Configuration > Ops Views window; then click the name of the ops view.

Note Be aware that Cisco IPICS displays this information in a browser window. As a best practice, make sure that you update your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative 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.

Cisco IPICS uses the following criteria to determine license consumption for LMR ports, multicast ports, PMC usage, IP phones, and dial ports usage:

- LMR Ports Usage—LMR ports determine the number of enabled channels that the system can use. After the channel is deleted or disabled or the VTG is deactivated, the server releases the license and makes it available for use. An ops view is only charged for active channels to which it belongs.

- Multicast Ports Usage—An activated VTG uses a multicast port license. After a VTG is deactivated, the server releases the multicast license and makes it available for use. An ops view is only charged for VTGs that have been activated by dispatchers who belong to the ops view. A VTG can belong to only one ops view but be activated by a different ops view to which another dispatcher belongs; however, the activating ops view is charged with the license.

Note Be aware that VTGs can be automatically activated by an enabled policy and, therefore, use a license. The ops view that a policy belongs to is charged the license usage for activation of that VTG. If the number of licenses has been exceeded, the policy is not able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.

- Cisco IPICS PMC Usage—A PMC user uses a license each time that the user logs in to a PMC session. This license is used against the ops view to which the user belongs.

  If the same PMC user logs in to multiple PMC sessions from different PMC client machines, that user uses 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.

- IP Phones Usage—An IP phone user uses a license each time that the user dials in to a VTG or channel via an IP phone. This license is used against the ops view to which the user belongs.
- Dial Ports Usage—Cisco IPICS uses these licenses for dial-in, dial-out, or notification connections. For dial ports that are allocated among the ops view, dial ports are used by dial-in according to the phone number that is dialed. Each ops view has a preassigned dial-in phone number for this purpose. For dial-out, the dial ports are used from the ops view to which the user, to be dialed, belongs.

Note The policy engine requires that a dial connection make use of two multicast addresses, one for receive and one for transmit. The two multicast addresses are used only if the dial connection is used to join a VTG or channel. If the dial connection is used for notification purposes, then no multicast addresses are used.

See the "Configuring Licenses for Ops Views Usage" section on page 6-28 for more information about allocating dial ports.

For more detailed information about the dial-in/invite and notification features, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine," and Chapter 7, "Using the Cisco IPICS Policy Engine."

Configuring Licenses for Ops Views Usage

You can configure the number of licenses that should be allocated to ports, PMC users, and IP phone users, and dial users on a per ops view basis by entering the values in the License Allocation Limit field in the Ops View Configuration window.

The ability to configure these license limits allows the administrator to distribute and balance the licenses amongst the ops views. This distribution ensures that no one ops view can use more licenses than it has configured. The total number of licenses that can be allocated for each licensable feature cannot exceed the total number of licenses that are available for the entire system.

Note Cisco IPICS automatically computes any available licenses that are not being used in other ops views and allocates them to the SYSTEM ops view.

At any time, the administrator can add and/or remove ops views. When this activity occurs, the available licenses may be taken from the SYSTEM ops view (if available) or added to the SYSTEM ops view. The system administrator can also modify the allocation of ops views licenses to allow redistribution among features or ops views. When the license limits are modified, Cisco IPICS assigns to the SYSTEM ops view any licensable features that are not assigned to a specific ops view.

Ports are allocated in proportion to the number of ports that are requested by an ops view, relative to the other ops views.

Additional licenses may be purchased for some or all of the licensable features. If the new license includes a greater number of licenses, Cisco IPICS allocates the additional licenses to the SYSTEM ops view.

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.

Allocating Dial Ports for the Dial-In/Invite and Notification Features

You must allocate dial ports for users to be able to dial in to Cisco IPICS, dial out to other users, or for the system to notify users. These dial ports are configured in the Dial Information and Dial Port Resources Allocation pane in the Ops View window, and are allocated per ops view. When you allocate the dial ports, be aware of the considerations in the following sections:

- Understanding Dial Port Pools, page 6-29
- Determining How Many Dial Ports to Allocate, page 6-31

Understanding Dial Port Pools

Dial port containers (also referred to as *dial pools*) allow you to configure reserve dial ports that are only used for specific dial functions (such as dial-in/invite and notification).

These reserved dial ports ensure that you always have ports configured specifically for this use and which cannot be used for any other purpose. The following dial pools are used for reserving ports for dial-in/invite and notification:

- Dial ports reserved for dial-in/invite—This dial pool contains dial ports that can only be used for the dial-in and invite features.
- Dial ports reserved for notification—This dial pool contains dial ports that can only be used for notification.

Note When you create a new ops view, dial port licenses are reallocated from the SYSTEM ops view to the new ops view, but there is no adjustment to the dial port numbers that were configured in the Dial ports reserved for dial-in/invite and Dial ports reserved for notification dial pools for the SYSTEM ops view. For the new ops view, if the dial port numbers that you configure in the reserved dial pools exceed the number of ports in the Dial Ports field, Cisco IPICS displays an error message to alert you. To resolve this issue, reduce the number of reserved ports in the SYSTEM ops view to an appropriate number and try again.

The following list provides detailed information about the dial port fields in the Dial Information and Dial Port Resource Allocation pane:

- The Dial ports reserved for dial-in/invite or notifications field is the dial pool that contains ports that Cisco IPICS uses for both dial-in/invite and for notification. This field is a read-only field that displays as dimmed.

  The ports that display in this field are the ports that remain after you have reserved dial ports for dial-in, invite, and notification actions. The remaining number are the dial ports that are reallocated from the total number of dial ports in the Dial Ports dial pool.

  For example if there are 20 dial ports total (in the Dial Ports pool) and you have configured 5 of those dial ports in the Dial ports reserved for dial-in/invite field, and 2 dial ports in the Dial ports reserved for notification field, the Dial ports reserved for dial-in/invite or notification field display 13 dial ports.

  This total equals the number of ports remaining after subtracting 5 ports for dial-in/invite and 2 for notification. The Dial Ports field still displays 20, the total number of dial ports.

- When a dial-in or invite action executes, Cisco IPICS first checks the Dial ports reserve for dial-in/invite or notification dial pool for an available dial port that can be used for dial-in/invite. If there are not enough available dial ports in that dial pool, Cisco IPICS checks the Dial ports reserved for dial-in/invite dial pool.

- In the same way, when a notification action executes and there are no available dial ports in the Dial ports reserved for dial-in/invite or notification dial pool, Cisco IPICS checks the Dial ports reserved for notification dial pool to obtain the dial ports.

- Ports from the available dial pool are used by the currently executing policy actions. If there are fewer dial ports available than what is needed, the other individual policy actions are held in a waiting state until ports become available.

Determining How Many Dial Ports to Allocate

When you need to determine how many dial ports to allocate for a particular function, you should consider that some actions, such as notification, are usually needed on a short-term basis. Other actions, such as dialing in to a VTG, usually require dial ports for longer periods of time.

For example, when notifications are sent out, the dial ports are used only briefly because once the notification has been sent the dial port is no longer needed and becomes available again. Therefore, when you allocate ports for dial-in/invite and notification, you may want to allocate a greater number of ports for dial-in and a smaller number for notification.

Note Be aware that when you are allocate the number of ports in your dial pool, this number should match the number of outbound/inbound ports that are available on the gateway. The available physical ports should match the total number of outbound and inbound calls.

To allocate dial ports in the Ops View window, see the "Adding Ops Views" section on page 6-18.

For license allocation and dial information field descriptions, see the "Adding Ops Views" section on page 6-18.

For more detailed information about the way that dial-in/invite (also referred to as *dial-out*) and notification features work, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine," and Chapter 7, "Using the Cisco IPICS Policy Engine."

Associating a User or User Group to an Ops View

After you create the ops view, an operator must be defined as belonging to the specific ops view.

Tip To add the first operator to an ops view, you must be logged in to the server with operator privileges and belong to the SYSTEM ops view.

Note Operators who do not belong to the SYSTEM ops view cannot assign the system administrator or all roles to users.

Operators who do belong to the SYSTEM ops view cannot change a system administrator or all role user to belong to or be accessible to an ops view.

For detailed information about how to associate a user to an ops view, see the "Managing Ops Views for a User" section on page 3-34, and the "Managing Ops Views for a User Group" section on page 3-46.

Associating a Channel or Channel Group to an Ops View

When you associate a channel or channel group to an ops view, you must also specify the Belongs To and the Accessible To fields in the Ops Views pane.

Note You must perform this procedure as a Cisco IPICS system administrator and belong to the SYSTEM ops view.

For detailed information about how to associate a channel or channel group to an ops view, see the "Associating Users to PTT Channels" section on page 2-24 and the "Associating a Channel or Channel Group to an Ops View" section on page 6-32.

Deleting Ops Views

To delete ops views from Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Configuration drawer in the Cisco IPICS Administration Console, click **Ops Views**.

Step 2 Check the check box next to the ops view that you want to delete.

Note By default, Cisco IPICS includes a SYSTEM ops view. You cannot delete or edit the SYSTEM ops view.

Step 3 Click **Delete**.

Step 4 To confirm the delete operation, click **OK** when prompted.

Step 5 From the list of provided ops views, choose the ops view to which all resources (users, user groups, channels, channel groups, and VTGs) and licenses should be transferred. All transferred resources are reallocated to belong to the selected ops view.

Step 6 To finalize the resource update and to delete the ops view, click **OK**.

Using the Cisco IPICS Policy Engine

The Cisco IPICS policy engine (hereafter referred to as policy engine) provides you with the ability to create and manage policies. A policy comprises one or more actions, which are discrete functions that perform when the policy executes. For example, you could create a policy that starts a VTG and invites designated users to join the VTG. Some policies can also include one or more triggers, which cause the policy to execute automatically and, optionally, to repeat according to a specified scheduled.

To enable the policy engine, you must install a Cisco IPICS license that includes a license for the policy engine and then restart the Cisco IPICS server. For more information about licenses, see the "Managing Licenses" section on page 2-72.

You perform the policy engine activities that are described in this chapter from the Policy Management drawer in the Cisco IPICS Administration Console. To access this drawer, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-11, then choose the **Policy Management** drawer in the Policy Engine tab. Any Cisco IPICS user can access this drawer, but some activities that are available from this drawer require that you be assigned certain Cisco IPICS roles, as explained in the "Policy Activities Available for Cisco IPICS Roles" section on page 7-3.

Before you can perform many of the activities that are described in this chapter, you must configure the policy engine. For details, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

This chapter includes the following topics:

- Policy Engine Overview, page 7-2
- Policy Activities Available for Cisco IPICS Roles, page 7-3

- Understanding the Policies Window, page 7-4
- Adding a Policy, page 7-6
- Managing Actions for a Policy, page 7-8
- Managing Triggers for a Policy, page 7-16
- Associating Users with a Policy, page 7-19
- Activating a Policy Manually, page 7-21
- Deleting a Policy, page 7-22
- Viewing Information about Executing or Executed Policies, page 7-22
- Viewing Information about Scheduled Policies, page 7-25
- Re-Activating a Policy or an Action, page 7-26
- Using the Policy Engine Telephony User Interface, page 7-27

Policy Engine Overview

The policy engine enables the creation of policies, which specify actions that the system executes according to instructions that you provide. You can create an invitation policy that causes the telephony user interface (TUI) to call designated users and invite them to join a VTG or channel. You can also create a Multi-Purpose policy that activates designated VTGs, adds participants to a VTG, contacts designated users at each e-mail, Short Message Service (SMS), or pager address that is associated with the user, or provides a specified message to designated users.

You can configure triggers to activate a Multi-Purpose policy according to a schedule that you specify. A trigger can be configured to activate a policy once at a designated start date and time or it can be configured to execute the policy repeatedly according to a designated schedule.

The policy engine includes the dial engine, which enables the TUI and its associated features. The TUI lets you use a touch-tone telephone to receive information from and provide instructions to the policy engine.

With the policy engine, you can automate a variety of standard procedures for your organization. You can also efficiently automate critical notification and communication processes so that these processes can be implemented quickly and accurately.

Policy Activities Available for Cisco IPICS Roles

Table 7-1 lists the Cisco IPICS roles that are required to perform various policy engine activities.

Table 7-1 Roles Required for Policy Activities

Role	Activate Policy	Add Policy	Modify Policy	Delete Policy	View Policies	View Users	View VTGs and Channels
User	Yes	No	No	No	Associated with this user	—	—
System Administrator	Yes	No	No	No	Created by users who belong to the ops view of this system administrator[1]	All users	All VTGs and channels
Operator	Yes	Yes	Yes	Yes	Created by users who belong to the ops view of this operator[1]	Created by users who belong to or are accessible to the ops view of this operator	Created by users who belong to or are accessible to the ops view of this operator
Dispatcher	Yes	Yes	Yes	Yes	Created by users who belong to the ops view of this dispatcher[1]	Created by users who belong to or are accessible to the ops view of this dispatcher	Created by users who belong to or are accessible to the ops view of this dispatcher

Table 7-1 Roles Required for Policy Activities (continued)

Role	Activate Policy	Add Policy	Modify Policy	Delete Policy	View Policies	View Users	View VTGs and Channels
Ops View Administrator	Yes	No	No	No	Created by users who belong to the ops view of this ops view administrator[1]	Created by users who belong to or are accessible the ops view of this ops view administrator	Created by users who belong to or are accessible the ops view of this ops view administrator
All	Yes	Yes	Yes	Yes	Created by users who belong to the ops view of this user[1]	All users	All VTGs and channels

1. If this user belongs to the system ops view, this user can view all policies.

Understanding the Policies Window

The Policies window lists information about each of the policies that you have configured in Cisco IPICS. It also provides you with the capability to perform several policy management functions.

To display the Policies window, access the Policy Management drawer and click **Policies**.

Table 7-2 describes the items in the Policies window.

Table 7-2 Items in the Policies Window

Item	Description	Reference
Name field	Unique name that is assigned to the policy	See the "Adding a Policy" section on page 7-6
Type field	Type of the policy	See the "Adding a Policy" section on page 7-6
Action Names field	Actions that are associated with the policy	See the "Managing Actions for a Policy" section on page 7-8
Trigger Names field	Triggers that are associated with the policy	See the "Managing Triggers for a Policy" section on page 7-16
Ops View field	Displays the ops view to which the policy belongs	A policy is automatically assigned the ops view of the user who created the policy (for related information, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views")
Prompt field	Indicates whether a spoken name prompt is recorded for the policy	See the "Managing Prompts for a User" section on page 3-36
Add button	Provides the ability to add a new policy	See the "Adding a Policy" section on page 7-6
Delete button	Provides the ability to delete a policy	See the "Deleting a Policy" section on page 7-22
Activate button	Provides the ability to activate a policy	See the "Activating a Policy Manually" section on page 7-21
Associations button	Provides the ability to associate users with a policy	See the "Associating Users with a Policy" section on page 7-19

Only the operator, dispatcher, or all role users who belong to a certain ops view should add, edit, or delete policies that are associated with that ops view. If an operator or a dispatcher who belongs to the SYSTEM ops view modifies a policy that belongs to an ops view other than SYSTEM, it is possible to associate with the policy resources that are not accessible to the operators or dispatchers who are

associated with that ops view. This situation can cause inconsistencies when users view policies. Operators or dispatchers who belong to the SYSTEM ops view should add, edit, or delete policies for that ops view only.

Adding a Policy

A policy defines a set of actions that the system executes according to instructions that you provide in the policy. A policy can be either of these types:

- Invitation—Policy activated only through the TUI that causes the TUI to call designated users and invite them to join a VTG or channel. You can invoke an invitation policy from the TUI breakout menu after you have joined a VTG or a channel. Users that the TUI calls are invited to join that VTG.
- Multi-Purpose—Policy that performs any one of the following activities:
  - Activates designated VTGs
  - Adds participants to a VTG
  - Contacts designated users at each e-mail, SMS, or pager address that is associated with the user as described in the "Managing Communications Preferences for a User" section on page 3-23
  - Provides the specified message to designated users by causing the TUI to call them according to the dial preferences that are configured as described in the "Managing Communications Preferences for a User" section on page 3-23

When you create a policy, make sure that your system has sufficient resources (multicast addresses and dial ports) to accommodate the associated VTGs when they execute. Cisco IPICS does not warn you that a policy that you define may over-commit system resources when it activates VTGs.

To add a policy, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

The Policy Management window displays.

Step 2 In the Policies area, click **Add**.

The New Policy window displays.

Step 3 In the **General** tab, take these actions:

a. In the Policy Name field, enter a unique name for the policy.

This entry is required. You might find it useful to name policies according to function, such as "Notify Emergency Team."

b. In the Policy Description field, enter a description for this policy.

c. From the Policy Type drop-down list, choose one of these types:

- Multi-Purpose—Creates a policy that activates designated VTGs, notifies designated users based on notification preferences, adds participants to a VTG, or dials designated users based on dial preferences
- Invitation—Creates a policy that invites designated users to join a designated VTG or a channel

d. Click **Save**.

Step 4 Perform the tasks that are described in Table 7-3, as needed.

You do not need to perform these tasks now. You can enter or update this information later.

Table 7-3 Tasks for Adding a Policy

Task	Reference
Enter one or more actions for the policy.	See the "Managing Actions for a Policy" section on page 7-8.
Designate the users who can activate or deactivate this policy.	See the Associating Users with a Policy, page 7-19.

Managing Actions for a Policy

An action specifies the activity that a policy performs when it executes. The actions available for a policy depend on the policy type. Actions include the activities that are described in Table 7-4.

Table 7-4 Policy Actions

Action	Associated Policy Type	Description
Invite to VTG	Invitation	Calls designated users and invites them to join a VTG by responding to TUI prompts. This policy can be activated only through the TUI when you break out of an existing VTG. In this case, this action calls users according to their dial preferences and invites them to join the VTG from which you broke out.
Activate VTG	Multi-Purpose	Activates the designated preconfigured VTGs.
Notification	Multi-Purpose	Sends the designated message to each designated user at the e-mail, SMS, or pager address that is associated with the user.
VTG Add Participants	Multi-Purpose	Adds the designated participants to the designated VTG.
Dial Out	Multi-Purpose	Calls the designated users according to their configured dial preferences to invite them join to the designated VTG.

A policy can have an unlimited number of actions. If a policy includes more than one action, the policy engine executes the actions in the order that they are listed in the Policies window.

You can add, update, or delete actions for any policy. The procedure that you perform to add or update an action depends on the type of policy.

Managing actions for a policy involves these activities:

- Adding or Updating an Action for a Multi-Purpose Type Policy, page 7-9
- Adding or Updating an Action for a Multi-Purpose Type Policy, page 7-9
- Deleting an Action, page 7-15

Adding or Updating an Action for a Multi-Purpose Type Policy

A Multi-Purpose type policy can activate a VTG, send notification messages to users, add participants to a VTG, or call users and invite them to a VTG.

To add or update actions for a Multi-Purpose type policy, perform the following procedure. If you update an action for a policy that is executing, that change takes affect with the policy execution completes.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy for which you want to add an action.

Step 3 Click the **Action** tab.

The Policies > *Policy Name* window displays a list of actions that have been created for this policy. The Action Type column displays the type of action and the Action Name column displays the name that was assigned to the corresponding action when it was created.

Step 4 Take either of these actions:

- To add a new action, choose one of these options from the **Add Action** drop-down list:
  - Activate VTG—Activates the designated VTGs
  - Notification—Sends the designated message to the designated user
  - VTG Add Participants—Adds designated participants to the designated VTG
  - Dial Out—Calls designated users to invite them to the designated VTG
- To view or update an existing action, click the link for the action in the Action Type column.

The New Action window displays. The areas and fields in this window vary depending on the action type that you choose.

Step 5 In the Action Name field, enter a name for this action.

This entry is required. If a policy includes more than one action, each action name must be unique.

Step 6 Follow the steps in Table 7-5 to enter additional information for the action type that you chose.

Table 7-5 Creating or Updating an Action for a Multi-Purpose Type Policy

Step	Notes
Action Type: Activate VTG	
1. In the Duration fields, enter the number of days, hours, or minutes that a VTG remains active after it is activated by the policy.	If you do not enter a value in this field, the VTG will remain active until it is deactivated manually.
2. Specify the VTGs that this action activates when the policy executes: • Choose **VTG** from the View drop-down list. • Click **Search** and, in the Search window, locate and choose the VTGs that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-13. If you want to remove any VTG from the list, click the check box next to the VTG in the Select VTGs area, click **Delete**, and then click **OK** in the confirmation dialog box that appears.
3. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.
Action Type: Notification	
1. From the Type drop-down list, choose the type of notification message.	Message types include the following: • Message—Plays a recorded message that instructs users to check their e-mail for messages. • Dial Engine Script—Plays a notification script to users.

Table 7-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
2. If you chose **Message** from the Type drop-down list, take these actions: – In the Subject field, enter a descriptive subject for the message. – In the Message area, enter the message to be sent to the e-mail, SMS, and pager addresses that are configured as notification preferences for the user. If you chose **Dial Engine Script** from the Type drop-down list, take these actions: – From the Dial Engine Script drop-down list, choose the desired script. – From the Language drop-down list, choose the language in which to play the script.	—
3. From the View drop-down list, choose the type of recipient to receive the notification.	View types include the following: • User—Users with any role that are configured in Cisco IPICS. • User Group—User groups that are configured in Cisco IPICS. • VTG—VTGs that are configured in Cisco IPICS. When you designate a VTG, the notification is sent to all participants in that VTG.

Table 7-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
4. Click **Search** and, in the Search window, locate and choose the recipients that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-13. If you want to remove any recipient from the list, click the check box next to the recipient in the Recipients area, click **Delete**, and then click **OK** in the confirmation dialog box that appears. If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.
5. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.
Action Type: VTG Add Participants	
1. From the VTG drop-down list, select the VTG to which participants will be added when this policy executes.	VTGs that you see depend on the ops views configuration. For more information, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views.")
2. From the View drop-down list, choose the type of participant to be added to the VTG.	View types include the following: • User—Users with any role that are configured in Cisco IPICS. • User Group—User groups that are configured in Cisco IPICS. • VTG—VTGs that are configured in Cisco IPICS.

Table 7-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
4. Click **Search** and, in the Search window, locate and choose the participants that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-13. If you want to remove any participant from the list, click the check box next to the participant in the Participants area, click **Delete**, and then click **OK** in the confirmation dialog box that appears. If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.
5. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.
Action Type: Dial Out	
1. From the VTG drop-down list, choose the VTG to which the user who is called will be added.	This list shows only VTGs that you are associated with.
2. From the View drop-down list, choose the type of recipient to be called and invited to join the VTG.	View types include the following: • User—Users with any role that are configured in Cisco IPICS. • User Group—User groups that are configured in Cisco IPICS.
3. Click **Search** and, in the Search window, locate and choose the recipient that you want.	For information about using the Search window, see the "Using Search Windows" section on page 1-13. If you want to remove any recipient from the list, click the check box next to the recipient in the Recipients area, click **Delete**, and then click **OK** in the confirmation dialog box that appears. If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.
4. Click **Save** to save your changes.	If you do not want to save your changes, click **Cancel**.

Adding or Updating an Action for an Invitation Type Policy

An invitation type policy calls designated users and invites them to join a VTG.

To add or update actions for an invitation type policy, perform the following procedure. If you update an action for a policy that is executing, that change takes affect when the policy execution completes.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy for which you want to add an action.

Step 3 Click the **Action** tab.

The Policies > *Policy Name* window displays a list of actions that have been created for this policy. The Action Type column displays the type of action and the Action Name column displays the name that was assigned to the corresponding action when it was created.

Step 4 Take either of these actions:

- To add a new action for the policy, choose **Invite To VTG** from the action type from the **Add Action** drop-down list.
- To view or update an existing action, click the link for the action in the Action Type column.

Step 5 In the Action Name field, enter a name for this action.

This entry is required. If a policy includes more than one action, each action name must be unique.

Step 6 Click **Search** and, in the Search window, locate and choose the users to be invited to the VTG.

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

If you want to remove any recipient from the list, click the check box next to the recipient in the Recipients area, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

If you want to see notification preferences for a user in the list, check the check box next to the user name and then click **Show User Prefs**.

Step 7 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Deleting an Action

You can delete a single action from a policy or you can delete several actions at one time. If you delete an action while its associated policy is executing, the action is removed after the execution completes.

To delete an action or actions, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy that includes the action that you want to delete.

Step 3 Click the **Action** tab.

Step 4 Check the check box next to each action that you want to delete.

Step 5 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 6 To confirm the deletion, click **OK**.

If you do not want to delete this action, click **Cancel**.

Managing Triggers for a Policy

A trigger is a mechanism that activates a Multi-Purpose type policy according to a schedule that you specify. Triggers do not apply to invitation policy types, which can be activated only through the TUI. A Multi-Purpose type policy can have an unlimited number of triggers.

A trigger can be configured to activate a policy once at a designated start date and time, or it can be configured to execute the policy repeatedly according to a designated schedule.

Managing triggers involves these activities:

- Adding, Viewing, or Updating a Trigger, page 7-16
- Deleting a Trigger, page 7-19

Adding, Viewing, or Updating a Trigger

You can add, view, or update triggers for any Multi-Purpose type policy.

Before you can configure a trigger, you must configure an action for the policy as described in the "Adding or Updating an Action for a Multi-Purpose Type Policy" section on page 7-9.

To add, view, or update a trigger for a Multi-Purpose type policy, perform the following procedure. If you update a trigger for a policy that is executing, that change takes affect with the policy execution completes.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the Multi-Purpose type policy for which you want to add an action.

Step 3 Click the **Trigger** tab.

The Policies > *Policy Name* window displays a list of triggers that have been created for this policy. The Trigger Type column displays the type of trigger and the Trigger Name column displays the name that was assigned to the corresponding trigger.

Step 4 Take either of these actions:

- To add a new trigger, click **Add** at the bottom of the list of triggers.
- To view or update an existing trigger, click the link for the trigger in the Trigger Type column.

The New Trigger window displays.

Step 5 From the Trigger Type drop-down list, choose **Time**.

Step 6 In the Trigger Name field, enter a descriptive name for the trigger.

This entry is required. If a policy includes more than one trigger, each trigger name must be unique.

Step 7 Designate when the policy first executes by taking these actions:

a. In the Start Date field, enter the date on which the policy first executes.

b. From the Start Time drop-down list, choose the hour, minute, and time designation (AM or PM) at which the policy executes on the start date.

For a non-recurring policy, these fields designate the date and time that the policy executes one time. For a recurring policy, these fields designate the date and time that the policy first executes and the time that each subsequent execution starts.

Step 8 Take either of these actions:

- If you want the policy to execute only once, choose None from the Recurrence drop-down list, and then go to Step 11.
- If you want the policy to execute more than once, choose one of the following options from the Recurrence drop-down list:
  - Daily—Policy executes every day or every certain number of days
  - Weekly—Policy executes every certain number of weeks on designated days
  - Monthly—Policy executes every certain number of months on designated days
  - Yearly—Policy executes once a year on the designated day

Step 9 If you chose a recurrence option, in the Recurrence End Date field, enter the date on which the policy will last execute.

Step 10 If you chose a recurrence option, follow the steps in Table 7-6 to designate how often the policy executes.

Table 7-6 Designating a Recurrence Pattern for a Trigger

Steps	Examples
Recurrence: Daily	
Enter a number between 1 and 999 to designate the cycle, in days, for the execution of the policy.	• Every 1 day(s)—Policy executes every day. • Every 2 day(s)—Policy executes every other day.
Recurrence: Weekly	
1. Enter a number between 1 and 999 to designate the cycle, in weeks, for the execution of the policy. 2. Check one or more check boxes to indicate the days on which a policy executes during a week that it executes.	• Every 1 week(s) on Monday, Tuesday—Policy executes on Monday and Tuesday of every week. • Every 3 week(s) on Monday, Wednesday, Friday—Policy executes on Monday, Wednesday and Friday every 3 weeks.
Recurrence: Monthly	
Take either of these actions: • Click the **Day** radio button, choose how often during a month the policy executes, and choose the cycle, in months, for the execution of the policy • Click the lower radio button and choose the day that a policy executes, and choose how often, in months, the policy executes.	• Day 04 every 1 month(s)—Policy executes the 4th day of every month. • Day 06 every 3 month(s)—Policy executes every 6th day of the month every 3 months. • The First Monday every 1 month(s)—Policy executes on the 1st Monday of every month. • The Last Friday every 6 month(s)—Policy executes on the last Friday every 6 months.
Recurrence: Yearly	
Choose the month and date on which the policy executes each year.	• January 3—Policy executes on January 3 each year.

Step 11 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Deleting a Trigger

You can delete a trigger at any time. You can delete a single trigger or you can delete several triggers at one time. If you delete a trigger while its associated policy is executing, the action is removed after the execution completes.

To delete a trigger or triggers, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 In the Policies column, click the link for the policy that includes the trigger that you want to delete.

Step 3 Click the **Trigger** tab.

Step 4 Check the check box next to each trigger that you want to delete.

Step 5 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 6 To confirm the deletion, click **OK**.

If you do not want to delete this trigger, click **Cancel**.

Associating Users with a Policy

A user who is associated with a policy can activate and deactivate the policy. A policy can have an unlimited number of associated users, and a user can be a associated with an unlimited number of policies.

To associate a user with a policy, perform the following procedure. If you update associations for a policy that is executing, that change takes effect when the policy execution completes.

Note A Cisco IPICS operator can associate users with a policy as described in the "Associating Policies with a User" section on page 3-32.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 Take either of these actions:

- Click the link for the policy in the Policies column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the Policy name, then click the **Associations** button at the bottom of the Policies window

Step 3 The Associated Users window appears, which displays the following information for each user that is associated with the policy:

- User Name—Unique identification name assigned to the user when the user was added to Cisco IPICS
- First Name—First name of the user
- Last Name—Last name of the user
- Status—Whether the user is enabled or disabled

Step 4 Click **Add** and, in the Search window, locate and choose the users to be associated with the policy.

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

The users that you choose appear in the list of associated users. If you want to remove any user from the list, click the check box next to the user, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

Activating a Policy Manually

You can manually activate a Multi-Purpose type policy at any time. When you activate a policy, it immediately begins to execute the actions that are configured for it.

You can manually activate a single policy, or you can manually activate several policies at one time.

Note A Multi-Purpose type policy can also be activated by a trigger, by re-activating it on the Execution Status window, or through the TUI.

An invitation type policy can be activated only through the TUI.

To manually activate a Multi-Purpose policy, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 Check the check box next to each Multi-Purpose type policy that you want to activate.

Step 3 Click **Activate**.

Deleting a Policy

You can delete a policy when you no longer need it. You can delete a single policy or you can delete several policies at one time. If you delete a a policy that is executing, the execution completes.

To delete a policy, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Policies**.

Step 2 Check the check box next to each policy that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this user group, click **Cancel**.

Viewing Information about Executing or Executed Policies

You can view summary or detailed information about policies that are executing or that have executed. This information includes the policy name, associated actions, status, start time, execution messages. You can also access additional information for actions, including a list of recipients that a policy calls, whether the call was successful, and if not, why not.

To view information about policies that have not executed, see the "Viewing Information about Scheduled Policies" section on page 7-25.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Execution Status**.

Step 2 Click the **Executing/Executed Policy** tab.

This tab displays the following information:

- Name—Name of the policy, or name of an action in an expanded policy view.
- Action Type—Type of action. Information displays if you expand the view of a policy.
- Status—Status of the policy, such as Successful, Executing, or Failed.

  If any action in a policy with more than one action fails, the status of the policy will show as Failed. The policy attempts to execute all actions even if one or more actions fail.
- Start Time—Date and time that an upcoming policy or action is scheduled to start, or date and time that an executing policy or action started.
- Message—Summary information regarding the execution of the policy.

Tip To make sure that the Execution Status window shows the most current information, click **Refresh**.

Step 3 To navigate this tab or to change the display, see Table 7-7.

Table 7-7 Executing/Executed Policy Tab Activities

Activity	Procedure
Designate how many rows of information appear on a page.	Choose a value from the Rows per page drop-down list and then click **Go**.
Go to another page of the display.	Use these buttons at the bottom of the window: • |< (go to first page) • < (go to previous page) • > (go to next page) • >| (go to last page)

Table 7-7 Executing/Executed Policy Tab Activities (continued)

Activity	Procedure
Display the list of policies in alphabetical or reverse alphabetical order by name or status, or in numerical order or reverse numerical order by start time.	Click the appropriate column heading, then click the Up Arrow or the Down Arrow next to that column heading.
See an expanded view with information about the actions that are associated with a policy.	Click **+** next to the policy name.
Close an expanded view with information about the actions that are associated with a policy.	Click **-** next to the policy name.
See additional information about the participants in a dial out or notification action that is associated with the policy.	Click the action name link after expanding the view of the policy.
Delete the information for a policy.	Click **Delete**, which appears at the bottom of the window. This action deletes execution information only. It does not delete the policy. You cannot select and delete information about individual actions in a policy.
Re-activate a policy, an action, or an action for a specific participant in a policy.	See the "Re-Activating a Policy or an Action" section on page 7-26.

Viewing Information about Scheduled Policies

You can view summary or detailed information about policies that are scheduled to execute. This information includes the policy name, associated actions, status, start time, and execution messages.

To view summary information about policies that are executing or that have completed executing, see the Viewing Information about Executing or Executed Policies, page 7-22.

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Execution Status**.

Step 2 Click the **Scheduled Policy** tab.

This tab displays the following information:

- Name—Name of the policy, or name of an action in an expanded policy view.
- Action Type—Actions that are created for this policy. Information displays if you expand the policy as described in Step 3.
- Status—Status of the policy, such as Successful, Executing, or Failed.
- Start Time—Date and time that an upcoming policy is scheduled to start, or date and time and an executing policy started.
- Message—Summary information regarding the execution of the policy.

Step 3 To see an expanded view with information about the actions that are associated with a policy, click **+** next to the policy name.

To close this expanded view, click **-**.

Re-Activating a Policy or an Action

You can use the re-activate feature to perform any of these activities:

- Re-activate a policy—Activates a Multi-Purpose type policy again. This activity has the same effect as manually activating the policy as described in the "Activating a Policy Manually" section on page 7-21. You can re-activate a single policy, or you can re-execute several policies at one time. You cannot reactivate an invitation type policy.
- Re-activate an action—Activates one or more specific actions in a designated policy.
- Re-activate an action for a specific participant—Activates a dial out or a notification action for one or more specific participants in that action.

To re-activate a policy or an action, perform the following procedure:

Procedure

Step 1 From the Policy Management drawer in the Cisco IPICS Administration Console, choose **Execution Status**.

Step 2 Click the **Executing/Executed Policy** tab.

Step 3 Perform the desired activity as described in Table 7-8.

Table 7-8 Re-activation Activities

Activity	Procedure
Re-activate a policy	1. Check the check box next to each policy or policies that you want to re-activate. 2. Click **Reactivate** at the bottom of the list of policies.

Table 7-8 Re-activation Activities (continued)

Activity	Procedure
Re-activate an action in a policy.	1. Click + next to the name of the policy that includes the action. 2. Check the check box next to each action or actions that you want to re-activate. 3. Click **Reactivate** at the bottom of the list of policies.
Re-activate a dial out or a notification action for a specific participant in the action.	1. Click + next to the name of the policy that includes the action. 2. Click the link in the Name column for the action that includes the participant. 3. Check the check box next to each participant or or participants that you want to re-activate. 4. Click **Reactivate** at the bottom of the list of participants.

Using the Policy Engine Telephony User Interface

The policy engine TUI lets you use a touch-tone telephone to receive information from and provide instructions to the policy engine. When you use the TUI, the policy engine communicates with you through verbal prompts that you hear on your telephone. You respond to these prompts by pressing keys on your telephone.

The TUI provides the capability for you to perform these activities:

- Join and participate in a VTG or a channel with which you are associated by using your phone as a push-to-talk (PTT) device

Note You can also use a Cisco Unified IP Phone as a Cisco IPICS PTT device as described Appendix B, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

- Activate a policy of any type
- Perform activities designated by a policy
- Invite other users to join a VTG
- Record spoken name prompts
- Change your digit password (PIN)
- Obtain status information about policies that have executed or are executing

Accessing the TUI

You can access the TUI from a touch-tone telephone. You can access the TUI in these ways:

- By calling the policy engine—Call the number that is configured in the Dial Number field for your ops view. (For related information, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views.")
- By receiving a call from the policy engine—You receive a call when another user invites you to join a VTG, when a Cisco IPICS dispatcher initiates a dial out from the VTG Management window, when a policy that includes one or more actions to call you executes, or when you record a prompt.

When you access the TUI, perform these actions:

1. Follow the verbal prompts to enter your user ID and PIN.

   A user ID and PIN are configured by a Cisco IPICS operator or by a user. Your login credentials work only for the dial number that is configured for the ops view that you belong to.

2. Follow the verbal prompts to perform the desired action or actions.

Guidelines for using the TUI

When you use the TUI, be aware of the guidelines that are listed in the following sections:

- General Guidelines, page 7-29
- Menu Guidelines, page 7-30

General Guidelines

The following general guidelines apply when you use the TUI:

- After you dial in to the TUI, the system prompts you to enter your user ID and PIN (password). You must authenticate before you can continue to use the system.
- When you call the system, the language in which you hear prompts is the default language that is configured for the ops view with which you are associated.
- The system spells out your user name if you do not have a recorded spoken name.
- After you authenticate, the system announces the available menu options, such as joining a channel or VTG, invoking a policy, or accessing the system menu.
- The TUI allows you to interrupt a prompt and dial ahead by entering your next option before the prompt has finished.
- A menu times out if you do not respond within the predefined allowable period of time. In most instances, this period of time is 3 seconds and includes a maximum retry limit of 3. When the allowable period of time has expired, the TUI responds with “Are you still there?” and the menu repeats. When the maximum retry limit has been exceeded, the TUI responds with a warning prompt to inform you that the call will be disconnected and then it terminates the call.
- If the system does not detect a response to the prompts after a predefined number of consecutive attempts, the system returns you to the previous menu or terminates the call, if you are using the main menu.
- When you enter an incorrect key option, the TUI responds with “Please try again” and the menu repeats.
- When you dial out to invite a party in to a call, the called user must press any key to authenticate before the call is connected to the channel or VTG. (As the call is being dialed out, the system does not play any sounds.)
- To terminate your input, press #.
- To return to the previous menu, except when you are using the main menu, press *.

- To select resources, such as channels, VTGs, or policies, from a menu, press the number that corresponds to your selection when the number of entries is 9 or less. When 10 or more entries exist, you must press the number that corresponds to your selection followed by #.
- The option to select a resource by spelling its name depends on your locale:
  - The TUI supports the following locales: Afrikaans (af), Albanian (sq), Basque (eu), Catalan (ca), Danish (da), Dutch (nl), English (en), Faroese (fo), Finnish (fi), French (fr), German (de), Icelandic (is), Irish (ga), Italian (it), Norwegain (no), Portuguese (pt), Rhaeto-Romanic (rm), Scottish (gd), Spanish (es), Swedish (sv)
  - If you use a locale that does not support dial by name, such as locales that do not have equivalent characters available on the phone keypad to enable dial by name, you must make your selection from the list of available resources.

Menu Guidelines

The following guidelines apply when you use the TUI menus:

- Transfer and conference features are not supported on a phone when the phone is connected to the TUI.
- From the TUI main menu, you can take the following actions:
  - To join a channel or VTG, press 1. Then, you can press 1 to select an assigned channel or VTG to join by spelling out the channel/VTG name, or press 2 to listen to the list of assigned channels/VTGs and then selecting from that list. (If you know the name of the channel or VTG that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available channels/VTGs.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke a general purpose policy, press 2. Then, you can press 1 to select a policy by spelling its name, or press 2 to listen to the list of available policies. (If you know the name of the policy that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available policies.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.

  - To invoke the system menu, press 0. From this menu, you can take the following actions:

    - To access system help, press 1. This option provides an overview of the system menu.

    - To manage your user profile, press 2. To change your PIN, or password, press 1. To change your recorded name, press 2.

    - To obtain policy status, press 3. To replay the information, press 1.

    - To return to the previous menu from these menus, press *.

- The TUI provides a dial-in floor control feature to support dial-in users:
  - From the TUI call menu, you can take the following actions:

    - To request the floor, press 1. You hear a single beep if you obtain the floor. You hear a busy tone if the floor is not available to you.

    - To release the floor, press 2. You hear a double-beep to confirm that the floor is released.

  - The dial-in floor allows one dial-in user at a time to speak in a VTG or channel. It does not control whether other PTT users can speak.
  - When you have the dial-in floor, you can speak and be heard by other users in a VTG or channel, but you cannot hear other users talking.
  - When you have the dial-in floor, the TUI prompts every two minutes to confirm that you want to keep the floor. Press 1 to keep the floor or press 2 to release the floor.
- From the TUI breakout menu, you can take the following actions:
  - To access system help, press 1. This option provides an overview of the system menu.
  - To invite a dial user to join the call by using an ad-hoc invitation or by using an invitation policy, press 2.

    - To perform an ad-hoc invitation, press 1. To confirm your selection, press 1 (no sounds play during the time that it takes for the remote party to pick up and authenticate). To try your call again, press 2. To cancel, press *.

    - To perform an invitation policy, press 2. To choose an invitation policy by spelling out the name, press 1. To listen to the list of invitation policies, press 2 and then select from that list. To confirm your selection, press 1. To cancel, press 2. To return to the previous menu, press *.

- To invoke a general purpose policy, press 3. To choose an invitation policy by spelling out the name, press 1. To listen to the list of invitation policies, press 2 and then select from that list. To confirm your selection, press 1. To cancel, press 2. To return to the previous menu, press *.
- To leave the call and return to the main menu, press 0.
- To return to the call, press *.

CHAPTER 8

Configuring and Managing the Cisco IPICS Policy Engine

The Cisco IPICS policy engine includes the dial engine, which enables the TUI and its associated features. Configuring and managing the policy engine includes the following activities:

- Managing the dial engine—Includes monitoring system status and logs, as needed. and configuring several features such as spoken names and direct dial. Also involves managing system and custom scripts and prompts. Scripts enable the TUI to handle incoming and outgoing calls. An executing script plays prompts, which provide audio instructions to users.
- Configuring Cisco Unified CallManager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider for use with the policy engine.

You perform the policy engine activities that are described in this chapter from the Dial Engine drawer in the Cisco IPICS Administration Console. To access this drawer, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-11, then choose the **Dial Engine** drawer in the Policy Engine tab.

To access the Dial Engine drawer, you must be assigned one of these Cisco IPICS roles: system administrator, dispatcher, operator role, or all. A system administrator or user with the All role can perform any activity in this drawer. A dispatcher or operator can perform only activities that relate to managing spoken names prompts, managing standard script prompts, and managing customized script prompts.

For additional information about using many of the policy engine features, see Chapter 7, "Using the Cisco IPICS Policy Engine."

Note

- The policy engine requires that dial ports be configured before users can dial in to Cisco IPICS and before the policy engine can dial out to users. For information about configuring dial ports, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 6-29.
- The dial-in and dial-out functionality also requires addresses be available in the multicast pool. For information about configuring the multicast pool, see the "Managing the Multicast Pool" section on page 2-47.

This chapter includes these topics:

- Obtaining Information about Dial Engine Services, page 8-2
- Managing Tracing for the Policy Engine, page 8-4
- Managing Prompts, page 8-10
- Managing Dial Engine Scripts, page 8-30
- Configuring SIP, page 8-34
- Configuring Dial Engine Parameters, page 8-36
- Managing the Direct Dial Feature, page 8-37
- Configuring the SIP Provider, page 8-41

Obtaining Information about Dial Engine Services

To operate properly, the dial engine requires a variety of services. You can check the status of these services and view related information, such as the date and time that the service last started. You can also obtain log files, if needed for troubleshooting purposes.

Note For related information about obtaining log files for troubleshooting, refer to the *Cisco IPICS Troubleshooting Guide*.

To obtain information about the dial engine service, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Status**.

The Status window displays. This window shows the following information for each service:

- Service Name—Name of the service
- Status—Current state of the service:
  - INITIALIZING—Service is starting up
  - IN_SERVICE—Service is operating
  - OUT_OF_SERVICE—Service is not operating
  - PARTIAL_SERVICE—Some service functions are not operating
- Description—Brief description of the service

Tip To make sure that the Status window shows the most current information, click **Refresh**.

Step 2 To see a list of subservices for a service, click **+** next to the service name.

To close this expanded view, click **-**.

Step 3 To see additional information or to obtain log files for a service, click the link for the service in the Service Name column.

The Status Details window displays. You can take the following actions in this window:

- View the following information about the service:
  - Service Name—Name of the service
  - Description—Brief description of the service
  - Status—Current state of the service
  - Last Failure—Date and time that the service last failed
  - Last Start Time—Date and time that the service last started

  - Latest Log File—Name of the most current log file that contains information that relates to the service

- Obtain the latest log file for the service. To do so, click the link for the log file and follow the on-screen prompts. (The Latest Log File line in the top part of the window shows the name of the most current log file.)
- Click **Refresh** to make sure that the Status Details window shows the most current information.
- Click **Done** to exit the window.

Managing Tracing for the Policy Engine

The policy engine tracing feature lets you obtain information that can be useful for troubleshooting your system. This feature logs the dial engine and cluster view daemon activities in various trace files. You can configure certain trace facilities and different trace levels to obtain the information that you need.

The policy engine includes these trace facilities:

- Cluster view daemon trace files—Provides information that relates to the cluster view daemon. The files are named Cisco*n*MCVD*n*.log, where *n* is a number that varies depending on your configuration.
- Dial engine trace files—Provides information that relates to the dial engine. The files are named Cisco*n*MIVR*n*.log, where *n* is a number that varies depending on your configuration.
- driverManager*n*.log files—Created if tracing is enabled for the LIB-MEDIA facility.
- Other trace files—Various additional files that may be required by the Cisco Technical Assistance Center (TAC) if you need troubleshooting assistance.

The policy engine provides these trace levels:

- Debug—Generates detailed information

Note XDebug *n* (extended debug)—Generates more verbose detailed information

Cisco IPICS provides default configuration settings for tracing. These settings are designed for optimal system performance, but you can change them if needed. Because tracing consumes system resources, follow these guidelines to conserve system resources if you require additional trace information for the dial engine:

- Increase the number or the size of trace files only if necessary
- Keep the number and the size of trace files to the minimum values that provide the information that you need
- Enable only the trace settings that you need or that you are instructed to enable by the Cisco TAC
- If you enable trace settings, disable them when you no longer need them

Managing tracing involves these activities:

- Configuring the Number and Size of Dial Engine Trace Files, page 8-5
- Configuring Trace Levels for Dial Engine Trace Files, page 8-6
- Performing Advanced Tracing Activities, page 8-8
- Obtaining Trace Files, page 8-9
- Interpreting Trace Files, page 8-10

Configuring the Number and Size of Dial Engine Trace Files

The dial engine trace facility logs information that is related to several dial engine services. It stores information in dial engine trace files. You can specify the number of dial engine trace files and the size of each trace file.

The system begins to log information in a new trace file each time that the current one reaches the designated maximum file size. When the number of trace files that are stored on the system reaches a designated value, each subsequent trace file overwrites the oldest existing trace file. The total size of all dial engine trace files that are stored on the system cannot exceed 3 GB.

To configure dial engine trace files, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Tracing**.

The Tracing window displays.

Step 2 In the Number of Trace Files field, enter the number of trace files that the system creates before starting to overwrite existing files.

The default number of trace files is 100.

Step 3 In the Trace File Size field, enter the maximum size, in KB, of each trace file.

The system starts a new trace file when the current one reaches this maximum size. The default file size is 3145 KB.

The default number of trace files multiplied by the trace file size should not exceed 3 GB.

Step 4 In the Trace File configuration area, click **Save**.

If you do not want to save your changes, click **Cancel**.

Configuring Trace Levels for Dial Engine Trace Files

Trace levels specify what information Cisco IPICS logs in the dial engine trace files.

Cisco IPICS provides default trace levels that are designed to log important information while ensuring optimal system performance. You can change tracing levels if you need additional tracing information. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Tracing**.

The Tracing window displays.

Step 2 In the Trace Settings area, take any of these actions:

- To enable Debug or various XDebug levels for a facility, check the appropriate check boxes. There are five XDebug levels available.
- To disable a Debug or XDebug level for a facility, uncheck its check box.
- To set the default trace levels, click **Restore Defaults**.

This action enables Debug tracing for the ENG and the SS_SIP facilities in the Trace settings area. It also enables tracing for the CVD and the CLUSTER-MGR facilities (under the CVD category) in the Advanced Trace settings area. All other tracing in both areas is disabled.

The Trace Settings area lists facilities under these categories:

- Workflow Application Scripts—Module that is responsible for the policy engine dial scripts at run time.
- Call Control—Module that is responsible for telephony signalling.

You may need to click the **+** next to a category name to see its associated facilities. To close an expanded view, click **-**.

Table 8-1 describes the facilities in the Trace Settings area.

Table 8-1 Facilities in Trace Settings Area

Facility	Description
Workflow Application Scripts Category	
APP_MGR	Provides trace information for the Applications Manager, which manages loading, invoking, and executing scripts
ENG	Provides trace information for the dial engine run time
Call Control Category	
SS_SIP	Provides trace information for the SIP Subsystem, which is the interface between the dial engine and the SIP provider (Cisco Unified CallManager or a Cisco router that is running a supported version of Cisco IOS)
LIB_MEDIA	Provides trace information for the Media Library, which manages media traffic between the dial engine and incoming or outgoing calls

Step 3 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Performing Advanced Tracing Activities

You can perform the following advanced tracing activities for dial engine trace files. Typically, you perform these activities only when instructed to by the Cisco TAC.

- Configure tracing for additional policy engine facilities—You can set trace levels for facilities other than those described in the "Configuring Trace Levels for Dial Engine Trace Files" section on page 8-6.
- Dump to the threads trace file—This file contains stack trace information about all threads that are running in the dial engine. You can dump information to this file when you need it. In addition, the system may create this file if it detects a potential problem. When new information is generated, it is appended to the existing threads trace file. The threads trace file is named JVM.log.
- Dump to the memory trace file—This file contains stack trace information about memory activities in the dial engine. You can dump information to this file when you need it. When new information is generated, the system creates a new memory trace file. The memory trace file is named memory-*n*.log, where *n* is a number that varies depending on your configuration.

To configure additional tracing or to dump to a trace file, perform the following procedure.

Note You can reset all trace levels to their default values by choosing **Control Center > Tracing** from the Dial Engine drawer and clicking **Restore Defaults** at the bottom of the Trace Settings area.

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Tracing**.

The Tracing window displays.

Step 2 Click **Advanced** at the bottom of the Tracing window.

Step 3 To set trace levels, take either of these actions in the Advanced Trace Settings area:

- To enable Debug or various XDebug *n* (extended debug) levels for a facility, check the appropriate check boxes.

- To disable a Debug or XDebug level for a facility, uncheck its check box.

The Trace Settings area lists facilities under various categories. You may need to click the **+** next to a category name to see its associated facilities. To close an expanded view, click **-**.

Step 4 To dump a trace file, take either of these actions in the Advanced Trace Settings area:

- Click **Dump Threads Trace** to dump data to the threads trace file.
- Click **Dump Memory Trace** to dump data to the memory trace file.

A message indicates whether the dump was successful.

You can view or download a file that you dumped as described in the "Obtaining Trace Files" section on page 8-9.

Step 5 Click **Save** to save any changes to the trace level settings.

If you do not want to save your changes, click **Cancel**.

Obtaining Trace Files

Trace files are stored on the Cisco IPICS server. You can obtain trace files from the Cisco IPICS Administration Console. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Control Center > Status**.

The Status window displays.

Step 2 Take one of these actions:

- To obtain cluster view daemon trace files, click the **Cluster View Daemon** link.
- To obtain dial engine trace files, a threads trace file or a memory trace file, click the **Dial Engine** link.

The Status Details window displays.

Step 3 In the Relate Log Files list, click the link for the desired log file and follow the on-screen prompts to open or save the file.

Interpreting Trace Files

Dial engine and cluster view daemon trace files contain information in standard Syslog format. These files include some or all of the following information for each event that they record:

- Line number
- Date and time that the event occurred
- Category and facility name
- Severity level
- Message name
- Explanation
- Parameters and values

For additional assistance with interpreting trace files, contact the Cisco TAC.

Managing Prompts

Prompts are recorded words or phrases. The policy engine TUI executes scripts, which use prompts to provide audio instructions and information to dial-in users.

Cisco IPICS stores prompts in the *repository* on the Cisco IPICS server. The repository is a logical storage medium in which prompts are contained and organized.

This section includes these topics:

- Managing Languages for Prompts, page 8-11—Describes how to add, rename, and delete logical language folders under which prompts are stored
- Managing Standard Script Prompts, page 8-14—Describes how to upload standard script prompts to the repository

- Managing Customized Script Prompts, page 8-16—Describes how to upload customized script prompts to the repository, download these prompts so that you can listen to them, view details about these prompts, rename these prompts, and delete these prompts
- Managing Spoken Names Prompts, page 8-20—Describes how to upload spoken names to the repository, download spoken names so that you can listen to them, record spoken names, and delete spoken names

Managing Languages for Prompts

Cisco IPICS stores prompts in the repository in logical folders that correspond to the languages of the prompts. When the policy engine TUI executes a script, it plays prompts from the language folder that is designated for the script. In this way, you can control the language in which a script executes. A special logical language folder, called default, makes prompts available to any script, regardless of the language that is designated for the script.

Managing languages for prompts involves performing the following activities to manage logical language folders:

- Viewing a List of Languages, page 8-11
- Adding a Language, page 8-12
- Renaming a Language, page 8-12
- Deleting a Language, page 8-13

Viewing a List of Languages

The Languages window displays a list of the logical language folders that are in the repository. For each language, this window shows the following information:

- Language—Descriptive name of the language obtained automatically based on the ISO-compliant name of the logical folder for the language
- Language Name—ISO-compliant name of the logical folder for the language
- Date Modified—Date and time that the folder was last modified
- Modified By—Cisco IPICS user ID of the user who last modified the folder

To display the Languages window, choose **Dial Engine** > **Prompt Management > Languages** from the **Policy Engine** tab.

Adding a Language

When you add a language, the system creates a logical folder for the language in the repository.

To add a language, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Languages**.

The Language window displays.

Step 2 Click **Add** at the bottom of the list of actions.

Step 3 In the Language Name field, enter a name for the logical folder.

This entry is required. The name must be ISO-compliant. For example, enter **en_US** for U.S. English, or enter **en** to use English as a base language if you will use several versions English.

Step 4 Click **Save** to save the new language.

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

Renaming a Language

When you rename a language, you change the name of a logical folder for the language.

If you rename a language while the policy engine is executing a dial engine script that uses that language, the script may not be able to access a prompt that it requires.

To rename a language, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Languages**.

The Language window displays.

Step 2 Check the check box next to the language that you want to rename.

Step 3 Click **Rename** at the bottom of the Language window.

Step 4 In the New Name field, enter the new name for the language.

This entry is required. The name must be ISO-compliant. For example, enter **en_US** for U.S. English or enter **en** to use U.S. English as the base language.

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

If you do not want to save your change, click **Cancel**.

Deleting a Language

When you delete a language, the logical folder for that language and all contents of the folder are removed from the repository. You can delete a single language or you can delete several languages at one time.

If you delete a language while the policy engine is executing dial engine script that uses that language, the script may not be able to access a prompt that it requires.

To delete a language or languages, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Languages**.

The Language window displays.

Step 2 Check the check box next to each language that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this language, click **Cancel**.

Managing Standard Script Prompts

Standard script prompts are used by the system-provided scripts. These prompts are stored on the Cisco IPICS server as .wav files. You cannot delete these prompts.

Managing standard script prompts involves these activities:

- Viewing a list of Standard Script Prompts, page 8-14—Displays a list of prompts and related information
- Uploading Standard Script Prompts, page 8-15—Copies prompt .wav files to the repository

Viewing a list of Standard Script Prompts

The Standard Script Prompts window displays a list of the policy engine prompts. For each prompt, this window shows the following information:

- Prompt—Name of the prompt .wav file.
- Size—Size of the prompt .wav file.
- Date Modified—Date and time that the prompt .wav file was last uploaded.
- Modified By—Cisco IPICS user ID of the user who last uploaded the prompt .wav file to the policy engine.
- Language—Name of the logical folder in which the prompt is stored. The name <default> indicates a folder that contains prompts that are available to any script, regardless of the language that is designated for the script.

To display the Standard Script Prompts window, choose **Dial Engine > Prompt Management > Standard Script Prompts** from the **Policy Engine** tab.

By default, the Standard Script Prompts window lists all standard script prompts. To see a list only of standard script prompts that are stored in a particular logical language folder, choose that language from the Language drop-down list and then click **Query**.

Tip To make sure that the Standard Script Prompts window shows the most current information, click **Refresh** at the bottom of the list of prompts.

Uploading Standard Script Prompts

Uploading a standard script prompt copies the .wav file for the prompt to the designated language folder. You must upload a prompt before it can be used in a script.

You can upload an individual standard script prompt or you can upload a .zip file that contains one or more prompts. The policy engine automatically extracts the prompt files after uploading a .zip file.

Prompts that you upload must conform to these guidelines:

- Encoding—CCITT u-law
- Bits per sample—8
- Sample rate—8 kHz
- Channels—1 (monaural)

To upload a standard script prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Standard Script Prompts**.

The Standard Script Prompts window displays.

Step 2 Click either of these buttons at the bottom of the list of prompts:

- **Upload**—Uploads a single prompt .wav file to the repository
- **Upload Zip**—Uploads a .zip file that contains one or more prompt .wav files to the repository, then extracts the files

Step 3 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 4 From the Language drop-down list, choose the logical language folder in which to store the prompt.

Step 5 Click **Save** to save to upload the prompt.

If you do not want to upload the prompt, click **Cancel**.

Managing Customized Script Prompts

Customized script prompts are prompts that you create for use in a customized script.

The following sections provide information about managing customized script prompts. For information about creating, editing, or integrating customized script prompts, contact your system integrator.

- Viewing a List of Customized Script Prompts, page 8-16—Displays a list of prompts and related information
- Uploading Customized Script Prompts, page 8-17—Copies prompt .wav files to the repository
- Downloading a Customized Script Prompt, page 8-18—Provides the capability for you to listen to a prompt
- Renaming a Customized Script Prompt, page 8-19—Changes the name of a customized script prompt
- Deleting a Customized Script Prompt, page 8-19—Removes the prompt .wav file from the repository

Viewing a List of Customized Script Prompts

The Customized Script Prompts window displays a list of customized script prompts. For each prompt, this window shows the following information:

- Prompt—Name of the prompt .wav file
- Size—Size of the prompt .wav file
- Date Modified—Date and time that the prompt .wav file was last uploaded or moved to another destination folder or language folder
- Modified By—Cisco IPICS user ID of the user who last modified the prompt .wav file
- Language—Logical language folder in which the prompt .wav file is stored

To display the Customized Script Prompts window, choose **Dial Engine > Prompt Management > Customized Script Prompts** from the **Policy Engine** tab.

By default, the Customized Script Prompts window lists all customized script prompts. To see a list only of customized script prompts that are stored in a particular logical language folder, choose that language from the Language drop-down list and then click **Query**.

Tip To make sure that the Customized Script Prompts window shows the most current information, click **Refresh** at the bottom of the list of prompts.

Uploading Customized Script Prompts

Uploading a customized script prompt copies the .wav file for the prompt to the designated language folder. You must upload a prompt before it can be used in a script.

Custom prompts files that are uploaded must be G.711 u-law encoded. The PSTN gateways must also encode the audio to G.711 u-law for the dial-in PTT functionality.

You can upload an individual customized script prompt or you can upload a .zip file that contains one or more prompts. The policy engine automatically extracts the prompt files after uploading a .zip file.

Prompts that you upload must conform to these guidelines:

- Encoding—CCITT u-law
- Bits per sample—8
- Sample rate—8 kHz
- Channels—1 (monaural)

To upload a customized script prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Click either of these buttons at the bottom of the list of prompts:

- **Upload**—Uploads a single prompt .wav file to the repository
- **Upload Zip**—Uploads a .zip file that contains one or more prompt .wav files to the repository, then extracts the files

Step 3 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 4 (Optional) In the Destination Folder field, enter the name of a a logical folder.

A language folder can include one or more destination folders. Destination folders are logical folders that let you group prompts under a language. For example, you may find it convenient to group prompts according to the scripts in which they are used.

A destination folder cannot have the same name as a language folder for prompts.

Step 5 From the Language drop-down list, choose the logical language folder for this prompt.

If you entered a destination folder in Step 4, the script is stored in that folder under the logical language folder that you specify.

Step 6 Click **Save** to save upload the prompt.

If you do not want to upload the prompt, click **Cancel**.

Downloading a Customized Script Prompt

Downloading a customized script prompt copies the .wav file for the prompt to a location that you specify. You can listen to the prompt by using any media player that plays .wav files.

To download a customized script prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Check the check box next to the prompt that you want to download.

Step 3 Click **Download** at the bottom of the Customized Script Prompts window.

If your browser has a default media player configured, the prompt plays automatically.

Otherwise, follow the on-screen prompts to download prompt. After you download the prompt, you can use a media player to listen to it.

Renaming a Customized Script Prompt

You can change the name of a customized script prompt, if necessary. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Check the check box next to the prompt that you want to rename.

Step 3 Click **Rename** at the bottom of the Customized Script Prompts window.

Step 4 In the New Name field, enter the new name for the prompt.

This entry is required.

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

If you do not want to save your change, click **Cancel**.

Deleting a Customized Script Prompt

When you delete a customized script prompt, it is removed from the repository. You can delete a single prompt or you can delete several prompts at one time.

Before you delete a prompt, make sure that it is not used by a script. The system does not warn you if the prompt is being used by a script.

To delete a prompt or prompts, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Prompt Management** > **Customized Script Prompts**.

The Customized Script Prompts window displays.

Step 2 Check the check box next to each prompt that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this prompt, click **Cancel**.

Managing Spoken Names Prompts

The TUI uses spoken names prompts to play the names of various Cisco IPICS resources to callers. You can record spoken names prompts for channels, channel groups, locations, policies, users, user groups, ops views, VTGs, and the main TUI greeting.

Note The TUI main greeting is the spoken names prompt for the ops view with which the dial-in number that you called is associated.

Managing spoken names prompts involves these activities:

- Viewing a List of Spoken Names Prompts, page 8-21—Displays a list of prompts and related information
- Uploading Spoken Names Prompts, page 8-22—Copies prompt .wav files to the repository
- Downloading a Spoken Names Prompt, page 8-24—Provides you with the capability to listen to a prompt
- Recording a Spoken Name Prompt, page 8-25—Lets you record a prompt

- Changing Information about a Spoken Names Prompt, page 8-28—Lets you change the name, language, resource type, and associated resource of a prompt
- Deleting a Spoken Names Prompt, page 8-29—Removes the prompt .wav file from the repository

Viewing a List of Spoken Names Prompts

The Spoken Names window displays a list of spoken names prompts that have been uploaded. For each prompt, this window shows the following information:

- Resource Type—Cisco IPICS resource type for which the prompt is recorded (channel, channel group, location, ops view, policy, user, user group, ops view, or VTG)
- Associated Resource—Name of the channel, channel group, location, ops view, policy, user, user group, ops view, or VTG for which the prompt is recorded
- Language—Logical language folder in which the prompt .wav file is stored
- Prompt—Shows *resource-language*, where resource is the resource that is associated with the prompt and language is the logical language folder in which the prompt .wav file is stored
- Size—Size of the prompt .wav file
- Date Modified—Date and time that the prompt .wav file was last uploaded, moved to another language folder, or updated with another associated resource
- Modified By—Cisco IPICS user ID of the user who last modified the prompt .wav file

To display the Spoken Names window, choose **Dial Engine > Prompt Management > Spoken Names** from the **Policy Engine** tab.

To see a list of specific prompts, make the desired choices from the following drop-down list and then click **Query**:

- Language—Displays prompts from the designated logical language folder. To display prompts in all language folders, choose **All**.
- Resource Type—Displays prompts for the designated resource. To display prompts for all resources, choose **All**.

- Associated Resource—Displays prompts for the designated channel, channel group, location, ops view, policy, user, user group, ops view, or VTG. The names that appear in this list depend on the resource type that you selected. This drop-down list is dimmed if you choose **All** for the resource type.

Tip To make sure that the Spoken Names window shows the most current information, click **Refresh** at the bottom of the list of prompts.

Uploading Spoken Names Prompts

Uploading a spoken names prompt copies the .wav file for the prompt to the designated language folder. You must upload a prompt before it can be used in a script.

You can upload an individual spoken names prompt or you can upload a .zip file that contains one or more prompts. The .zip file can be up to 1 GB (1,024 MB) in size. The policy engine automatically extracts the prompt files after uploading a .zip file.

Prompts that you upload must conform to these guidelines:

- Encoding—CCITT u-law
- Bits per sample—8
- Sample rate—8 kHz
- Channels—1 (monaural)

To upload a spoken names prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

Step 2 If you want to upload a .zip file that contains one or more prompt .wav files to the repository, click **Upload Zip**, and then go to Step 3.

If you want to upload a single .wav file, take these actions:

a. From the Resource Type drop-down list, choose the type of resource for which this prompt is to be associated (channel, channel groups location, ops view, policy, user, user group, or VTG).

b. Click **Search** and, in the Search Results window, locate and choose the resource or resources for which this prompt is to be associated.

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

c. From the Associated Resource drop-down list, choose a resource for which this prompt is to be associated.

   This list shows the items that you chose in the Search Results window.

Step 3 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 4 From the Language drop-down list, choose the logical language folder in which to store the prompt or prompts.

Step 5 If you are uploading a .zip file, take the following actions to associate the prompts in that file with the appropriate Cisco IPICS resources.

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

a. Click **Associate**.

   The Prompt Association window displays.

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

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

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

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

d. Click **Associate**.

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

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

e. Repeat Step 5 b, c, and d as needed to associate other prompts in the .zip file with resources.

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

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

Step 6 If you are uploading a single file, click **Save** to upload the prompt.

If you do not want to upload the prompt, click **Cancel**.

Downloading a Spoken Names Prompt

Downloading a spoken names prompt copies the .wav file for the prompt to a location that you specify. You can listen to the prompt by using any media player that plays .wav files.

To download a spoken names prompt, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

The Spoken Names window displays.

Step 2 Check the check box next to the prompt that you want to download.

Step 3 Click **Download** at the bottom of the Spoken Names window.

Step 4 Follow the on-screen prompts to download the prompt.

If your browser has a default media player configured, the prompt plays automatically.

Otherwise, follow the on-screen prompts to download prompt. After you download the prompt, you can use a media player to listen to it.

Recording a Spoken Name Prompt

You can use either of the following methods to record a spoken names prompts:

- Recording a Spoken Names Prompt Using the Dial Engine, page 8-25
- Recording a Spoken Names Prompt Using the Windows Sound Recorder, page 8-27

You can also record a spoken names prompt by calling the TUI and following the prompts to record the name. For more information, see the "Using the Policy Engine Telephony User Interface" section on page 7-27.

Recording a Spoken Names Prompt Using the Dial Engine

When you record a spoken names prompt using the dial engine, you instruct the dial engine to call you at a telephone number that you specify. When you answer the call, the TUI guides you through recording the prompt. Then the policy engine automatically uploads the prompt to the repository.

To record or rerecord a spoken names prompt by using the dial engine, perform the following procedure. If you use this procedure to rerecord an existing spoken names prompt, the system creates a new .wav file for the prompt.

Note If you want to replace the .wav file for an existing prompt with a new .wav file, perform Step 1 through Step 5 in the following procedure. Then click the link for the prompt. In the Prompt Information window, click the **Browse** button to enter, the path and file name of the file to upload. and then click **Save**.

Procedure

Step 1 Take one of these actions to display the Spoken Names window:

- In the **Policy Engine** tab, choose **Dial Engine** > **Prompt Management** > **Spoken Names**.
- From the management window for a Cisco IPICS resource, click the **Recorded** or the **Not Recorded** link in the Prompt column.

  If you take this action, Cisco IPICS automatically fills in the Resource Type, Associated Resource, and Language fields with the information needed to record the prompt for the resource. You can change this information as described in the next four steps, if needed. If the information is correct, go to Step 6.

Step 2 From the Resource Type drop-down list, choose the type of resource for which this prompt is to be recorded (channel, channel groups location, ops view, policy, user, user group, or VTG).

Step 3 Click **Search** and, in the Search Results window, locate and choose the resource or resources for which this prompt is to be recorded.

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

Step 4 From the Associated Resource drop-down list, choose a resource for which this prompt is to be recorded.

This list shows the items that you chose in the Search Results window.

Step 5 If you want re-record an existing prompt, take these actions to locate existing prompts for this resource:

a. From the Language drop-down list, choose the logical language folder in which existing prompts are stored.

Choose **All** if you want to display prompts from all language folders.

Choose **Default** if you want to display prompts from the default language folder.

b. Click **Query**.

Step 6 Take one of these actions:

- To record a spoken names prompt for the first time, click **Record**.
- If you want to re-record an existing prompt, check the check box for the prompt in the list of prompts and then click **Rerecord**.

Step 7 From the Language drop-down list, choose the logical language folder in which to store the .wav file for the prompt.

Choose **default** if you want this prompt to be available to any script, regardless of the language that is designated for the script.

Step 8 In the Phone Number field, enter a telephone number where the system should call you.

You can include parentheses, spaces, and dashes in the telephone number.

The SIP provider must be able to route the call to the number that you enter.

Step 9 Click **Call**.

The dial engine calls the telephone number that you specified.

Step 10 Answer the telephone and follow the verbal prompts to log in to the TUI and record the prompt.

Recording a Spoken Names Prompt Using the Windows Sound Recorder

You can record a spoken names prompt by using the Microsoft Windows Sound recorder. To do so, perform the following procedure. (The procedure shown is for systems that are running the Microsoft Windows XP operating system.)

Procedure

Step 1 From the Windows Start menu, choose **Start > Programs > Accessories > Entertainment > Sound Recorder**.

The Sound Recorder dialog box displays.

Step 2 Click the **Record** button and speak the name that you want to record into the microphone.

Step 3 Click the **Stop** button when you finish recording.

Step 4 Check your recording by clicking the **Rewind** button or by dragging the slider to the beginning of the recording, and then clicking the **Play** button.

Step 5 When you are satisfied with the recording, choose **File > Save As**.

The Save As window opens.

Step 6 Click **Change** to set the recording options.

You can also set recording properties by choosing **Properties** from the Sound Recorder File menu.

The Sound Selection dialog box displays.

Step 7 From the Format drop-down menu, choose **CCITT u-Law**.

Step 8 From the Attributes drop-down menu, choose 8.000 kHz, 8 Bit, Mono 7 kb/sec.

Step 9 Click **Save As.**

The Save As dialog box displays.

Step 10 Enter a name for this format, and then click **OK**.

Step 11 In the Sound Selection dialog box, click **OK**.

Step 12 In the Save As window, save the recording file in the directory of your choice, and then click **Save**.

To use this prompt with the policy engine, you must upload it as described in the "Uploading Spoken Names Prompts" section on page 8-22.

Changing Information about a Spoken Names Prompt

You can change the name, language, resource type, and associated resource of a prompt. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

The Spoken Names window displays.

Step 2 Locate the desired prompt by making choices from the Language, Resource Type, and Associated Resource drop-down lists, and clicking **Query**.

For description of the drop-down lists, see the "Viewing a List of Spoken Names Prompts" section on page 8-21.

Step 3 Click the link in the Prompt column for the desired prompt.

Step 4 Click the **Browse** button to enter, in the Name field, the path and file name of the file to upload.

This entry is required.

Step 5 From the Language drop-down list, choose the logical language folder in which to store the prompt.

Step 6 From the Resource Type drop-down list, choose the Cisco IPICS resource type for which the prompt is recorded (channel, channel group, location, policy, user, user group, ops view, or VTG).

Step 7 From the Associated Resource drop-down list, choose the name of the channel, channel group, location, policy, user, user group, ops view, or VTG for which the prompt is recorded.

Step 8 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Deleting a Spoken Names Prompt

When you delete a spoken names prompt, it is removed from the repository. You can delete a single prompt or you can delete several prompts at one time.

To delete a spoken names prompt or prompts, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Prompt Management > Spoken Names**.

The Spoken Names window displays.

Step 2 Check the check box next to each prompt that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this prompt, click **Cancel**.

Managing Dial Engine Scripts

The policy engine executes scripts that enable the TUI to communicate with users. Scripts provide instructions that the TUI follows to play prompts and perform other operations. A script plays prompts in the language that you designate for the script.

The dial engine includes the following system scripts, which cannot be modified or deleted. You can add other scripts.

- IppeDialin—TUI main menu
- IppeDialout—Used to place outbound calls
- IppeRecording—Used to record spoken names

Cisco IPICS stores scripts in the *repository*, which is a logical storage medium in which scripts are contained and organized.

Managing dial engine scripts involves these activities:

- Viewing a List of Dial Engine Scripts, page 8-31
- Adding a Dial Engine Script, page 8-31
- Viewing or Changing Information about a Custom Dial Engine Script, page 8-32
- Deleting a Custom Dial Engine Script, page 8-33

Viewing a List of Dial Engine Scripts

The dial engine Scripts window displays a list of dial engine scripts. For each script, this window shows the following information:

- Name—Name of the script
- Script—Filename of the script and its location in the logical file structure
- App Type—Type of application:
  - DIAL_IN—Script is invoked when a user calls the TUI
  - DIAL_OUT—Script is invoked when the system dials out to a user
- Trigger—Mechanism that invokes a script:
  - For DIAL-IN app type—Dial-in telephone number configured for this dial engine script
  - For DIAL-OUT app type—Not applicable

To display the Dial Engine Scripts window, choose **Dial Engine** > **Dial Engine Script Management** from the **Policy Engine** tab.

Adding a Dial Engine Script

When you add a dial engine script, you make it available for use by the policy engine. For additional information about adding a dial engine script, contact your system integrator.

To add a dial engine script, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Script Management**.

The Dial Engine Scripts window displays.

Step 2 Click **Add** at the bottom of the list of scripts.

Step 3 In the Dial Engine Script Name field, enter a name for this script.

This entry is required.

Step 4 In the Script field, enter a name for the script.

Step 5 (Optional) Use the **Browse** button to enter, in the Destination Folder field, the path and file name of the file to upload.

Destination folders let you group or organize scripts. For example, if you have two scripts with the same name, put each one in a separate destination folder.

This entry is required.

Step 6 From the Trigger Type drop-down list, choose one of these options:

- Dial In—Script is invoked by a call to the TUI
- Dial Out—Script is invoked by a call from the TUI

You must choose one of these options.

Step 7 For a Dial In trigger type, in the DN field, enter the telephony access string that is dialed to invoke the script.

This entry is required for a Dial In trigger type. This string must be configured on the SIP provider so that the SIP provider can route the directory number (DN) to the policy engine. This field can contain numbers and letters.

This field does not display if the trigger type is Dial Out.

Step 8 From the Language drop-down list, choose the logical language folder that contains the prompts to be played by this script.

Step 9 To add the script, click **Add**.

If you do not want to add this script, click **Cancel**.

Viewing or Changing Information about a Custom Dial Engine Script

You can view or modify information for any custom dial engine script. You cannot view or modify information for any of the five system scripts that are listed in the "Managing Dial Engine Scripts" section on page 8-30.

To view or modify information about a custom dial engine script, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Script Management**.

The Dial Engine Scripts window displays.

Step 2 Click the link in the Name column for the custom script.

System scripts do not have a link.

Step 3 View or update the following information as needed:

- Dial Engine Script Name—Name assigned to this script
- Current Script (*display only*)—Script that is currently for the DN
- Script—Script file that executes
- Destination Folder— Logical folder under the language folder in which the script is stored
- Trigger Type—Either of these options:
  - Dial In—Script is invoked by a call to the TUI
  - Dial Out—Script is invoked by a call from the TUI
- Language— Logical language folder in which the script is stored

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

If you do not want to save your changes, click **Cancel**.

Deleting a Custom Dial Engine Script

When you delete a dial engine script, it is removed from the repository. You can delete any custom script, but you cannot delete the system scripts that are listed in the "Managing Dial Engine Scripts" section on page 8-30.

You can delete a single script or you can delete several scripts at one time.

To delete a custom script or scripts, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Script Management**.

The Dial Engine Scripts window displays.

Step 2 Check the check box next to each custom script that you want to delete.

These check boxes are dimmed for the system scripts.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this script, click **Cancel**.

Configuring SIP

The SIP configuration process provides the policy engine with the parameters that it needs to work with the SIP provider.

For related information, see the "Configuring the SIP Provider" section on page 8-41.

To configure SIP for the Policy Engine, perform the following steps:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **SIP Configuration**.

The SIP Configuration window displays.

Step 2 In the SIP Subsystems Configuration pane, take these actions to enter required information:

- In the Port field, enter the SIP port that the policy engine uses.

  The default value is 5060.

- In the User Agent field, enter the user agent that the policy engine uses.

  The default value is Cisco-IPPE/2.0.

- In the Maximum Retransmissions field, enter the maximum number of times that SIP requests and responses are transmitted.

  The default value is 2. Valid values are 0 through 10.

- In the First Retransmission field, enter the number of milliseconds to wait before performing the first retransmission.

  The default value is 500. Valid values are 100 through 4000.

Note The default maximum transmissions and first retransmission values are appropriate in most cases. You should not change these values unless you fully understand the characteristics of the network on which Cisco IPICS and the SIP provider are deployed and understand the SIP retransmission algorithms that are described in the RFC 3261 specification.

Step 3 In the SIP Provider Configuration pane, take these actions:

- In the Host field, enter the IP address or the host name of the SIP provider. This entry is required.
- In the Port field, enter the port number that the SIP provider uses for SIP. This entry is required.
- From the Transport drop-down list, choose the transport protocol (TCP or UDP) that matches the transport protocol of the SIP provider.

  If both protocols are configured on the SIP provider, choose either protocol.

- In the Username field, enter the appropriate information. This information is required.
  - If Cisco Unified CallManager is the SIP provider, enter the Cisco Unified CallManager user name for the SIP trunk.
  - If a Cisco router that is running a supported version of Cisco IOS is the SIP provider, enter any value in this field.
- In the Password field, enter the appropriate information. This information is required.
  - If Cisco Unified CallManager is the SIP provider, enter the Cisco Unified CallManager password for the SIP trunk.

- If a Cisco router that is running a supported version of Cisco IOS is the SIP provider, enter any value in this field.

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

If you do not want to save your changes, click **Cancel**.

Step 5 To cause your changes to take effect, follow these steps to restart the dial engine:

a. Log in to the Cisco IPICS server as the root user.

b. Enter the following command at the command prompt:

```
[root]# service ipics restart
```

Configuring Dial Engine Parameters

The dial engine parameters configuration process provides system settings for the dial engine.

To configure dial engine parameters, perform the following steps:.

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Dial Engine Parameters**.

The Dial Engine Parameters window appears.

Step 2 In the SMTP Server field, enter the IP address or the host name of the SMTP server that is used by the dial engine.

Leave this field blank if there is no SMTP server configured for the dial engine.

Step 3 In the Sender Email Address field, enter the e-mail address that appears as the "From" address when the policy engine sends e-mail notifications to users.

If you specify a sender e-mail address when configuring an ops view, that value overrides the value in this field.

Step 4 In the Outbound Dial Number field, enter the telephone number that appears as the caller ID number when the policy engine calls a user.

This number must not be the same as a dial-in number that is used to call the policy engine.

If this number is not configured, the policy engine is not able to dial out.

Note If the policy engine call goes through more than one voice gateway, the caller ID of the last gateway appears as the caller ID, regardless of the value that is configured in the Outbound Dial Number field.

Step 5 From the Default Language drop-down list, choose the logical language folder that the TUI uses at run time.

Step 6 In the Default Session Timeout field, enter the number of seconds that a call session is kept in memory after the call completes.

The default value is 500. You should change this value only if you are instructed to do so by the Cisco TAC.

Step 7 Click **Save** to save your changes.

If you do not want to save your changes, click **Cancel**.

Note The Dial Engine Parameters window displays the codec that the policy engine uses. This codec is G.711 u-law and cannot be changed.

Managing the Direct Dial Feature

The direct dial feature allows a PMC user to use the PMC push-to-talk (PTT) features to speak directly with a telephone user. A direct dial call is a SIP call that originates from a PMC and flows through the RMS to the SIP provider. The telephone can be any one that can be reached by the SIP provider.

For information about configuring the RMS and the SIP provider, see Appendix A, "Configuring the Cisco IPICS RMS Component" and see the "Configuring the SIP Provider" section on page 8-41.

Note

- Before a telephone can be called by a PMC by using the direct dial feature, the phone must have its destination number configured and it must be assigned a label. For instructions, see the "Designating a Dial Prefix for Direct Dial Numbers" section on page 8-39 and the "Adding a Direct Dial Number" section on page 8-39.
- A phone must be associated with a user before the user can access that phone from a PMC. To associate phones with users, see the "Managing Your User Profile" section on page 5-2 or the "Associating Phones with a User to Configure the Direct Dial Feature" section on page 3-31.

For information about using direct dial on a PMC, refer to *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Managing the direct dial feature involves these activities:

- Viewing a List of Direct Dial Numbers, page 8-38
- Designating a Dial Prefix for Direct Dial Numbers, page 8-39
- Adding a Direct Dial Number, page 8-39
- Viewing or Changing Information about a Direct Dial Number, page 8-40
- Deleting a Direct Dial Number, page 8-41

Viewing a List of Direct Dial Numbers

The Direct Dial Management window provides you with the ability to designate global dial settings, which is a number that is prepended to a direct dial number. This window also displays a list of direct dial numbers that have been configured. For each number, this window shows the following information:

- Label—Description of the number that displays on a PMC
- Dial Destination—Telephone number that the SIP provider dials

To display the Direct Dial Management window, choose **Dial Engine > Direct Dial Management** from the **Policy Engine** tab.

Designating a Dial Prefix for Direct Dial Numbers

A dial prefix is an optional digit string that the server prepends to each direct dial number when it dials the number. Using a dial prefix can help avoid dial plan conflicts. The string should match the value that is configured in the SIP provider as the destination pattern in the RMS dial peer trunk. For example, if the dial prefix string is 9 and the direct dial number is 1234, the number 91234 is dialed. (For related information, see the "Configuring the SIP Provider" section on page 8-41.)

To designate a dial prefix, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Direct Dial Management**.

The Direct Dial Management window displays.

Step 2 In the Dial Prefix field, enter the dial prefix string.

Step 3 Click **Save** under the Global Settings area.

Adding a Direct Dial Number

When you add a direct dial number, that number becomes available to associate with users.

To add a direct dial number, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Direct Dial Management**.

The Direct Dial Management window displays.

Step 2 Click **Add** at the bottom of the list of direct dial numbers.

Step 3 In the Label field, enter a description for this direct dial number.

The label can contain up to 15 characters. It appears on a PMC as a label for this number.

This entry is required.

Step 4 In the Dial Destination field, enter the telephone number that the SIP provider dials.

You can include parentheses, spaces, and dashes in the telephone number.

Make sure to include an initial access number (such as 8 or 9), if required by your SIP provider.

This entry is required.

Step 5 Click **Save** to add the direct dial number.

If you do not want to add the number, click **Cancel**.

Viewing or Changing Information about a Direct Dial Number

You can view or update information about any direct dial number. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > Direct Dial Management**.

The Direct Dial Management window displays.

Step 2 Click the link in the Label column for the number.

Step 3 View or update the following information as needed:

- Label—Label of this number, which displays on a PMC
- Dial Destination—Telephone number that the SIP provider dials

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

If you do not want to save your changes, click **Cancel**.

Deleting a Direct Dial Number

When you delete a direct dial number, it is no longer available in the system or to PMC users.

You can delete a single number or you can delete several numbers at one time.

To delete a direct dial number or numbers, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine** > **Direct Dial Management**.

The Direct Dial Management window displays.

Step 2 Check the check box next to each number that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete this number, click **Cancel**.

Configuring the SIP Provider

The policy engine requires that a SIP provider be configured in your network if you use the dial-in, dial-out, or PMC direct dial features. A SIP provider handles calls to and from the policy engine.

You must use Cisco Unified CallManager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider, enter any value in this field as the SIP provider. To do so, configure the application as described in the following sections. These sections assume that Cisco Unified CallManager or the router is installed and running in your network.

- Configuring Cisco Unified CallManager as the SIP Provider, page 8-42
- Configuring a Cisco Router as the SIP Provider, page 8-46

Configuring Cisco Unified CallManager as the SIP Provider

Assuming that Cisco Unified CallManager is configured and running in your network, this section describes additional configuration that is required for Cisco Unified CallManager to function as the SIP provider for the policy engine.

Before you configure Cisco Unified CallManager for the policy engine, you must provide SIP configuration information as described in the "Configuring SIP" section on page 8-34.

When you perform the procedure in this section, you must provide the information that is listed Table 8-2. You may find it convenient to gather this information before you start the procedure.

Table 8-2 Information Required for Cisco Unified CallManager Configuration

Information	Your Value
User ID that you entered when you configured SIP as described in the "Configuring SIP" section on page 8-34	
Password that you entered when you configured SIP as described in the "Configuring SIP" section on page 8-34	
Incoming port, if other than the default 5060	
Partitions, if configured for Cisco Unified IP Phones	
Calling search spaces, if configured for Cisco Unified IP Phones	
IP address of the Cisco IPICS server	
DNs for ops views and custom dial engine scripts	

Table 8-2 Information Required for Cisco Unified CallManager Configuration (continued)

Information	Your Value
User name that you entered when you configured the RMS (required only if you are using the direct dial feature)	
Password that you entered when you configured the RMS (required only if you are using the direct dial feature)	

To configure Cisco Unified CallManager for the policy engine, perform the following procedure.

Procedure

Step 1 In Cisco Unified CallManager Administration, take the following actions to configure an Application User for the policy engine.

This Application User requires digest credentials and will be used by the policy engine to authenticate calls that it makes to Cisco Unified CallManager.

a. Choose **User Management > Application User**.

b. Click **Add New**.

c. In the Application User Configuration Page, enter the following information:

- User ID—Enter the same user ID that you entered when you configured SIP.
- Password and Confirm Password—Enter a password that the user will use to log into Cisco Unified CallManager.
- Digest Credentials and Confirm Digest Credentials—Enter the password that you entered when you configured SIP.
- Update other fields as needed for your deployment or accept the default values.

d. Click **Save**.

Step 2 In Cisco Unified CallManager Administration, take the following actions to define a SIP trunk security profile with digest authentication enabled.

The default SIP trunk does not provide security. This new profile enables digest authentication for calls from the policy engine to Cisco Unified CallManager.

a. Choose **System > Security Profile > SIP Trunk Security Profile**.
b. Click **Add New**.
c. In the Name field, enter **Digest Authenticated SIP Trunk Profile**.
d. In the Description field, enter **Digest Authenticated SIP Trunk Profile**.
e. From the Device Security Mode drop-down list, choose **Non Secure**.
f. From the Incoming Transport drop-down list, choose **TCP+UDP**.
g. From the Outgoing Transport drop-down list, choose **TCP**.
h. Check the **Enable Digest Authentication** check box.
i. In the Nonce Validity Time field, enter **5**.
j. In the **Incoming Port** field, enter the default value of 5060 or enter another value if appropriate for your deployment.
k. Click **Save**.

Step 3 In Cisco Unified CallManager Administration, take the following actions to create a SIP trunk for the policy engine.

The SIP trunk is used to exchange dial-in and dial-out calls between Cisco Unified CallManager and the policy engine.

a. Choose **Device > Trunk**.
b. Click **Add New**.
c. From the Trunk Type drop-down list, choose **SIP Trunk**.
d. From the Device Protocol drop-down list, choose **SIP**.
e. Click **Next**.
f. Enter information that is appropriate for your Cisco Unified CallManager deployment, making sure to follow these guidelines:
   - If you configured partitions and calling search spaces for your Cisco Unified IP Phones, enter the same calling search spaces for the policy engine.
   - In the Destination Address field, enter the IP address of the Cisco IPICS server.

- In the SIP Trunk Security Profile field, enter the name of the profile that you created in Step 2.

g. Click **Save**.

Step 4 In Cisco Unified CallManager Administration, take the following actions to create a route pattern for the new SIP trunk.

The route pattern that is associated with the SIP trunk instructs Cisco Unified CallManager which calls to send to the policy engine.

a. Choose **Call Routing > Route/Hunt > Route Pattern**.

b. Click **Add New**.

c. Enter information that is appropriate for your Cisco Unified CallManager deployment.

In the Route Pattern field, make sure to include in the route pattern all DNs that you want to be routed to the policy engine (DNs for ops views and custom dial engine scripts).

d. From the Gateway/Route List drop-down list, choose the SIP trunk that you created in Step 3.

e. Click **Save**.

Step 5 (Optional—required only if you are using the direct dial feature) In Cisco Unified CallManager Administration, take the following actions to configure and Application User for the RMS:

a. Choose user **Management > Application User**.

b. Click **Add New**.

c. In the Application User Configuration page, enter the following information:

- User ID—Enter the same user ID that you entered when you configured the RMS.
- Password and Confirm Password—Enter the same password that you entered when you configured the RMS
- Other fields—Enter information as appropriate for your deployment.

d. Click **Save**.

Step 6 (Optional—required only if you are using the direct dial feature) In Cisco Unified CallManager Administration, take the following actions to create a SIP trunk for the RMS:

a. Choose user **Device > Trunk**.

b. Click **Add New**.

c. From the Trunk Type drop-down list, choose **SIP Trunk**.

d. From the Device Protocol drop-down list, choose **SIP**.

e. Click **Next**.

f. Enter information that is appropriate for your Cisco Unified CallManager deployment, making sure to follow these guidelines:

- If you configured partitions and calling search spaces for Cisco Unified IP Phones, enter those calling search spaces.
- In the Destination Address field, enter the IP address of the RMS.
- In the SIP Trunk Security Profile field, enter the name of the profile that you created in Step 2.

g. Click **Save**.

Configuring a Cisco Router as the SIP Provider

Assuming a Cisco router that is running a supported version of Cisco IOS is configured and running in your network, this section describes additional configuration required for configuring the router as the SIP provider for direct dial calls from a PMC.

Note Although Cisco IOS supports values other than those shown for some of the fields in this configuration, Cisco recommends that you configure the values that are shown to ensure consistency.

Procedure

Step 1 Enter the following command to start configuration mode:

```
Router# configure terminal
```

Step 2 If the router has other SIP devices configured, such as Cisco Unified CallManager Express with SIP phones, enter the following commands to allow SIP to SIP connections.

If no other SIP devices are configured, skip this step.

```
Router(config)# voice service voip
Router(con-voi-serv)# allow-connections sip to sip
Router(con-voi-serv)# exit
```

Step 3 Enter the following commands to define a voice class codec that uses the G.711 u-law codec.

```
Router(config)# voice class codec 2
Router(config-class)# codec preference 1 g711ulaw
Router(config-class)# exit
```

Step 4 Enter the following commands to define a dial-peer for each route pattern that you allocated for ops views.

Route patterns must span the DNs that are associated with each ops view and custom script. For example, if your system has ops views with the DNs 8100–8199 and 9200–9299, you could define two route patterns, 81*nn* and 92*nn*, where *n* is any digit. You would then define one dial peer for each route pattern.

```
Router(config)# dial-peer voice 554 voip
Router(config-dial-peer)# destination-pattern route-pattern
Router(config-dial-peer)# voice-class codec 2
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# session target ipv4:ip-address
```

(replace *ip-address* with the IP address of the Cisco IPICS server)

```
Router(config-dial-peer)# session transport transport-protocol
```

(replace *transport-protocol* with UDP or TCP, depending on which value is configured for SIP as described in the "Configuring SIP" section on page 8-34)

```
Router(config-dial-peer)# dtmf-relay rtp-nte
```

```
Router(config-dial-peer)# exit
```

Step 5 (Optional—skip this step if the SIP provider and RMS are configured on the same router) Enter the following commands to configure the incoming voice dial peer to turn off voice activity detection (VAD) and use RFC 2833 for DTMF for calls from IPICS):

```
Router(config)# dial-peer voice 555 voip
Router(config-dial-peer)# voice-class codec 2
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# incoming called number .
Router(config-dial-peer)# no vad
Router(config-dial-peer)# dtmf-relay rtp-nte
```

Step 6 Enter this command:

```
Router(config)# end
```

Performing Cisco IPICS Database Backup and Restore Operations

This chapter describes the procedures that you perform to back up your Cisco IPICS database and to restore your database from the backup location.

This chapter includes the following sections:

- Overview of Cisco IPICS Database Backup and Restore Operations, page 9-1
- Backing up the Cisco IPICS Server Database, page 9-2
- Restoring Data from a Database Backup, page 9-12
- Downloading and Viewing the Backup and Restore Logs, page 9-19
- Using CLI to Export and Import the Cisco IPICS Databases, page 9-21
- Troubleshooting Cisco IPICS Backup and Restore Procedures, page 9-30

Overview of Cisco IPICS Database Backup and Restore Operations

As a best practice, Cisco recommends that you back up your Cisco IPICS database on a regular basis and maintain your backups in a secure location. This best practice ensures that you do not lose all system configuration if your Cisco IPICS server experiences a software or hardware failure.

Cisco IPICS performs regularly-scheduled database backups to preserve your data. For more information about scheduled database backups, including the default settings for the scheduled database backups and how to modify them, see the "Changing the Default Settings for a Scheduled Database Backup" section on page 9-9.

You can also perform a database backup at any time by manually executing the backup operation. For more information about manual backup procedures, see the "Restoring Data from a Database Backup" section on page 9-12.

After you have backed up your data, you can restore your data by choosing from various options. By accessing the **Administration > Database Management** window, you can identify the backup that you want to restore. For more information regarding restore operations, see the "Restoring Data from a Database Backup" section on page 9-12.

Backing up the Cisco IPICS Server Database

Cisco IPICS provides you with the following options to back up your database:

- Manual backups—You can perform a manual database backup to capture the current state of the Cisco IPICS database.
- Scheduled backups—By default, Cisco IPICS backs up the database every day at a predefined time and stores the backup in a predefined location. You can change the time, frequency, and/or location of the scheduled backup.

This section includes information about backing up the database and includes the following topics:

- Managing Database Backups from the Database Management Window, page 9-3
- Performing a Manual Database Backup, page 9-3
- Restoring Data from a Database Backup, page 9-12
- Changing the Default Settings for a Scheduled Database Backup, page 9-9
- Choosing a Destination for the Database Backup, page 9-11
- Caveats for Remote Host Database Backups, page 9-11

Managing Database Backups from the Database Management Window

To configure the parameters for backing up your database, and performing backup-related operations, navigate to the **Administration > Database** Management window.

The Database Management window includes the following tabs:

- Database Backup—From this tab, you can configure the options to back up your database. See the "Performing a Manual Database Backup" section on page 9-3 for more information about the Database Backup tab.
- Restore From Backup—From this tab, you can restore your database backup. See the "Restoring Data from a Database Backup" section on page 9-12 for more information about restoring your database backup.
- Schedule Backup—From this tab, you can configure the options that apply to regularly-scheduled backups. You can specify the location of the backup and the length of time for which the backup is saved. In addition, you can specify when, and how often, Cisco IPICS performs the scheduled backups.

  See the "Changing the Default Settings for a Scheduled Database Backup" section on page 9-9 for more information about changing the settings for the scheduled database backups.
- Log—From this tab, you can view the database logs, which include backup and restore activity. The logs include status messages and information about any errors that might have occurred during a database backup or restore procedure. See the "Downloading and Viewing the Backup and Restore Logs" section on page 9-19 for more information about the database logs.

Performing a Manual Database Backup

To perform a manual database backup, navigate to the **Administration > Database Management > Database Backup** window.

The settings that you choose for a manual database backup, such as the location of the backup, can be different from the destination that you choose for the scheduled backups. (Settings for manual database backups do not affect or change the settings for scheduled database backups.)

To manually back up the database, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Database Backup** window.

Step 2 In the **Backup Destination** pane, choose one of the following destinations:

- **Default**—Click this radio button to place the backup in the default (**/idspri/backup**) directory.

  Cisco IPICS creates a subdirectory in the /idspri/backup directory for the database backup named **IDSB**_*yyyy-mm-dd_hh-mm-ss*. See the "Understanding Naming Conventions for Backup Directories" section on page 9-8 for more information about backup directory naming conventions.

- **Local Directory**—Click this radio button to specify a directory in the Cisco IPICS server to back up your database.

Note Cisco IPICS prepopulates the Local Directory field with the **/idspri/backup** directory. If you back up your files to a local directory in the server, that directory must be a subdirectory of the **/idspri/backup** directory. Any directory within the **/idspri/backup** directory (for example, **/idspri/backup/mybackups**) is valid as a location for a database backup. If the directory that you specify does not exist, Cisco IPICS creates the directory for you.

Make sure that you enter the path within the **/idspri/backup** directory in the Cisco IPICS server, and that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays a pop-up window with an error and does not perform the backup.

- **Remote Host**—Click this radio button to back up your database to a remote location.

Note Use the Remote Host option only if the remote host supports the Linux Secure Copy (scp) command. If you are using a remote host that does not support scp (for example, a Windows PC or server), click the **Local Directory** radio button. You must back up your data to the Cisco IPICS server, then use a secure file transfer protocol (SFTP) client software program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. For more information, see the procedure in the "Backing Up Data to a Remote Host Without scp Support" section on page 9-31 to back up your files to a remote host that does not support scp.

When you click the Remote Host radio button, you must specify the following information:

- Remote Host IP Address—Enter the IP address of the remote host.
- User Name—Enter a valid user name for access to the remote host.
- User Password—Enter a valid password for this user.
- Remote Directory—Enter the location of the full directory path on the remote host where you want the database to be stored. If the directory that you specify for the backup does not exist on the remote host, Cisco IPICS creates it for you.

  For more information, see the "Caveats for Remote Host Database Backups" section on page 9-11.

Step 3 Click **Backup Now**.

Cisco IPICS begins the database backup process. An information icon appears in the tab to inform you that the backup is in process, along with the following text:

```
Database backup in progress. Please wait...
```

Step 4 To view the activity for the backup, wait a few moments for the screen to refresh and view the Backup Log pane.

The Backup Log pane in the Database Backup tab displays the log entries for the backup process. The screen refreshes periodically with log messages until the database backup completes.

Note To manually refresh the screen, click **Refresh**.

Step 5 To view the results of the backup operation, wait until the screen stops refreshing, then view the Backup Log pane.

Note The backup log pane can contain multiple pages of items. To view items in the list, use the navigation buttons as described in the "Navigating Item Lists" section on page 1-15.

If the backup operation was successful, you see a Status Text of **Available**.

Table 9-1 describes the fields in the Backup Log pane.

Table 9-1 Field Descriptions in the Backup Log Pane

Field	Description
ID	This field represents the internal ID of the database backup. Cisco IPICS gives each backup operation a unique ID.
Backup Destination	This field represents the full directory path of the database backup, beginning with a forward slash (/). If the backup was a Remote Host backup, this field displays the full directory path on the remote server on which Cisco IPICS placed the Remote Host backup. **Note** Cisco IPICS creates a subdirectory inside the directory that you specify for each backup operation. Each directory is time-stamped with the date and time of the backup, as described in the "Restoring Data from a Database Backup" section on page 9-12.
IP Address	This field represents the IP address of the remote server, if the backup was a Remote Host backup. If Cisco IPICS performed a Default or Local Directory backup, this field is blank. If the backup operation was not successful, this field displays **none**.

Table 9-1 Field Descriptions in the Backup Log Pane (continued)

Field	Description
Status	This field represents the status of the backup operation. The status field displays one of the following states: • **Initialized**—The backup process has begun the initial stages of the database backup. • **In Progress**—Cisco IPICS successfully completed the initial stages of the backup process and is performing the database backup. • **Available**—The database backup was successful and the specified backup is available for a restore operation. • **Not Available - Purged**—The specified database backup exceeded the retention period as specified by the **Backup Retention** list box and Cisco IPICS deleted the database backup. The date and time that the database was purged is displayed in the field. • **Canceled**—Cisco IPICS canceled the backup due to a known error (for example, a lack of hard disk space). • **Failed**—Cisco IPICS could not complete the database backup because of an unexpected error. If you see a **Canceled** or **Failed** error status, your database backup failed. You can find more information about the cause of the failure by navigating to the **Administration > Database Management > Log** window and viewing the contents of the backup log.
Size in Bytes	This field represents the total size, in bytes, of the specified database backup.
Backup Start Time	This field represents the time that Cisco IPICS started the specified database backup.
Backup End Time	This field represents the time that Cisco IPICS completed the specified database backup.
Purge Time	This field represents the time that Cisco IPICS deleted the specified database backup.

You can also view the database logs by navigating to the **Administration > Database Management > Logs** window. To visually identify the type of status message that appears in the Database Logs pane, Cisco IPICS displays certain log entries in the following text colors:

- Green—Green messages indicate the completion of a script.

Note Carefully check the text of green messages to ensure that the script completed successfully with no errors. Green messages do not indicate whether the script completed successfully.

- Black—Black messages are informational messages, and indicate normal database backup processes.
- Blue—Blue messages are warning-level messages, and indicate problems that are less severe than error-level messages, such as a backup operation that completed with errors. Occasionally a warning-level error message can indicate a greater problem, such as a restore operation that did not complete successfully.
- Red—Red messages are error-level messages, and indicate that a process did not complete successfully. Red messages usually indicate errors of a greater severity than warning-level (blue) messages.

For more information about troubleshooting problems that you might encounter, see the "Troubleshooting Cisco IPICS Backup and Restore Procedures" section on page 9-30.

Understanding Naming Conventions for Backup Directories

Cisco IPICS creates a subdirectory in the backup directory for each database backup. Cisco IPICS time-stamps each subdirectory with the date and time that Cisco IPICS performed the backup operation. The subdirectory name is in the following format:

IDSB_*yyyy-mm-dd_hh-mm-ss*

Where *yyyy-mm-dd_hh-mm-ss* represents the year, month, day, hour, minute and second, respectively, of the time that the Cisco IPICS performed the database backup (for example, IDSB_2006-09-04_17-13-55).

Changing the Default Settings for a Scheduled Database Backup

Cisco IPICS is preconfigured with default settings for database backups. Table 9-2 shows the default settings for scheduled database backups:

Table 9-2 Default Settings for Scheduled Database Backups

Setting	Value
Frequency	Daily
Time of day	23:59 (11:59 p.m.)
Destination directory	The Cisco IPICS server **/idspri/backup** directory. This directory displays as part of the Local Directory option.
Backup retention	8 days

You can modify any of the default settings that are displayed in Table 9-2. Your changes become effective only after you click Save and they become the default settings.

To modify the automated settings for a database backup, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Schedule Backup** window to access the Schedule Backup tab.

Step 2 In the **Schedule Destination** pane, choose from one of the following destinations for your database backup:

- **Default**—Click this radio button to place the database backup in the **/idspri/backup** directory.
- **Local Directory**—Click this radio button to specify a subdirectory of the **/idspri/backup** directory on the local server to back up your database. If you backup your files to a local directory on the server, that directory must be a subdirectory of the **/idspri/backup** directory. If the directory does not exist, Cisco IPICS creates the directory for you.

Note Make sure that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays an error message in the **Administration > Database Management > Log** window and does not perform the database backup.

- **Remote Host**—Click this radio button to back up your database to a remote location. When you choose this option, you must specify the following information:
  - Remote Host IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user name for access to the remote host.
  - User Password—Enter a valid password for this user.
  - Remote Directory—Enter the location of the full directory path on the remote host where you want the database to be stored.

See the "Choosing a Destination for the Database Backup" section on page 9-11 for more information about choosing a destination, user name, and password for your backup.

Step 3 To change the retention settings for the database backup, click the **Backup Retention** drop-down list box to choose the number of days that you want the database to be stored.

Cisco IPICS deletes any backup files that are older than the backup retention setting whenever it performs a scheduled or manual backup.

Note Cisco IPICS does not purge Remote Host backups.

Step 4 In the **Schedule Time** pane, view the default time and day values for the scheduled backup and, if required, modify the values by performing the following steps:

a. Modify the time of day for the scheduled backup to begin by clicking the **Start Time** drop-down list boxes and choose the appropriate values.

b. Under **Repeat Every**, modify the frequency of the scheduled backups by clicking the radio button that corresponds to one of the following options:
   - **Day**—This option schedules a daily backup. Click this radio button to configure daily database backups.

- **Specific Days**—This option activates the check boxes for individual days of the week. Click this radio button and check the appropriate days of the week to perform a database backup on the days of the week that you select.

Step 5 Click **Save** to apply and save your changes.

Caution If you do not click **Save**, your changes are not saved and the server reverts to the current default settings.

To discard your changes and return to the current default settings, click the **Cancel** button.

Choosing a Destination for the Database Backup

When you specify the options for a scheduled database backup, or when you perform a manual backup, you should determine the best place to store the backup. For more information, refer to the "Guidelines for Choosing a Destination for Database Backups" section in the *Release Notes for Cisco IPICS Release 2.0(1)*.

Caveats for Remote Host Database Backups

When you specify the Remote Host option, be aware of the following caveats:

- You must know the IP address of the remote host.
- You must use a valid user name and password on the remote host.
  - The user name for the remote host is not encrypted in the Cisco IPICS server and is stored as clear text. Therefore, Cisco recommends that you create a special user name that has restricted access to the remote host, has scp access, and has write access to only the directory to where you save the database backup.
  - 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.

- The remote host that you specify must be capable of running the scp command. If there are no remote hosts on your network that support scp (for example, a Windows PC or server), use the Local Directory option to back up your data, then use an SFTP client program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. Follow the procedure in the "Backing Up Data to a Remote Host Without scp Support" section on page 9-31 to back up your data to a remote host that does not support scp.
- If the directory that you specify for the backup does not exist on the remote host, Cisco IPICS creates it for you.

Restoring Data from a Database Backup

When you perform a restore operation, you retrieve data from a database backup, and restore the Cisco IPICS database to the state that it was in at the time that Cisco IPICS performed the backup.

You may need to restore your database if you encounter one or more of the following situations:

- You have to reinstall the server software and you need to restore the database to the state that it was in before you reinstalled the software.
- Server data, such as channels, channel groups or VTG templates, were deleted from the database in error and you need to retrieve them.
- You need to copy a database from one Cisco IPICS server to another Cisco IPICS server. You copy the database by performing a database backup from one server, and restoring the database from that backup to another server.

Note You can restore data from one server to another only if both servers are using the same version of Cisco IPICS software. If the software versions of the two servers differ, the database schema might not be the same. In this case, the restore operation fails.

This section contains information about restoring your data and includes the following topics:

- Options for Using the Restore Procedure, page 9-13
- Performing the Restore Procedure, page 9-14
- Checking the Restore Status in the Database Log, page 9-17

Options for Using the Restore Procedure

To configure the restore parameters and perform all restore operations, access the **Administration > Database Management > Restore from Backup** window.

Caution A restore operation logs all users out of the Cisco IPICS database and users cannot log in to Cisco IPICS until the restore operation completes. To minimize any disruption that the restore procedure may cause to users, Cisco recommends that you perform a restore operation during a maintenance window or other off-peak hours.

You can restore your data from the default location, from another local directory that you specify, or from a remote host.

Note Before you restore your database, be aware that any configuration changes that you made to the server after Cisco IPICS performed the database backup are not restored to your server by the restore operation. If you want to ensure that all your recent configuration changes are restored, perform another database backup before you perform the restore operation. For more information, see the "Backing up the Cisco IPICS Server Database" section on page 9-2.

Performing the Restore Procedure

To restore your data, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Restore from Backup** window.

Step 2 In the **Restore Destination** pane, choose from the following options to restore your data:

- **Default**—Click this radio button to restore your data from the default location, which is **/idspri/backup**. If you backed up your database in the default location, choose this option. If there is more than one database backup in the default directory (for example, if you perform regularly scheduled database backups), Cisco IPICS uses the most recent backup for the restore operation.
- **Local Directory (requires full path)**—Click this radio button to restore your data from the local directory that you specify.

  When you specify a local directory or remote host for your restore operation, make sure that you specify the entire directory path. Make sure that you include the following directories in the directory path:

  – The **/idspri/backup** directory. Cisco IPICS places every backup to a local directory in the **/idspri/backup** directory

  – The **IDSB**_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss* directory that Cisco IPICS created when it performed the database backup.

  Note You also specify the Local Directory option if you backed up your data to a remote host that does not support scp. If you backed up your files to a remote host that does not support scp, follow the procedure in the "Restoring Data from a Remote Host Without scp Support" section on page 9-32 to move the backed-up files from the remote host to a local directory. Then, continue with this procedure.

- **Remote Host**—Click this radio button to restore your data from a remote host, in the directory location that you specify.

When you click the Remote Host radio button, you must specify the following information:

- Remote Host IP Address—Enter the IP address of the remote host.
- User Name—Enter a valid user name for access to the remote host.

  Your data is more secure if the same user performs both the backup and restore operations; therefore, the user name to restore the data must be the same user name that you used to back up the database. If you specify a different user name, the restore procedure does not succeed because the user does not have the correct permissions to access the backed-up database.
- User Password—Enter a valid password for this user.
- Remote Directory—Enter the directory path for the remote host from which you want the database to be restored. Enter the full directory path, including the directory that was generated by Cisco IPICS for the database backup, for example **/mybackups/IDSB_2006-08-25_17-13-55**.

Note Be sure to enter the correct user name, password, and remote directory; otherwise, the scp process fails. If the scp process fails, you can determine the cause of the failure by checking the logs in the **Administration > Database Management > Log** window.

Step 3 Click **Restore Now**.

A pop-up window displays to confirm the restore process.

Note If you confirm the restore process, all of the data that has been saved since the last time that your data was backed up, is lost. If you want to cancel the restore process and retain the data that has been saved since the last backup, click **Cancel**.

Step 4 Click **OK**.

Cisco IPICS begins the restore process and logs all users out of the Administration Console.

Note Unlike a database backup operation, you cannot view the log details of the restore operation while it is in progress. The Tomcat service restarts during the restore operation and automatically logs all users out of Cisco IPICS. You must wait for the restore process to complete before you can log in again. You can check the status of the restore process in the **/opt/cisco/ipics/database/logs/db-maintenance.log** file on the Cisco IPICS server. For more information, see the "Checking the Restore Status in the Database Log" section on page 9-17.

Step 5 To see the status of the restore operation, perform one of the following actions:

- To view the status of the restore operation by using CLI commands, see the "Checking the Restore Status in the Database Log" section on page 9-17. The use of CLI commands allows you to see the status of the restore operation before you are able to log back in to the server.
- To view the final status of the restore operation, perform the following procedure:

  a. Wait about 10 to 15 minutes, then log in to the Administration Console by using the ipics user ID.

  If you attempt to log in to the Administration Console before the restore process completes, Cisco IPICS displays the following message:

  ```
  You entered an invalid user name or password.
  Please try again.
  If this problem persists, the database may be unavailable.
  Contact your System Administrator for help.
  ```

  If you receive the preceding message, you can check the progress of the restore operation by opening a terminal window and checking the log as described in the "Checking the Restore Status in the Database Log" section on page 9-17. If you continue to be unable to log in, follow the troubleshooting procedures in the "Unable to Log In To the Administration Console After Restoring Data" section on page 9-34 to attempt to fix the problem.

  b. Navigate to the **Administration > Database Management > Log** window.

  c. Check the Database Logs pane to view the most recent status messages regarding the restore procedure.

Note Click **Refresh** to refresh the log window and view new messages.

Step 6 To view the entire database log file, perform the following procedure:

a. Wait approximately 20 minutes and then log in to the Administration Console.

b. Navigate to the **Administration > Database Management > Log** window.

c. Click **Download**.

d. Perform the actions as listed in Step 3 in the "Downloading and Viewing the Backup and Restore Logs" section on page 9-19 to unzip the .zip file and view or download the db-maintenance.log file.

Checking the Restore Status in the Database Log

Cisco IPICS logs out all users from the Cisco IPICS Administration Console when the restore process begins. You cannot log in to the Administration Console until the process completes. To check the status of the restore procedure before it completes, log in to the Cisco IPICS server and view the contents of the db-maintenance.log file.

The db-maintenance.log file is located in the following directory on the server: **/opt/cisco/ipics/database/logs**. For more information about the db-maintenance.log file, and other log files in Cisco IPICS, see the "Downloading and Viewing the Backup and Restore Logs" section on page 9-19.

To manually access the database log and check the status of the restore operation, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the ipicsadmin user ID.

- From a direct server connection, log in by using the ipicsadmin user ID.
- From a remote secure client, open a terminal window using SSH Secure Shell Client software or similar software. Then, log in by using the ipicsadmin user ID.

A terminal window displays.

Note The ipicsadmin user 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. You can also use the root user ID to perform this procedure.

Step 2 Enter the following command to see the last 25 lines of text in the db-maintenance.log file:

[ipicsadmin]# **tail -25 /opt/cisco/ipics/database/logs/db-maintenance.log**

The last 25 lines of the log file displays. If the log file contains less than 25 lines, the entire file displays.

Step 3 Check the last lines of the db-maintenance.log file to see whether the restore process completed successfully.

Step 4 To check the status of the restore operation, perform one or more of the following actions, depending on the output in the db-maintenance.log file:

- If you see the "Restore process ended without errors" log entry, the restore process completed successfully and no further action is required.
- If you do not see the "Restore process ended without errors" log entry, or if you do not see any other message that indicates that the restore process has completed, wait several minutes and then repeat Step 2.
- If you see an error message indicating that the restore process ended but was not successful, check the log files by performing the following procedure:

  a. Enter the following command:

  [ipicsadmin]# **more /opt/cisco/ipics/database/logs/db-maintenance.log**

  Press the Spacebar to see additional lines of text, if necessary.

  b. View and evaluate the log file entries.

  The log file should give an indication as to why the restore process did not complete successfully. For example, if you performed a backup to a remote host and specified a user name that does not have the proper permissions to perform an scp operation, a message similar to the following example displays:

```
2007-01-16 15:10:21 Error: Remote scp failed because of a
password error on host: 10.1.1.1 User: invalidscpuser
```

c. Note the failure that occurred.

d. Perform any actions as indicated by the failure to fix the problem. If you require further assistance, see the "Troubleshooting Cisco IPICS Backup and Restore Procedures" section on page 9-30 to attempt to fix the problem.

e. Retry the restore operation by following the procedure in the "Performing the Restore Procedure" section on page 9-14.

Downloading and Viewing the Backup and Restore Logs

Cisco IPICS stores the logging details of backup and restore activity in two files, db-maintenance.log and dbm_log_archive.log.gz.

- The db-maintenance.log file captures the logging information that Cisco IPICS generates for backup or restore operations in a single day. Cisco IPICS saves the log information for the day that it last performed a backup or restore operation in the db-maintenance.log file.

  You can view the contents of the db-maintenance.log file in the **Administration > Database Management > Log** window.

Note The db-maintenance.log file does not exist on the server until you perform a database backup or restore operation for the first time.

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

  Whenever you perform a backup or restore operation, Cisco IPICS checks the db-maintenance.log file to see if it contains log data for that day. If the db-maintenance.log file contains data for a previous day, Cisco IPICS moves

the information in the db-maintenance.log file to the dbm_log_archive.log.gz file. Cisco IPICS then saves the log data from the current backup or restore operation to the db-maintenance.log file.

The default maximum allowable size of the dbm_log_archive.log.gz file is 5 MB. When the file reaches the maximum size, Cisco IPICS removes 5 percent of the oldest information in the dbm_log_archive.log.gz file until the file is smaller than the configured maximum size.

You can download the dbm_log_archive.log.gz file, along with the db-maintenance.log file, and save it to your PC by clicking the **Download** button in the **Administration > Database Management > Log** window. Once you download the files to your PC, you can view them as a text file.

Note The downloaded files are joined and compressed into a single zipped file. The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files.

To download the db-maintenance.log and the database archive file from the Administration Console, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Log** window to access the Log tab.

Step 2 Click **Download** to open the Download dialog box.

The Download dialog box displays.

Step 3 Click **Save** to save the compressed file to your PC.

The **Save As** dialog box opens.

Step 4 Navigate to the directory location where you want to save the file; then, click **Save**.

The download program saves the .zip file to the location that you specified.

Step 5 Navigate to the directory location where you saved the .zip file.

Step 6 Double-click the .zip file to open it.

The .zip file opens and displays the db-maintenance.log and dbm_log_archive.log.gz files.

Step 7 Click **Extract**.

The Extract window opens.

Step 8 Navigate to the location of the directory where you want to save the log files.

Step 9 Click **Extract**.

The extract program saves the log files to the location that you specified on your PC.

Step 10 To view the content of the log files, open the files with any software program that allows you to view text files.

Using CLI to Export and Import the Cisco IPICS Databases

In some situations, you may not be able to back up and restore your data by using normal backup and restore operations.

The following examples represent situations when you cannot use the backup and restore functionality in the Administration Console.

- A hardware error rendered your browser inoperable, and you cannot access the Cisco IPICS Administration Console. However, you can still access the database files by using CLI commands.
- You need to upgrade your system to a later version of the Cisco IPICS operating system and Cisco IPICS software. The database schema might be different between the Cisco IPICS software releases. In this situation, you would export your data to an external source, load the newest release of Cisco IPICS operating system (if required) and Cisco IPICS software onto the server, and import the data to the current release of Cisco IPICS.

To perform backup and restore operations without using the Administration Console, or migrate your data to a later version of Cisco IPICS, use the CLI-based import and export script utilities. To manually perform this functionality, use the **export_ipics_db** utility program to back up your databases, and the **import_ipics_db** utility program to restore your databases.

This section describes the import and export procedures and includes the following topics:

- Using the Database Export Utility, page 9-23
- Using the Database Import Utility, page 9-26

Understanding the Cisco IPICS Databases

Cisco IPICS has four databases. See Table 9-3for a description of the databases.

Table 9-3 Cisco IPICS Databases

Database Name	Description
ipics	This is the primary database for the Cisco IPICS application.
ippe	This is the database for the policy engine.
db_cra	This is the primary database for the dial engine. It contains the dial engine configuration including the following: • SIP provider configuration • Dial engine application definitions (for example, an instance of a dial engine script with an associated trigger) • Application triggers (for SIP and HTTP) • System configuration parameters
db_cra_repository	This is the script and prompt database for the dial engine. The following elements are stored in this database: • Standard dial engine scripts (in *.aef format) • Custom dial engine scripts (in *.aef format) • Standard script prompts (in *.wav format) • Customized script prompts (in *.wav format) • Spoken names (in *.wav format)

Using the Database Export Utility

The **export_ipics_db** utility program backs up your database, and creates the ipics.exp directory and the dbexport.out file.

Before you run the export utility, you must create a subdirectory for each of the four databases. If you do not create a separate subdirectory for each database, the export utility overwrites any export files that exist in the directory.

Note When you perform an upgrade from Cisco IPICS release 1.0(2) to release 2.0(1), you only export the ipics database. The ipics database is the only database that exists in Cisco IPICS release 1.0(2).

You can run the export utility program as often as you require. You create a directory for each export operation. Cisco recommends that you name the subdirectory of each backup set to include a date so that you can easily identify it.

To use the export utility, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the root user ID.

- From a direct server connection, log in by using the root user ID.
- From a remote secure client, open a terminal window using SSH Secure Shell Client software or similar software. Then, log in by using the root user ID.

  A terminal window displays.

Step 2 If it does not already exist, create a main directory for your export by entering the following command:

[root]# **mkdir -p /idspri/backup/IPICS_BACKUPS/**<*subdirectory_name*>

where:

<*subdirectory_name*> is the name that you specify to identify this backup set. Cisco recommends that you include the day and month of the backup, for example **ipics_backup_02_07_2007**.

Step 3 Navigate to the directory that you just created by entering the following command:

[root]# **cd /idspri/backup/IPICS_BACKUPS/**<*subdirectory_name*>

Step 4 Create a subdirectory for the ipics database export operation by entering the following command:

[root]# **mkdir ipics**

Step 5 If you are performing an export from Cisco IPICS release 2.0(1), create subdirectories for the three additional databases that exist in release 2.0(1) by performing the following steps:

a. Create a subdirectory for the ippe database export operation by entering the following command:

[root]# **mkdir ippe**

b. Create a subdirectory for the db_cra database export operation by entering the following command:

[root]# **mkdir db_cra**

c. Create a subdirectory for the db_cra_repository database export operation by entering the following command:

[root]# **mkdir db_cra_repository**

Note If you are performing an upgrade from Cisco IPICS release 1.0(2) to 2.0(1) you do not need to perform this step, as the ipics database is the only one that exists in Cisco IPICS release 1.0(2).

Step 6 Make sure that the informix user and the ipics group own the **/idspri/backup/IPICS_BACKUPS** directory and its subdirectories by entering the following command:

[root]# **chown -R informix:ipics /idspri/backup/IPICS_BACKUPS**

Step 7 Log in as the informix user by entering the following command:

[root]# **su - informix**

Step 8 Navigate to the export directory by entering the following command:

[informix]# **cd /idspri/backup/IPICS_BACKUPS/<***subdirectory_name***>**

Step 9 Navigate to the ipics subdirectory by entering the following command:

[informix]$ **cd ipics**

Step 10 Execute the export utility program and export the ipics database by entering the following command:

[informix]$ **export_ipics_db ipics**

Cisco IPICS displays the following message on the console:

```
WARNING: This action will bring the database server to Single-user
mode - Confirm?([Y]/N):
```

Step 11 Enter **Y** to confirm the database export operation.

Cisco IPICS backs up your primary ipics database and places the contents in the ipics.exp subdirectory.

Step 12 If you are performing an upgrade procedure from Cisco IPCS release 1.0(2) to Cisco IPICS 2.0(1), perform the following steps:

a. Copy the information in the ipics directory to an external host.

b. Install the Cisco IPICS operating system software and server software.

c. Perform the import procedure as described in the "Using the Database Import Utility" section on page 9-26.

Step 13 If you are performing an export procedure from Cisco IPICS release 2.0(1), perform the following steps:

a. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

b. Navigate to the ippe subdirectory by entering the following command:

[informix]$ **cd ippe**

c. Export the ippe database by entering the following command:

[informix]$ **export_ipics_db ippe**

Cisco IPICS displays the following message on the console:

```
WARNING: This action will bring the database server to Single-user mode - Confirm?([Y]/N):
```

d. Enter **Y** to confirm the database export operation.

Cisco IPICS backs up the database for the policy engine and places the content in the ipics.exp subdirectory.

e. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

f. Navigate to the db_cra subdirectory by entering the following command:

[informix]$ **cd db_cra**

g. Export the db_cra database by entering the following command:

[informix]$ **export_ipics_db db_cra**

h. Enter **Y** to confirm the database export operation.

Cisco IPICS backs up the dial engine database.

i. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

j. Navigate to the db_cra_repository subdirectory by entering the following command:

[informix]$ **cd db_cra_repository**

k. Export the db_cra database by entering the following command:

[informix]$ **export_ipics_db db_cra_repository**

l. Enter **Y** to confirm the database export operation.

Cisco IPICS backs up the script and prompt database for the dial engine.

Using the Database Import Utility

After you save the exported backup files to a new or existing server, you run the **import_ipics_db** utility program for each database. This utility program imports the backed-up content and rebuilds the databases on your server.

You can run the import utility program from any Cisco IPICS installation. If you have several backup sets from which to restore, be sure to run the import utility program from the subdirectory that contains the specific backup set that you want.

Procedure

Step 1 Open a console terminal or remote terminal window, and log in by using the root user ID.

Step 2 Stop the database processes by entering the following command from the command prompt:

[root]# **service ipics stop**

Note Cisco IPICS cancels any active policy engine dial-in or dial-out calls when you enter the **service ipics stop** command. For more information about the policy engine, refer to the "Using the Cisco IPICS Policy Engine" chapter of the *Cisco IPICS Server Administration Guide*.

Step 3 Navigate to the **/idspri/backup/IPICS_BACKUPS** directory by entering the following command:

[root]# **cd /idspri/backup/IPICS_BACKUPS**

Step 4 If you have several backup sets in this directory, find the subdirectory for the backup set that you want to restore by entering the following command:

[root]# **ls -l**

Step 5 Navigate to the subdirectory that contains the backup set that you want to restore by entering the following command:

[root]# **cd** <*subdirectory_name*>

where:

<*subdirectory_name*> is the name of the subdirectory that contains the backup set.

Step 6 Navigate to the ipics subdirectory by entering the following command:

[root]# **cd ipics**

Step 7 Verify that the ipics.exp directory exists in this subdirectory by entering the following command:

[root]# **ls -l**

The following information displays:

```
[informix]$ ls -l
total 120
-rw-r-----    1 informix ipics 110699 Oct 23 16:26 dbexport.out
drwxr-x---    2 informix ipics 4096 Oct 23 16:26 ipics.exp
```

Step 8 Enter the following command to retrieve the full path of the directory that contains the backup set:

[root]# **pwd**

Step 9 Make a note of the full directory path that displays.

Step 10 Log in as the informix user by entering the following command:

[root]# **su - informix**

The server logs you in as the informix user and places you in the /home/informix directory.

Step 11 Navigate to the directory in which the ipics.exp directory is located by entering the following command:

[informix]$ **cd /idspri/backup/IPICS_BACKUPS/**<*subdirectory_name*>**/ipics**

where:

<*subdirectory_name*> is the name of the subdirectory that contains the backup set.

Step 12 Execute the import utility program by entering one of the following commands, depending on the release of Cisco IPICS from which the database was exoirted:

- If the data was exported from Cisco IPICS release 1.0(2), enter the following command:

  [informix]$ **import_ipics_db ipics -convert**

- If the data was exported from Cisco IPICS release 2.0(1), enter the following command:

  [informix]$ **import_ipics_db ipics -drop_db**

Step 13 Enter **Y** to confirm the database import operation.

If you are upgrading from Cisco IPICS release 1.0(2), Cisco IPICS converts the 1.0(2) database schema to the 2.0(1) database schema, and restores your primary ipics database. If you are importing data from Cisco IPICS release 2.0(1), Cisco IPICS drops the existing database in your server, and imports the imported database to your server.

Step 14 If you are upgrading from Cisco IPICS release 1.0(2), proceed to Step 15. If you are restoring a database set from Cisco IPICS release 2.0(1), perform the following steps:

a. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

b. Navigate to the ippe subdirectory by entering the following command:

[informix]$ **cd ippe**

c. Execute the import utility program and import the ippe database by entering the following command:

   [informix]$ **import_ipics_db ippe -drop_db**

   Cisco IPICS restores the database for the policy engine.

d. Enter **Y** to confirm the database import operation.

   Cisco IPICS drops the current database, and imports the exported database for the policy engine.

e. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

   [informix]$ **cd ..**

f. Navigate to the **db_cra** subdirectory by entering the following command:

   [informix]$ **cd db_cra**

g. Execute the import utility program and import the ippe database by entering the following command:

   [informix]$ **import_ipics_db db_cra -drop_db**

h. Enter **Y** to confirm the database import operation.

   Cisco IPICS drops the current database, and imports the exported dial engine database.

i. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

   [informix]$ **cd ..**

j. Navigate to the **db_cra_repository** subdirectory by entering the following command:

   [informix]$ **cd db_cra_repository**

k. Execute the import utility program and import the **db_cra_repository** database by entering the following command:

   [informix]$ **import_ipics_db db_cra_repository -drop_db**

l. Enter **Y** to confirm the database import operation.

   Cisco IPICS drops the current database, and imports the exported script and prompt database for the dial engine.

After the import process is complete, you must restart the Tomcat service to synchronize the information in the database and the RMS.

Step 15 To restart the Tomcat service, follow these steps:

a. Enter **exit** to log out of the informix user ID.

b. Enter the following command to restart the Tomcat service and the policy engine:

[root]# **service ipics restart**

Note Cisco IPICS cancels any active policy engine dial-in or dial-out calls when you enter the service **ipics restart** command.

Cisco IPICS displays the `[OK]` message after the Tomcat service has successfully stopped, and again after it has successfully restarted.

If the Tomcat service does not successfully start, refer to the *Cisco IPICS Troubleshooting Guide, Release 2.0(1)* for more information.

There may be a slight delay before users can access the Administration Console after the Tomcat service restarts.

Troubleshooting Cisco IPICS Backup and Restore Procedures

This section describes how to troubleshoot backup and/or restore activity.

The procedures that are described in this section require that you have access to one or more of the following user IDs:

- root
- informix
- ipicsadmin

This section includes the following topics:

- Backing Up Data to a Remote Host Without scp Support, page 9-31

- Restoring Data from a Remote Host Without scp Support, page 9-32
- Unable to Log In To the Administration Console After Restoring Data, page 9-34
- Unable to Retrieve a Database Backup from a Remote Host after Reinstalling Cisco IPICS, page 9-36

Backing Up Data to a Remote Host Without scp Support

Problem The remote host to which you want to back up your data does not support the scp command (for example, if the remote host is a Windows PC or server).

Solution Choose the Local Directory option when you back up your files, then use an SFTP client software program to copy your backup data to a remote host.

Perform the following procedure to back up your data to a remote host that does not support scp:

Procedure

Step 1 Back up your files to a local directory by following the procedure in the "Performing a Manual Database Backup" section on page 9-3.

Step 2 Open a program that can act as an SFTP program, such as SSH Secure Shell Secure File Transfer Client or similar software. If you are using SSH Secure Shell File Transfer Client, choose **Start > Programs > SSH Secure Shell > Secure File Transfer Client** to connect remotely to the Cisco IPICS server from your PC.

The SSH Secure Shell File Transfer Client window displays. The desktop of your PC displays in the left pane.

Step 3 Click **Quick Connect** to connect to the server.

The Connect to Remote Host window displays.

Step 4 In the Host field, enter the DNS host name or the IP address for your server. Then, press the **Tab** key.

Step 5 In the User Name field, enter **root**.

Step 6 Click **Connect**.

The Enter Password window displays.

Step 7 Enter the password for the root user and click **OK**.

The SSH Secure Shell File Transfer Client connects to the server and displays the contents of the **/root** directory in the right pane of the window.

Step 8 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 9 In the **Enter Folder Name** field, enter the name of the folder where you backed up your files (for example, **/idspri/backup/mybackup**).

The right pane of the window displays the contents of the folder. The folder contains a directory that is timestamped with the date and time that the local directory backup was performed, for example **IDSB2006-11-02_14-04-52**. This directory contains your backup files.

Step 10 In the left pane of the window, navigate to the folder on your PC where you want to copy the backup files.

Step 11 Click the timestamped **IDSB***yyyy-mm-dd_hh-mm-ss* folder in the right pane of the window.

Step 12 Drag the folder from the right pane of the window to the left pane to initiate the copy procedure.

A progress window displays while the file copies the backup folder to the folder that you specified on your PC. When the copy completes, the backup folder displays in the left pane.

Step 13 Close the SSH Secure Shell File Transfer Client.

Restoring Data from a Remote Host Without scp Support

Problem You backed up your data to a remote host that does not support scp (for example, a Windows PC or server), and you need to retrieve the backup files from the remote host.

Solution Use an SFTP client software program to move the backup files from the remote host to the server, then restore your data from the Local Directory to which you moved the backed-up data.

Perform the following procedure to restore your data from a remote host that does not support scp:

Procedure

Step 1 Access the remote host to where you backed up your data.

Step 2 Open a program that can act as an SFTP program, such as SSH Secure Shell Secure File Transfer Client or similar software. If you are using SSH Secure Shell File Transfer Client, choose **Start > Programs > SSH Secure Shell > Secure File Transfer Client** to connect remotely to the Cisco IPICS server from your PC.

The SSH Secure Shell File Transfer Client window displays. The desktop of your PC displays in the left pane.

Step 3 Click **Quick Connect** to connect to the server.

The Connect to Remote Host window displays.

Step 4 In the Host field, enter the DNS host name or the IP address for your server. Then, press the **Tab** key.

Step 5 In the Host field, enter the DNS host name or the IP address for your server. Then, press the **Tab** key.

Step 6 In the User Name field, enter **root**.

Step 7 Click **Connect**.

The Enter Password window displays.

Step 8 Enter the password for the root user and click **OK**.

The SSH Secure Shell File Transfer Client connects to the Cisco IPICS server and displays the contents of the **/root** directory in the right pane of the window.

Step 9 In the left pane of the window, navigate to the folder location on your remote host where you stored the backup files, for example, **C:\My Documents\IDSB2006-11-02_14-04-52**.

Step 10 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 11 In the **Enter Folder Name** field, enter **/idspri/backup**.

The right pane of the window displays the contents of the **/idspri/backup** folder.

Step 12 Drag the backup folder on your PC from the left pane of the window to the right pane to initiate the copy procedure.

A progress window displays while the file copies from your PC to the **/devices** directory. When the copy completes, the backup folder displays in the right pane, for example **IDSB2006-11-02_14-04-52**.

Step 13 Click the **New Terminal Window** icon or choose **Window > New Terminal** from the menu bar to open a terminal window session.

Step 14 Enter the following command to change the ownership of the backup folder and files:

[root]# **chown -R informix:ipics /idspri/backup/IDSB***

Step 15 Enter the following command to enable Cisco IPICS to read from and write to the backup folder and files:

[root]# **chmod -R 550 /idspri/backup/IDSB***

Step 16 Close the SSH Secure Shell terminal window.

Step 17 Close the SSH Secure Shell File Transfer Client.

Step 18 Restore your files from the local directory by following the procedure in the "Performing the Restore Procedure" section on page 9-14. Be sure to specify the **/idspri/backup** directory, as well as the entire path name of the **IDSB***yyyy-mm-dd_hh-mm-ss* directory, when performing the local restore operation.

Unable to Log In To the Administration Console After Restoring Data

If you cannot log in to the Administration Console after you restore your data, note any errors that you receive in your browser and compare the error against the problem descriptions that follow. Then, perform the procedure that is listed in the corresponding solution to attempt to fix your problem.

Problem You performed a restore operation. After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 9-17, you determine that the restore process has completed

successfully. When you attempt to log in to the Cisco IPICS console, you receive a "Cannot find server or DNS Error" error message in the Internet browser, and you cannot access the Administration Console.

Solution It is possible that the Tomcat service was not restarted after the restore operation. To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server using the root user ID.

Step 2 To restart the Tomcat service and the policy engine, enter the following command at the prompt:

[root]# **service ipics restart**

Note Cisco IPICS cancels any active policy engine dial-in or dial-out calls when you enter the service **ipics restart** command.

The Tomcat service and the policy engine stops and restarts.

Step 3 Log in to the Administration Console.

Problem After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 9-17, you determine that the restore process has completed successfully. When you attempt to log in to the Cisco IPICS console, you receive the following pop-up window:

```
You entered an invalid name or password.
Please try again.
If this problem persists, the database may be unavailable. Contact
your system administrator for help.
```

Solution It is possible that the Cisco IPICS database did not restart after the restore operation. To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server using the root user ID.

Step 2 To check the status of the database, enter the following command at the prompt:

[root]# **onstat -**

If the database is online and running, the command displays the following response.

```
IBM Informix Dynamic Server Version 10.00.UC1 -- On-Line -- Up
00:16:14 -- 124036 Kbytes
```

If the database is not running, the command displays the following response:

```
shared memory not initialized for INFORMIXSERVER 'IPICSDBServer'
```

Step 3 If the database is not running, manually start the Informix database by entering the following command at the prompt:

[root]# **service ipics_db start**

Step 4 Log in to the Administration Console.

Unable to Retrieve a Database Backup from a Remote Host after Reinstalling Cisco IPICS

Problem You reinstalled the Cisco IPICS operating system software server software and attempted to restore your data from a remote host. The restore operation failed.

Solution When you reinstall the Cisco IPICS operating system, the host keys that are used by the scp process are deleted from the Cisco IPICS system. These host keys are used by the remote system for authentication purposes. In this case, the host keys that are used by the remote system to authenticate the Cisco IPICS system no longer match the host keys for the newly-installed Cisco IPICS system.

To configure the remote host so that the new host keys are recognized, perform the following steps:

Procedure

Step 1 Open a terminal window to the remote host by using SSH Secure Shell Client software or similar software.

Step 2 Log in to the remote host by using the same user name that you used for the database backup to the remote host.

Step 3 Open a secure shell terminal to the Cisco IPICS server by entering the following command:

ssh <*ip_address*> | <*dns_name*>

where:

<*ip_address*> or <*dns_name*> represents the IP address or DNS host name of the server.

You should receive a message similar to the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@        WARNING: HOST IDENTIFICATION HAS CHANGED!        @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key in /yoursystem/ssh/known_hosts to get rid of this
message.
Agent forwarding is disabled to avoid attacks by corrupted servers.
X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)?
```

Step 4 Enter **Yes** at the prompt to accept the new public host key for the Cisco IPICS server.

Step 5 Enter **exit** at the prompt to log out of the Cisco IPICS server.

Step 6 Enter **exit** at the prompt to log out of the remote host.

Step 7 Retry the restore operation from the Cisco IPICS Administration Console as described in the "Restoring Data from a Database Backup" section on page 9-12.

CHAPTER 10

Understanding Cisco IPICS Serviceability and Diagnostic Information

This chapter describes the serviceability and diagnostic information that is available for Cisco IPICS and contains the following sections:

- Introducing the Serviceability Drawer, page 10-1
- Viewing the Information in the Dashboard Window, page 10-2
- Viewing Cisco IPICS Server Diagnostic Information, page 10-8
- Viewing Cisco IPICS Server Diagnostic Information, page 10-8
- Viewing the Cisco IPICS System Logs, page 10-13
- SNMP Support for Cisco IPICS, page 10-18

Introducing the Serviceability Drawer

This release of Cisco IPICS introduces the Serviceability drawer, which is included under the Server tab in the Administration Console. This drawer provides a centralized location for diagnostic and status information, such as system and resource dashboard data, diagnostic information to help enable problem resolution, and quick access to system logs.

The Serviceability drawer enables your access to the following windows:

- Dashboard—The Dashboard window provides you with Cisco IPICS system and resource information. For more information about the information that is included in this window, see the "Viewing the Information in the Dashboard Window" section on page 10-2.
- Diagnostics—This window contains summary information about the Cisco IPICS server and the components of the Cisco IPICS system that interact with the server. From this window, you can also execute a diagnostic script, and download the results of that diagnostic script and additional diagnostic information. For more information about the Diagnostics window, see the "Viewing Cisco IPICS Server Diagnostic Information" section on page 10-8
- System Logs—This window displays logging information for Cisco IPICS. This information can be useful for troubleshooting or debugging your system. For more information about the System Logs window, see the "Viewing the Cisco IPICS System Logs" section on page 10-13.

Viewing the Information in the Dashboard Window

The dashboard window displays current, real-time information regarding the overall status of your system. This window displays the resources that you have used in your system, and the resources that you have available. These resources range from system resources, such as central processing unit (CPU) and memory usage, to entity resources, such as channel, VTG, user, license, and RMS details.

There are multiple panes in this window, one for each resource. Each pane is also known as a dashboard.

Tip To refresh the elements in this window and obtain the latest information, click **Refresh** at the top of the window.

This section contains the following topics:

- Understanding the System Dashboard, page 10-3
- Understanding the Channel Dashboard, page 10-5
- Understanding the Virtual Talk Group Dashboard, page 10-5
- Understanding the User Dashboard, page 10-6
- Understanding the License Dashboard, page 10-6
- Understanding the RMS Dashboard, page 10-7

Understanding the System Dashboard

The System Dashboard displays information about the Cisco IPICS policy engine, server memory and hard disk usage, and multicast address information. See Table 10-1 for all of the elements that are contained in this pane.

For related information about policy engine services and trace files, see the "Obtaining Information about Dial Engine Services" section on page 8-2 and the "Managing Tracing for the Policy Engine" section on page 8-4.

Table 10-1 Elements in the System Dashboard

Element	Description
Policy counts [multi-purpose, invitation]	The total number of policies (either active or inactive) that are available for the policy engine, grouped by multi-purpose and invitation policies. For more information about policy types, see the "Adding a Policy" section on page 7-6 and the "Managing Actions for a Policy" section on page 7-8.
Policy Engine status	The status of the policy engine. Up indicates that the policy engine is active, Down indicates that the policy engine is inactive.

Table 10-1 Elements in the System Dashboard (continued)

Element	Description
Configured activity log size (in MB)	The maximum size of the activity log file. **Note** The activity log file is not the same as the system log file that you view in the **Serviceability > System Logs** window. You access the activity log information in the **Administration** drawer. For more information about activity logs, see the "Managing Activity Logs" section on page 2-83.
Current activity log size (in MB)	The current size of the activity log file.
Free memory (in MB)	The amount of random access memory (RAM) that is available in the Cisco IPICS server. The RAM is obtained from the Dual Inline Memory Modules (DIMMs) in the Cisco IPICS server.
Used memory (in MB)	The amount of RAM that the server is currently using.
CPU - percent idle	The percentage of CPU resources that are idle and available. The CPU resources are obtained from the CPU in the server.
Disk usage (in GB) [used / free / total]	This field provides you with the following information: • The amount of disk space that is currently used in your server. • The amount of free disk space that is currently available in your server. • The total amount of hard disk space that is available in your server.
Total/Available number of multicast addresses in pool	This field represents the total number of multicast addresses in the multicast address pool, and the number of multicast addresses that are available, respectively. For more information about the multicast address pool, see the "Managing the Multicast Pool" section on page 2-47.

Understanding the Channel Dashboard

The Channel Dashboard displays information about the total number of channels, the number of enabled, disabled, active, and connected channels in your system, and the current status of those channels. For more information about channels and how they are used in Cisco IPICS, see the "Managing PTT Channels and Channel Groups" section on page 2-2.

See Table 10-2 for all of the elements that are contained in this pane.

t

Table 10-2 Elements in the Channel Dashboard

Element	Description
Total number of channels	This field represents the total number of channels that you have configured for the Cisco IPICS server.
Number of enabled channels	This field represents the number of channels that are enabled.
Number of disabled channels	This field represents the number of channels that are disabled.
Media Connection Count (for enabled channels)	This field represents the total number of media connection assignments that are mapped to enabled channels in the **Configuration > Channels** window. If any enabled channel has more than one media connection assignment, this number will be greater than the number of enabled channels.
Number of active channels	This field represents the number of enabled channels that are present in a virtual talk group (VTG).

Understanding the Virtual Talk Group Dashboard

The Virtual Talk Group Dashboard displays information about the number of VTGs and VTG templates in your system. For more information about VTGs, see the "Managing VTGs" section on page 4-2.

See Table 10-3 for all of the elements that are contained in this pane.

Table 10-3 Elements in the VIrtual Talk Group Dashboard

Element	Description
Number of VTG templates	This field represents the number of VTG templates that exist in the server.
Number of active VTGs	This field represents the number of VTGs that are currently active.

Understanding the User Dashboard

The User Dashboard displays information about the number of users who are logged in to the Administration Console, the number of users who are logged in to Cisco IPICS by using an IP phone, and the number of users who are logged in to Cisco IPICS by using the PMC. For more information about users, see the "Managing Users" section on page 3-2.

See Table 10-4 for all elements in the user dashboard.

Table 10-4 Elements in the User Dashboard

Element	Description
Number of users logged in to the administration console	total number of users who are logged in to the Administration Console.
Number of IP phone users logged in to Cisco IPICS	The total number of IP phone users who are logged in to the Cisco IPICS system.
Number of PMC users logged in to Cisco IPICS	The total number of PMC users who are logged in to the Cisco IPICS system.
Number of users dialed in to Cisco IPICS	The total number of users who are using the dial-in functionality of the Cisco IPICS system.

Understanding the License Dashboard

The License Dashboard displays information about the total and available number of ports that are licensed for use with Cisco IPICS. For more information about licenses, see the "Managing Licenses" section on page 2-72.

See Table 10-5 for all of the elements that are contained in this pane.

Table 10-5 Elements in the License Dashboard

Element	Description
Multicast Ports	The total number of multicast ports that your Cisco IPICS system is licensed to use, and the number of multicast ports that are available for use.
IP phone Ports	The total number of IP phone ports that your Cisco IPICS system is licensed to use, and the number of IP phone ports that are available for use.
LMR Ports	The total number LMR ports that your Cisco IPICS system is licensed to use, and the number of LMR ports that are available for use.
Dial Ports	The total number of policy engine dial ports that your Cisco IPICS system is licensed to use, and the number of dial ports that are available for use.
PMC Ports	The total number of PMC ports that your Cisco IPICS system is licensed to use, and the number of PMC ports that are available for use.

Understanding the RMS Dashboard

The RMS Dashboard displays information about the status of your RMS component(s) and the total and available number of voice ports that your system is licensed to use. For more information about the RMS, see the "Managing the RMS" section on page 2-56.

See Table 10-6 for all of the elements that are available in this pane.

Table 10-6 Elements in The RMS Dashboard

Element	Description
RMS <*rms-name*>	The status of your RMS component. This value is specified as operational or not operational. <*rms-name*> is the name of your RMS.
Total/Available voice ports	The total number of voice ports that are configured for your server, and the number that are available for use.

Viewing Cisco IPICS Server Diagnostic Information

The Diagnostics window displays diagnostic information for various components of the Cisco IPICS server.

When you access the Diagnostics window, Cisco IPICS runs a script to obtain the diagnostic information; the information displays in the Diagnostic Summary pane. To refresh the pane and display the most current diagnostic information for your server, click the **Execute Diagnostic Script** button, which is located on the lower left side of the window.

You can click the **Download Diagnostic Results** button, which is next to the **Execute Diagnostic Script** button, to download all diagnostic information that is included in this window, along with the ipics.log file. For more information about how to download the diagnostic results, see the "Downloading the Server Diagnostic Information" section on page 10-11. For more information about the ipics.log file, see the "Understanding the System Log Entries" section on page 10-13.

See Table 10-7 for all of the elements that are contained in the Diagnostic Summary pane.

Table 10-7 Elements in the Diagnostic Summary Pane

Element	Description
Cisco IPICS Server Hostname:	This field displays the host name of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **hostname**

Table 10-7 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Cisco IPICS Server Current Date and Time:	This field displays the current date and time of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **date**
Cisco IPICS Server OS Version:	This field displays the version of the Cisco IPICS operating system that is currently installed on the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/redhat-release**
Cisco IPICS Server Software Version:	This field displays the current version of the Cisco IPICS server software. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **grep -i "ipics.server.version=" ${TOMCAT_HOME}/webapps/ipics_server/WEB-INF/classes/resources/common.properties**
Hardware Platform Details:	This field displays detailed information for the hardware platform. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/hwprofile**
CPU Details:	This field displays detailed information for the CPU. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /proc/cpuinfo**
Cisco IPICS Server Network Interface Card Information:	This field displays the configuration of the Network Interface Cards (NICs), and the packets that have been transmitted and received on the NICs, that are installed on the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session. [root]# **ifconfig**

Table 10-7 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Uploaded License File Name(s):	This field displays the name of the license file(s) that have been uploaded onto the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **ls -l ${TOMCAT_HOME}/webapps/license/***
Uploaded License File Contents:	This field displays the contents of the license file(s) that have been uploaded onto the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat ${TOMCAT_HOME}/webapps/license/***
Cisco IPICS Database Status:	This field displays the current status of the database. The database can be either online or offline. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **onstat -**
Cisco IPICS Tomcat Web Server Status:	This field displays the current status of the Tomcat service. The Tomcat service functions as the Web server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **ps -ef | grep tomcat** **Note** If the Tomcat service is inactive (down), you may not be able to access the Administration Console. In specific situations, your Cisco technical support representative may direct you to manually run the **ps -ef | grep tomcat** script to gather details about the overall state of the system.
Cisco IPICS Server Hard Disk Utilization Information:	This field displays usage information for the hard disks in the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **df -a**

Table 10-7 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Cisco IPICS PMC Configuration File Contents:	This field displays the contents of the pmc.ini file. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat ${TOMCAT_HOME}/webapps/ipics_server/pmcdownloads/pmc.ini** **Note** Cisco IPICS uses the pmc.ini file to determine how to communicate with the Cisco IPICS server. The pmc.ini file is present only if you have generated a PMC installer. If you have not yet generated the PMC installer file, Cisco IPICS displays the following message: **Cannot find any pmc.ini files under the /opt/cisco/ipics/tomcat/current/webapps/ipics_files/store/installer folder**. For more information about the pmc.ini file, and how to generate a PMC installer, see the "Managing PMC Versions" section on page 2-106.

Downloading the Server Diagnostic Information

Cisco IPICS displays the diagnostic summary of your system in the Diagnostic Summary pane. You can download this diagnostic summary, along with the current system log information, to your PC.

When you download the diagnostic summary, Cisco IPICS creates a tar file that contains the diagnostic summary and the most current ipics.log file. For more information about the ipics.log file, see the "Understanding the System Log Entries" section on page 10-13.

To download the server diagnostic information, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > Diagnostics**.

Step 2 Click **Download Diagnostic Results**.

The File Download dialog box displays.

Step 3 Click **Open** to open the tar file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The tar file opens and displays the following files:

- The **tacout** file contains the latest diagnostic summary information.
- The **ipics.log** file contains the latest log information for Cisco IPICS.
- The **lmgrd.log** file contains log information for the license manager.

Step 4 To save the tar file to your PC, click **Save**.

A Save As dialog box displays.

Step 5 Navigate to the location on your PC where you want to save the tar file.

Step 6 Click **Save**.

The system unpacks the **tacout**, **ipics.log** and **lmgrd.log** files from the tar file, saves the files to the location that you specified, and closes the Save As dialog box.

Step 7 Use a text file viewer on your PC to view the log files.

Note You must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Viewing the Cisco IPICS System Logs

Cisco IPICS provides the ability to view the latest server log information in the System Logs window. The Recent System Log Entries pane in the **Serviceability > System Logs** window contains the log information that shows you the processes that have occurred in the different components of the Cisco IPICS system. For example, you can view the recent Tomcat service or policy engine entries. The information that is contained in these logs can help you to troubleshoot problems that you might encounter with Cisco IPICS.

To refresh this window and see updated status information, click **Refresh**.

You can view the log information by using the Administration Console or you can save the log to a file and download it to your PC.

Note Cisco IPICS provides you with other logs that are not available in the **System Logs window**. You can view and download logs such as the Activity Log in the Administration Console. Cisco IPICS provides additional logs that are available by accessing the server with a console terminal. For a full list of the logs that Cisco IPICS provides, refer to the "Understanding the Cisco IPICS Logs" chapter of the *Cisco IPICS Troubleshooting Guide, Release 2.0(1)*.

This section includes the following topics:

- Understanding the System Log Entries, page 10-13
- Sorting the System Logs By ERROR or WARNING Messages, page 10-15
- Downloading System Logs, page 10-16

Understanding the System Log Entries

The system log entries include messages of different severities. These messages range from informational-level messages to messages that indicate that a fatal error has occurred with Cisco IPICS.

Table 10-8 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 10-8 System Log Entry Types

Log Entry Type	Purpose
TRACE	Fine-grained debug information (maximum detail) about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational message about noteworthy events, such as the starting of a scheduled policy.
WARN	Warning message about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.
ERROR	Message that is similar to a WARN message, but with higher severity, such as in the case of insufficient licenses. ERROR messages display in red in the Recent System Log Entries pane
FATAL	When a FATAL error occurs, Cisco IPICS generates an error notification message and displays the message prominently in the current window of any user with system administrator or All privileges. Also, FATAL messages display in red in the Recent System Log Entries pane. A FATAL message concerns an unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires that you take immediate action to fix the specified error. If you continue to encounter FATAL errors, or if you experience unexpected system failures, contact your Cisco technical support representative for further analysis.

Note By default, Cisco IPICS does not capture the TRACE and DEBUG messages in the system logs. You should not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Sorting the System Logs By ERROR or WARNING Messages

To visually identify the type of status messages that display in the Recent System Log Entries pane, Cisco IPICS displays log entries of differing severities in the following text colors:

- Red—Red messages indicate that an ERROR-level error has occurred.
- Blue—Blue messages indicate that a WARNING-level error has occurred.
- Black—Black messages indicate that an INFO-level error has occurred.

Cisco IPICS displays the total number of ERROR, WARNING and INFO messages in the Status Summary area, directly below the Recent System Logs pane.

You can also view each ERROR or WARNING message by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Logs**.

Step 2 Determine if there are any ERROR or WARNING messages in the log by viewing the Status Summary area, which is indicated by colored dots. The Status Summary area provides you with the total number of messages that appear in the Recent System Log Entries pane.

If the number of red (ERROR) or blue (WARNING) messages is greater than zero, proceed to the next step.

Step 3 From the drop-down list box that is located in the upper right of the window, choose one of the following options:

- **Errors—**To find ERROR-level messages
- **Warnings—**To find WARNING-level messages

Step 4 Click on the arrow buttons to navigate and view each ERROR or WARNING message:

- Click **| <** to find the first message in the System Log.
- Click **<** to move backward one message in the System Log.
- Click **>** to move forward one message in the System Log.
- Click **> |** to move to the last message in the System Log.

Note If you are viewing the first message in the System Log, the **| <** and **<** arrow buttons are dimmed. If you are viewing the last message in the System Log, the **>** and **> |** arrow buttons are dimmed.

Downloading System Logs

Cisco IPICS displays the most current system log information in the Recent System Log Entries pane and allows you to download all the system logs to your PC.

Cisco IPICS saves the log information in sequential log files, starting with ipics.log and continuing with ipics.log.1 through ipics.log.10.

- Cisco IPICS records system log information in the ipics.log file and continues to add data to it until the file reaches a size of approximately 5.2 MB.
- When the ipics.log file reaches its maximum size, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new ipics.log file to capture the most current log data.

  This process of filling and incrementing files continues until you have ten system log files that range from ipics.log.1 to ipics.log.10, in addition to the most recent ipics.log file.
- When you have accumulated ten files, Cisco IPICS automatically purges the oldest file.

When you download your system logs, Cisco IPICS creates a zip file of all the ipics.log files.

The system logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

To download the system logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Logs**.

Step 2 Click **Download** at the bottom of the window, under the **Recent System Log Entries** pane.

The File Download dialog box displays.

Step 3 Click **Open** to open the tar file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The zip file opens and displays the list of ipics.log files.

Note To view the log file, you must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Step 4 To save the zip file to your PC, click **Save**.

A Save As dialog displays, from which you can navigate to the location to save the zip file on your PC.

Step 5 If you chose to save the zip file, click **Save**.

The system unzips the files from the zip file, saves the files to the location you specified, and closes the Save As dialog box.

SNMP Support for Cisco IPICS

The Cisco IPICS server software includes read-only support for Simple Network Management Protocol Version 3 (SNMPv3). SNMPv3 is a protocol that facilitates the secure exchange of management information between network devices.

Note Cisco IPICS does not support SNMP traps.

This section describes how you configure and use SNMP with Cisco IPICS and includes the following topics:

- Supported MIBs and RFCs, page 10-18
- Configuring an SNMP Management Console and MIB Browser for Use with Cisco IPICS, page 10-25

Supported MIBs and RFCs

The server software provides a set of management information base (MIB) files and Request for Comments (RFC) documents to support SNMPv3.

The MIBs are divided into the following types:

- MIBs that provide you with information about the Cisco Media Convergence Server (MCS) hardware. Table 10-9 lists the Cisco MCS hardware MIBs that Cisco IPICS supports and the object ID (OID) for each MIB.

Note Cisco IPICS does not supply you with the hardware MIBs. If your SNMP management console (such as, a MIB browser) does not contain these MIBs, you can search for the MIBs by accessing the Hewlett-Packard web site at http://www.hp.com and downloading them to your SNMP management console. You can search for the MIBs by specifying either the MIB name or OID.

- MIBs that provide you with information about network and system status. Table 10-10 lists the network status MIBs.

  These MIBs are the standard MIBs that are installed with the Net-SNMP package for the Cisco IPICS operating system. The MIBs are located in the following directory in the Cisco IPICS server:

  /usr/share/snmp/mibs

  If your SNMP management console does not contain these MIBs, you can download the MIBs from the server to your SNMP management console:

Cisco IPICS also includes RFCs with SNMP. RFCs provide you with definitions for MIBs and other SNMP elements. See Table 10-11 for the RFCs.

Table 10-9 lists the MIBs that are used for monitoring the status of the Cisco MCS hardware.

Table 10-9 Supported MIBs for Cisco MCS Hardware

Name	OID	Description
CPQIDA-MIB	1.3.6.1.4.1.232.3	This MIB module provides you with information about the Intelligent Drive Array.
CPQHOST-MIB	1.3.6.1.4.1.232.11	This MIB module provides you with host operating system information, including free memory, total memory size, free disk space, and total disk size.
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	This MIB module provides you with information about the standard equipment configuration for your server.
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	This MIB module provides you with information about threshold management functions.
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	This MIB module provides you with information about the files that are on the system.
CPQSINFO-MIB	1.3.6.1.4.1.232.2	This MIB module provides you with general system information.

Table 10-9 Supported MIBs for Cisco MCS Hardware (continued)

Name	OID	Description
CPQSM2-MIB	1.3.6.1.4.1.232.9	This MIB module provides you with information about the Remote Insight and Integrated Lights-Out Drivers and Agents (hprsm) service. This MIB also displays information about the network interface card (NIC), including NIC model, NIC type, NIC location, and the maximum transmission unit for the NIC.
CPQNIC-MIB	1.3.6.1.4.1.232.18	This MIB module provides you with information about the NIC.
CPQIDE-MIB	1.3.6.1.4.1.232.14	This MIB module provides you with information about the disk, including the disk model, its capacity, and its condition.

Table 10-10 lists the Net-SNMP MIBs that are used for monitoring the network.

Table 10-10 MIBs for Cisco IPICS Network and System Status

Name	Description
AGENTX-MIB.txt	This is the MIB module for the SNMP Agent Extensibility Protocol (AgentX).
DISMAN-EVENT-MIB.txt	The MIB module defines event triggers and actions for network management purposes.
DISMAN-SCHEDULE-MIB.txt	This MIB module defines a set of objects that provides mechanisms to schedule SNMP set operations periodically or at specific points in time.
DISMAN-SCRIPT-MIB.txt	This MIB module defines a set of objects that allow delegating management scripts to distributed managers.
EtherLike-MIB.txt	This MIB module describes generic objects for Ethernet-like network interfaces.
HCNUM-TC.txt	This MIB module contains textual conventions for high capacity data types.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
HOST-RESOURCES-MIB.txt	This MIB module defines a uniform set of objects that are useful for the management of host computers. Host computers are independent of the operating system, network services, or any software application.
HOST-RESOURCES-TYPES.txt	This MIB module registers type definitions for storage types, device types, and file system types.
IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt	This MIB module defines the AddressFamilyNumbers textual convention.
IANAifType-MIB.txt	This MIB module defines the IANAifType Textual Convention, and the enumerated values of the ifType object that is defined in the MIB-II ifTable.
IANA-LANGUAGE-MIB.txt	This MIB module registers object identifier values for well-known programming and scripting languages.
IANA-RTPROTO-MIB.txt	This MIB module defines the IANAipRouteProtocol and IANAipMRouteProtocol textual conventions, which are used in MIBs that need to identify unicast or multicast routing mechanisms.
IF-INVERTED-STACK-MIB.txt	This MIB module provides the Inverted Stack Table for interface sub-layers.
IF-MIB.txt	This MIB module describes generic objects for network interface sublayers. This MIB is an updated version of the MIB-II ifTable, and incorporates the extensions defined in Request for Comments (RFC) 1229.
INET-ADDRESS-MIB.txt	This MIB module defines textual conventions for representing Internet addresses. An Internet address can be an IPv4 address, an IPv6 address, or a domain name system (DNS) name. This module also defines textual conventions for Internet port numbers, autonomous system numbers, and the length of an Internet address prefix.
IP-FORWARD-MIB.txt	This MIB module provides information regarding Classless Inter-Domain Routing (CIDR) multi-path IP routes.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
IP-MIB.txt	This MIB module manages IP and Internet Control Message Protocol (ICMP) implementations, excluding the management of IP routes.
IPV6-ICMP-MIB.txt	This MIB module is used for entities that implement ICMP version 6 (ICMPv6).
IPV6-MIB.txt	This MIB module is used for entities that implement IP version 6 (IPv6).
IPV6-TC.txt	This MIB module is used for entities that implement the IPv6 TC protocol.
IPV6-TCP-MIB.txt	This MIB module is used for entities that implement TCP over IPv6.
IPV6-UDP-MIB.txt	This MIB module is used for entities that implement the User Datagram Protocol (UDP) over IPv6.
NET-SNMP-AGENT-MIB.txt	This MIB module defines control and monitoring structures for the Net-SNMP agent.
NET-SNMP-EXAMPLES-MIB.txt	This MIB module provides example MIB objects for agent module example implementations.
NET-SNMP-EXTEND-MIB.txt	This MIB module defines a framework for scripted extensions for the Net-SNMP agent.
NET-SNMP-MIB.txt	This MIB module provides information about the top-level infrastructure of the net-SNMP project enterprise MIB tree.
NET-SNMP-TC.txt	This MIB module provides textual conventions and enumerations for the Net-SNMP project.
NOTIFICATION-LOG-MIB.txt	This MIB module MIB module is used for logging SNMP notifications (traps and informs).
RMON-MIB.txt	This MIB module contains standard information relating to remote network monitoring.
SMUX-MIB.txt	This MIB module describes SNMP Multiplexing (SMUX) protocol management objects.
SNMP-COMMUNITY-MIB.txt	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2c, and SNMPv3.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
SNMP-FRAMEWORK-MIB.txt	This MIB module is used for SNMP management architecture.
SNMP-MPD-MIB.txt	This MIB module is used for message processing and dispatching.
SNMP-NOTIFICATION-MIB.txt	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters that are used by an SNMP entity for the generation of notifications.
SNMP-PROXY-MIB.txt	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters that are used by a proxy forwarding application.
SNMP-TARGET-MIB.txt	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters that are used by an SNMP entity for the generation of SNMP messages.
SNMP-USER-BASED-SM-MIB.txt	This MIB module provides definitions for the SNMP user-based security model.
SNMP-USM-AES-MIB.txt	This MIB Defines object identities for the advanced encryption standard (AES) by the SNMP user-based security model.
SNMP-USM-DH-OBJECTS-MIB.txt	This MIB module lists definitions for providing forward secrecy for key changes to the usmUserTable, and provides a method to kick-start access to the agent via a Diffie-Helman key agreement.
SNMP-VIEW-BASED-ACM-MIB.txt	This MIB module provides definitions for the View-based Access Control Model for SNMP.
SNMPv2-CONF.txt	This MIB module includes definitions for conformance groups.
SNMPv2-MIB.txt	This MIB module defines MIB objects for SNMPv2 entities.
SNMPv2-SMI.txt	This MIB module defines MIB objects for the Structure of Management Information (SMI).
SNMPv2-TC.txt	This MIB module defines MIB objects for SNMPv2 textual conventions.
SNMPv2-TM.txt	This MIB module defines MIB objects for SNMPv2 over UDP over IPv4.
TCP-MIB.txt	This MIB module manages TCP implementations.
TRANSPORT-ADDRESS-MIB.txt	This MIB module provides commonly used transport address definitions.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
UCD-DEMO-MIB.txt	This MIB module is used for the University of California, Davis (UCD) demonstration.
UCD-DISKIO-MIB.txt	This MIB module defines objects for disk input and output (I/O) statistics.
UCD-DLMOD-MIB.txt	This MIB module defines the MIB objects for dynamic loadable MIB modules.
UCD-IPFWACC-MIB.txt	This MIB module defines the MIB components for reading information from the accounting rules IP firewall.
UCD-SNMP-MIB.txt	This MIB defines the private UCD SNMP MIB extensions.
UDP-MIB.txt	This MIB module manages UDP implementations.

Table 10-11 lists the RFCs that are part of the Cisco IPICS SNMP infrastructure.

Table 10-11 RFCs for Cisco IPICS SNMP

Name	Description
RFC-1215.txt	This RFC specifies a straightforward approach to defining traps that are used with SNMP.
RFC1155-SMI.txt	This RFC provides the common definitions for the structure and identification of management information for TCP/IP-based internets.
RFC1213-MIB.txt	This RFC defines the second version of the Management Information Base (MIB-II) that are used with network management protocols in TCP/IP-based internets.

Configuring an SNMP Management Console and MIB Browser for Use with Cisco IPICS

To configure a MIB browser for Cisco IPICS on your SNMP management console, perform the following procedure:

Procedure

Step 1 (Optional) If your SNMP management console does not contain the MIBs, download the MIBs to your SNMP management console by performing the following actions:

- Download the hardware status MIBs by downloading them from the Hewlett-Packard web site at http://www.hp.com. See Table 10-9 for a list of the system hardware status MIBs.
- Download the Net-SNMP MIBs that provide overall network status by performing the following steps:
  a. Log in to the Cisco IPICS server by using the root user ID.
  b. Navigate to the **/usr/share/snmp/mibs** directory by entering the following command:

     [root]# **cd /usr/share/snmp/mibs**

  c. Locate the MIB file(s) that you want to use.
  d. Use a secure FTP program to download the MIB file(s) from the Cisco IPICS server to your SNMP management console.

     See Table 10-10 for a list of the Net-SNMP MIBs.

Step 2 From your SNMP management console, open a MIB browser that supports SNMPv3.

Step 3 Create a profile in the SNMP management console with the following information:

- Host: The IP address of the Cisco IPICS server
- User name: **ipics_snmp_user**
- Authentication password: **access_snmp**
- Authentication protocol (MD5 or Secure Hash Algorithm (SHA)): **MD5**

- Privacy/encryption password: **access_snmp**
- Privacy protocol (DES or AES): **DES**

Note The authentication protocol and privacy protocol are used to authenticate SNMPv3 messages.

Step 4 Use the supported MIB browser from your SNMP management console to perform read-only SNMP queries from the Cisco IPICS server.

Configuring the Cisco IPICS RMS Component

This appendix describes the configuration steps that you must follow to configure the RMS router for use with the Cisco IPICS server. The Cisco IPICS server accesses the RMS by using Secure Shell Client software; it authenticates the RMS by using the credentials that you configure in the RMS in the Cisco IPICS Administration Console Manage RMS window. (See the RMS management tasks that are described in Chapter 2, "Performing Cisco IPICS System Administrator Tasks," for more information.)

Note

- Before you can use an RMS with Cisco IPICS or perform RMS management tasks, you must first configure the RMS.
  - You manage the RMS from the Cisco IPICS server.
  - You must configure at least one RMS per Cisco IPICS server.
  - You cannot configure the same RMS in multiple Cisco IPICS servers.
- To ensure proper functionality, make sure that you map one RMS to one Cisco IPICS server; otherwise, you may encounter usability issues. For example, if the same RMS is mapped to more than one server, PMC users may hear a busy tone when they attempt to activate a channel or VTG because of configuration discrepancies.
- Be aware that Cisco IPICS provides support only for RMS components that are configured as described in this appendix.

FCS DRAFT -- CISCO CONFIDENTIAL

This appendix contains information about how to configure the RMS, and includes the following topics:

- Configuring Security Features, page A-2
- Connecting and Configuring T1/E1 Controllers, page A-5

Configuring Security Features

As with other routers that you use, Cisco recommends that you configure security features, such as access control, on the RMS. Access control allows you to designate the users who may access the router and specific services. The Cisco IOS software enables authentication, authorization, and accounting (AAA) network security services to provide access control on your router.

Cisco recommends that you configure AAA as your primary method for access control to provide an additional layer of security for your network. Specifically, Cisco recommends that you configure authentication on the RMS to enable the identification of users before they are permitted to access the network and network services. This identification includes login and password dialog, challenge and response, messaging support, and encryption (depending on the security protocol that you choose).

You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed.

Note Cisco IPICS supports the *default* method list, which is automatically applied to all interfaces if no other method list is defined.

To configure AAA and implement a basic level of security on the RMS, perform the following procedure:

Procedure

Step 1 To enable the AAA access control system, enter the following CLI command in global configuration mode:

FCS DRAFT -- CISCO CONFIDENTIAL

Router(config)# **aaa new-model**

This command initializes AAA.

Step 2 To set AAA authentication at login to use the default method with the *local* method keyword, enter the following command:

Router(config)# **aaa authentication login default local**

The default method list is automatically applied to all interfaces.

The *local* method keyword configures the router to use the local user name database for authentication.

Step 3 To configure a password for privileged EXEC mode, enter the following command:

Router(config)# **enable password** <*password*>

where *password specifies the enable password.*

Step 4 Establish a username-based authentication system by entering the following command in global configuration mode.

Router(config)# **username** <*name*> **privilege 15 password 0** <*password*>

where:

name specifies the user name that you configure on the RMS and *password* specifies the user enable password that you configured in Step 3.

Note Make sure that you configure the RMS with a valid user name and password.

This command creates a user name and password on the router. You enter this user name and password in the Cisco IPICS Administration Console when you configure the RMS.

The privilege parameter defines the privilege level for the user; this value ranges from 0 to 15, with 15 designating the highest privilege level.

Note To ensure successful authentication, the Cisco IPICS server requires that the user name that you create to access the RMS be configured with a minimum privilege level of 7.

FCS DRAFT -- CISCO CONFIDENTIAL

The single digit that follows the password parameter defines whether the text that follows the password is encrypted; a value of 0 signifies that the password is entered in clear text.

Step 5 Enable Secure Shell (SSH) version 2 protocol by entering the following command:

Router(config)# **ip ssh version 2**

This command specifies the SSH control parameters for the RMS. Version 2 ensures that the RMS does not inadvertently establish a weaker SSH version 1 connection.

Note The only protocol that the Cisco IPICS server requires to properly communicate with the RMS is SSH version 2. To ensure that the RMS is as secure as possible, Cisco recommends that you disable FTP, TFTP, HTTP, and HTTPS on the RMS after it has been deployed. For more information about the Cisco IOS commands that are required to disable these services, refer to the Cisco IOS documentation.

Step 6 Create cryptographic keys to enable Secure Sockets Layer (SSL) access from the Cisco IPICS server via SSH by entering the following commands:

Router(config)# **ip domain name** <*any domain name*>
Router(config)# **crypto key generate rsa**

where:

any domain name specifies default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name).

The **crypto key generate rsa** command generates Rivest, Shamir, and Adelman (RSA) key pairs, one public RSA key and one private RSA key, for the RMS.

Step 7 To disable the HTTP server (which is enabled by default), enter the following command:

Router(config)# **no ip http server**

If you enable the secure HTTP server by using the **ip http secure-server** command, you should disable the standard HTTP server by using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

Step 8 To enable log in by using Telnet and SSH, enter the following commands:

FCS DRAFT -- CISCO CONFIDENTIAL

```
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
Router(config-line)# exec-timeout 22 0
Router(config-line)# privilege level 15
```

Note The exec-timeout parameter sets the interval that the EXEC command interpreter waits until user input is detected. Optimally, you should set the exec-timeout to 22 (22 minutes). Setting this value to a shorter time, such as 5 or 10 minutes, can cause undesirable delays every time that Cisco IPICS accesses the router (such as when you change a VTG). Setting a longer time, such as 60 minutes, can cause authorized logins to accumulate and result in the router running out of open lines. Make sure that you do not set the exec-timeout to 0, which specifies no timeout.

You may implement more stringent security measures and harden your system security by configuring additional security features that Cisco IOS provides. For more information about configuring authentication, password security, and additional layers of security, refer to the *Cisco IOS Security Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/index.htm

Connecting and Configuring T1/E1 Controllers

The Cisco IPICS solution requires that you install at least one T1 or E1 loopback in the RMS to support mixing. (The RMS provides support for mixing multicast channels in support of VTGs and for mixing remote PMC SIP-based (unicast) connections to a multicast channel or VTG.)

The configuration steps that are required to implement the loopback pairs may vary depending on card type, Cisco IOS version, and the type of supported RMS that you use.

FCS DRAFT -- CISCO CONFIDENTIAL

Note For a complete list of supported interface cards and RMS routers, refer to the *Cisco IPICS Compatibility Matrix* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

This section contains guidelines for using T1 and E1 connectivity with Cisco IPICS and configuration procedures that you must follow for these card types; it includes the following topics:

- RMS Connectivity Guidelines, page A-6
- RMS IP Address Selection Guidelines, page A-8
- Configuring T1/E1 Controllers, Interfaces, and Voice Parameters, page A-9

RMS Connectivity Guidelines

To configure an RMS router for T1 or E1 connectivity, follow these guidelines:

- Configure at least two T1 or E1 controllers and assign ds0 groups to each controller.
- Allocate only as many ds0s on a controller as the RMS router can support simultaneously.
- Make sure that the ports that you allocate start with port 0 and are configured sequentially.
- Typically, a T1 controller will support 24 ds0s, but your controller may support fewer ds0s, depending on the number of available digital signal processors (DSPs). For more information about DSPs, see Step 6.

Note Timeslot 24 must always be configured even if you use a fractional T1. For more information, see the "DS0 Group-to-Timeslot Mapping Guidelines" section on page A-7.

- Typically, an E1 controller will support 30 ds0s, but your controller may support fewer ds0s, depending on the number of available DSPs.

FCS DRAFT -- CISCO CONFIDENTIAL

Note Timeslot 31 must always be configured, even if you use a fractional E1. For more information, see the "DS0 Group-to-Timeslot Mapping Guidelines" section on page A-7.

- Be careful not to allocate more ds0s than a controller has resources to support; otherwise, you may encounter lost audio and other voice quality issues.
- Configure T1 or E1 controllers for individual voice ports by entering the following command in the router configuration:

  ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type e&m-lmr**

  This command specifies the ds0 time slots that define logical voice ports on a T1 or E1 controller and configure the signaling type by which the router communicates with the PSTN.

  where:

  – **ds0-group** *ds0-group number* identifies the ds0 group

  For T1 connectivity, the allowable values range from 0 to 23
  For E1 connectivity, the allowable values range from 0 to 29

Note Be aware that ds0 groups must start with 0 and they must be sequential.

  – **timeslots** *timeslot-list* specifies a single time-slot number

  For T1 connectivity, the allowable values range from 1 to 24
  For E1 connectivity, the allowable values range from 1 to 31

DS0 Group-to-Timeslot Mapping Guidelines

You must configure the ds0-group-to-timeslot mapping according to the following associations. If you deviate from this configuration, the server will not be able to properly add the loopback pairs (one loopback equals one ds0 pair).

- T1:
  – ds0-group 0 = timeslot 24
  – ds0-group 1-23 = timeslot 1-23 (1 to 1, 2 to 2....23 to 23)

FCS DRAFT -- CISCO CONFIDENTIAL

For example, if you need to configure only 12 ds0s, configure ds0-group 0 through ds0-group 11. Be aware that ds0-group 0 must always map to timeslot 24.

- E1:
  - ds0-group 0 = timeslot 31
  - ds0-group 1-15 = timeslot 1-15
  - ds0-group 16 = timeslot 30
  - ds0-group 17-29 = Timeslot 17-29

  For example, if you need to configure only 16 ds0s, configure ds0-group 0 through ds0-group 15. Be aware that ds0-group 0 must always map to timeslot 31 and ds0-group 16 must always map to timeslot 30.

Note For detailed configuration information, see the procedure in the "Configuring T1/E1 Controllers, Interfaces, and Voice Parameters" section on page A-9. The configuration must be entered exactly as it is shown in this procedure.

RMS IP Address Selection Guidelines

The following guidelines pertain to the IP addresses that you must use with Cisco IPICS, as described in the "Configuring T1/E1 Controllers, Interfaces, and Voice Parameters" section on page A-9.

For successful interoperability with Cisco IPICS components, you must configure the following interfaces for the RMS:

- Ethernet0 Interface
  - This interface is the physical port that provides network connectivity
  - The IP address that you configure must be routable; that is, reachable by the network
- Loopback0 Interface
  - This virtual interface is used for network connectivity
  - The IP address that you configure must be routable (that is, reachable by the network); otherwise, your SIP connectivity will be affected
  - This IP address is assigned as the RMS IP address

FCS DRAFT -- CISCO CONFIDENTIAL

  - The server and the PMC components use this address to connect to the RMS

Note Cisco recommends that you configure the Loopback0 interface if there is more than one IP path to the RMS.

- Vif1 Interface
  - This virtual interface (Vif) is used to associate an IP address with the voice ports on the RMS
  - The VIF subnet that you configure must be routable (that is, reachable by the network); otherwise, your Cisco IPICS network connectivity will be affected
  - The actual IP address that is associated with the voice ports is the configured vif1 address + 1

Note Be aware that the IP addresses that you configure for both the Loopback0 and the Vif interfaces must be routable; this requirement is mandatory for both of these interfaces to ensure proper operation with Cisco IPICS. If the IP addresses for either of these interfaces are not routable, you may experience intermittent delays, of varying duration, from the time that you press the PMC PTT button to the time that the media is established between the remote PMC and multicast channels. This delay results from the inability of the RMS to perform Reverse Path Forwarding (RPF) checks on multicast Real-time Transport Protocol (RTP) packet source addresses. Therefore, to avoid this issue, make sure that the IP addresses for both the Loopback0 and the Vif interfaces are routable.

Configuring T1/E1 Controllers, Interfaces, and Voice Parameters

To configure T1 or E1 controllers, interfaces, and required voice parameters on an RMS, perform the following procedure.

FCS DRAFT -- CISCO CONFIDENTIAL

Procedure

Step 1 If you use a T1/E1 combination interface card, such as the Cisco 1- and 2-port T1/E1 Multiflex Trunk (MFT) Voice/WAN Interface Card (VWIC2), you must configure the card type for T1 or E1 by entering the following command:

Router(config)# **card type {t1 | e1}** *slot* [*bay*]

where:

slot specifies the port number of the interface, and *bay* is an optional parameter that specifies the card interface bay number in a slot on certain route/switch processor [RSP] platforms.

Examples of this command for both T1 and E1 connections appears below:

```
Router(config)# card type t1 0 3
Router(config)# card type e1 0 3
```

If you are using a T1/E1 combination interface card and want to replace one card type for another, proceed to Step 2. Otherwise, continue with Step 3.

Note Be aware that you cannot use an E1-only interface card or T1/E1 combination interface card in E1 mode with other interface cards, such as T1-only, in the same router because the global **signal pattern idle transmit 0000** command is not supported with all interface cards. (This command is supported for use only with the E1-only interface card and the T1/E1 combination card in E1 mode.) For more information about this command, see Step 15.

Step 2 To change the card type configuration and replace the T1 with an E1, as an example, enter the following commands:

a. Router(config)# **no card type t1** *slot* [*bay*]

Note When you use the card type command to change your configuration, be aware that changes become effective only after you reload or reboot the router.

b. Exit the router configuration mode by entering the following command:

FCS DRAFT -- CISCO CONFIDENTIAL

Router(config)# **exit**

a. Execute the following commands to save your changes and to reload the router:

Router# **copy running-config startup-config**
Router# **reload**

b. Configure the card type for E1 connectivity by entering the following command:

Router(config)# **card type e1** *slot* [*bay*]

where:

slot specifies the port number of the interface and *bay* is an optional parameter that specifies the card interface bay number in a slot on certain route/switch processor [RSP] platforms.

An example of this command appears below:

```
Router(config)# card type e1 0 3
```

Step 3 To enable the ports on the interface card to use the network clock for timing and ensure that the router backplane clock references are synchronized with the T1/E1 interface card, enter the following command:

Router(config)# **network-clock-participate** [**slot** *slot-number* | **wic** *wic-slot* | **aim** *aim-slot-number*]

where:

slot *slot-number* is an optional parameter that specifies the network module slot number on the router chassis
wic *wic-slot* specifies the WAN interface card (WIC) slot number on the router chassis
aim *aim-slot-number* specifies the Advanced Integration Module (AIM) in the specified slot (for applicable hardware)

An example of this command appears below; wic 3 designates the WAN interface card in physical slot 3:

```
Router(config)# network-clock-participate wic 3
```

To configure T1 controllers, proceed to Step 4. To configure E1 controllers, continue with Step 5.

FCS DRAFT -- CISCO CONFIDENTIAL

Note The following steps use Protocol Independent Multicast, or ip pim, sparse mode on the interface. Check to make sure that the design of your multicast network does not require you to use a different ip pim mode. For more information about multicast configurations, refer to the Cisco IOS Software Release 12.4 product documentation at the following URL and click the link for "Cisco IOS IP Multicast Configuration Guide, Release 12.4" http://www.cisco.com/en/US/products/ps6350/tsd_products_support_configure.html

Step 4 Configure ds0 groups on the T1 controllers by entering the following commands in the router configuration:

Tip Make sure that you configure the ds0-group-to-timeslot mapping exactly as shown and according to the guidelines that are described in the "DS0 Group-to-Timeslot Mapping Guidelines" section on page A-7.

Note The clock command should be used for only one of the two T1 controllers in the loopback.

a. To configure the first controller in the loopback pair, enter the following commands:

```
Router(config)# controller T1 1/0
Router(config-controller)# framing esf
Router(config-controller)# clock source internal
Router(config-controller)# linecode b8zs
Router(config-controller)# cablelength short 133
Router(config-controller)# ds0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
```

FCS DRAFT -- CISCO CONFIDENTIAL

```
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 16 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

ds0-group ds*0-group number* identifies the ds0 group and must be a value from 0 to 23; ds0 groups must start with 0 and must be sequential.

timeslots *timeslot-list* specifies a single time-slot number; for T1 connectivity, allowable values range from 1 to 24.

b. To configure the second controller in the loopback pair, enter the following commands:

```
Router(config)# controller T1 1/1
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# cablelength short 133
Router(config-controller)# ds0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
```

FCS DRAFT -- CISCO CONFIDENTIAL

```
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 16 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

ds0-group ds*0-group number* identifies the ds0 group and must be a value from 0 to 23; ds0 groups must start with 0 and must be sequential.

timeslots *timeslot-list* specifies a single time-slot number; for T1 connectivity, allowable values range from 1 to 24.

Step 5 Configure ds0 groups on the E1 controllers by entering the following commands in the router configuration.

Note

- The clock command should be used for only one of the two E1 controllers in the loopback.
- In E1 framing and signaling, 30 of the 32 available channels, or time slots, are used for voice or data transmission. Time slot 0 and time slot 16, which you do not configure, do not carry voice or data. Time slot 0 provides frame synchronization, alarm transport, and international carrier use while time slot 16 provides supervisory signaling for the 30 voice and data channels.

a. To configure the first controller in the loopback pair, enter the following commands:

```
Router(config)# controller e1 slot port
Router(config-controller)# clock source internal
Router(config-controller)# ds0-group 0 timeslots 31 type e&m-lmr
```

FCS DRAFT -- CISCO CONFIDENTIAL

```
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 30 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# ds0-group 24 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 25 timeslots 25 type e&m-lmr
Router(config-controller)# ds0-group 26 timeslots 26 type e&m-lmr
Router(config-controller)# ds0-group 27 timeslots 27 type e&m-lmr
Router(config-controller)# ds0-group 28 timeslots 28 type e&m-lmr
Router(config-controller)# ds0-group 29 timeslots 29 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

slot port specifies the backplane slot number and port number on the interface. An example of this command appears below:

```
Router(config)# controller e1 0/3/0
```

b. To configure the second controller in the loopback pair, enter the following commands:

FCS DRAFT -- CISCO CONFIDENTIAL

Router(config)# **controller e1** *slot port*
Router(config-controller)# d**s0-group 0 timeslots 31 type e&m-lmr**
Router(config-controller)# **ds0-group 1 timeslots 1 type e&m-lmr**
Router(config-controller)# **ds0-group 2 timeslots 2 type e&m-lmr**
Router(config-controller)# **ds0-group 3 timeslots 3 type e&m-lmr**
Router(config-controller)# **ds0-group 4 timeslots 4 type e&m-lmr**
Router(config-controller)# **ds0-group 5 timeslots 5 type e&m-lmr**
Router(config-controller)# **ds0-group 6 timeslots 6 type e&m-lmr**
Router(config-controller)# **ds0-group 7 timeslots 7 type e&m-lmr**
Router(config-controller)# **ds0-group 8 timeslots 8 type e&m-lmr**
Router(config-controller)# **ds0-group 9 timeslots 9 type e&m-lmr**
Router(config-controller)# **ds0-group 10 timeslots 10 type e&m-lmr**
Router(config-controller)# **ds0-group 11 timeslots 11 type e&m-lmr**
Router(config-controller)# **ds0-group 12 timeslots 12 type e&m-lmr**
Router(config-controller)# **ds0-group 13 timeslots 13 type e&m-lmr**
Router(config-controller)# **ds0-group 14 timeslots 14 type e&m-lmr**
Router(config-controller)# **ds0-group 15 timeslots 15 type e&m-lmr**
Router(config-controller)# **ds0-group 16 timeslots 30 type e&m-lmr**
Router(config-controller)# **ds0-group 17 timeslots 17 type e&m-lmr**
Router(config-controller)# **ds0-group 18 timeslots 18 type e&m-lmr**
Router(config-controller)# **ds0-group 19 timeslots 19 type e&m-lmr**
Router(config-controller)# **ds0-group 20 timeslots 20 type e&m-lmr**
Router(config-controller)# **ds0-group 21 timeslots 21 type e&m-lmr**
Router(config-controller)# **ds0-group 22 timeslots 22 type e&m-lmr**
Router(config-controller)# **ds0-group 23 timeslots 23 type e&m-lmr**
Router(config-controller)# **ds0-group 24 timeslots 24 type e&m-lmr**
Router(config-controller)# **ds0-group 25 timeslots 25 type e&m-lmr**
Router(config-controller)# **ds0-group 26 timeslots 26 type e&m-lmr**
Router(config-controller)# **ds0-group 27 timeslots 27 type e&m-lmr**
Router(config-controller)# **ds0-group 28 timeslots 28 type e&m-lmr**
Router(config-controller)# **ds0-group 29 timeslots 29 type e&m-lmr**
Router(config-controller)# **no shutdown**

where:

slot port specifies the backplane slot number and port number on the interface. An example of this command appears below:

```
Router(config)# controller e1 0/3/1
```

Step 6 Determine if dspfarms are enabled by executing the following command:

Router# **show run**

FCS DRAFT -- CISCO CONFIDENTIAL

If dspfarms are enabled, the output displays as shown in the following example; continue with Step 8:

```
voice-card 0
 dspfarm
!
voice-card 1
 dspfarm
```

If dspfarms are not enabled, the output displays as shown in this example; proceed to Step 7 to enable dspfarms:

```
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
```

Note

- For DSPs to be shared, you must first enable dspfarm, as described in Step 7, and make sure that all modules are participating in the network clock, as described in Step 3.
- When you enable dspfarm, you add specific voice cards to the DSP resource pool; this configuration allows multiple interface cards to share the installed DSP resources. (DSPs can be shared among digital modules and/or ports (such as T1/E1) and the motherboard, but DSPs cannot be shared among analog ports (such as an FXS)).
- At a minimum, you should enable one dspfarm.
- After the dspfarm is enabled on all modules that have DSPs installed, and all modules are participating in the main network clock, Cisco IOS interacts with these DSPs as part of the DSP resource pool.

Tip

To help calculate the DSPs that you need, based on your specific configuration, refer to *High-Density Packet Voice Digital Signal Processor Modules*, which is available at the following URL:
http://www.cisco.com/en/US/products/hw/modules/ps3115/products_qanda_item0900aecd8016c6ad.shtml

FCS DRAFT -- CISCO CONFIDENTIAL

Step 7 To enable dspfarms, enter the following commands:

Router(config)# **voice-card** <*slot number*>
Router(config-voicecard)# **dspfarm**

where:

slot number specifies the slot number for the voice interface card.

For example, the following command enables the dspfarm on the interface card that is installed in slot 0:

```
Router(config)# voice-card 0
Router(config-voicecard)# dspfarm
```

Step 8 To enable multicast routing, enter the following command:

Router(config)# **ip multicast-routing**

When IP multicast routing is enabled, the Cisco IOS software is enabled to forward multicast packets.

Step 9 If you use Cisco IPICS over a high latency, low bandwidth link, modify the maximum TCP outgoing queue per connection by entering the following command:

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

This command sets the maximum TCP outgoing queue to 100000 packets.

Note This step is optional; if you do not use Cisco IPICS over a high latency, low bandwidth connection, you do not need to configure this command.

Step 10 Create a virtual interface for multicast communications by entering the following commands:

Router(config)# **interface vif1**
Router(config-if)# **ip address** *ip_address subnet_mask*
Router(config-if)# **ip pim sparse-mode**

where:

ip_address specifies the IP address that you assign to this interface
subnet_mask specifies the 30-bit subnet mask that you assign to this interface; for example, 255.255.255.252

FCS DRAFT -- CISCO CONFIDENTIAL

This command configures a virtual interface that is similar to a loopback interface; that is, a logical IP interface that is always up when the router is active. The RMS assigns a virtual address of vif1 + 1 as the source address when it mixes voice traffic and then sends out this traffic via multicast.

For more information about IP address guidelines, see the "RMS IP Address Selection Guidelines" section on page A-8.

Step 11 To enable loopback mode and assign an IP address and subnet mask to the interface, create a loopback interface for voice signaling and media by entering the following commands:

Router(config)# **interface Loopback0**
Router(config-if)# **ip address** *ip_address subnet_mask*
Router(config-if)# **ip pim sparse-mode**

where:

ip_address specifies the IP address that you assign to this interface; this IP address gets assigned to the RMS
subnet_mask specifies the 30-bit subnet mask that you assign to this interface; for example, 255.255.255.252
0 specifies the identification number that you assign to the loopback interface

This command creates a software-only loopback interface that emulates an interface that is always up. (This virtual interface is supported on all platforms.) For more information about IP address guidelines, see the "RMS IP Address Selection Guidelines" section on page A-8.

Note Cisco recommends that you configure the Loopback0 interface if there is more than one IP path to the RMS.

Step 12 To configure voice signaling and media on the loopback interface, enter the following commands:

a. Router(config)# **voice service voip**

This command switches to voice-service configuration mode, from global configuration mode, and specifies the voice encapsulation type.

b. Router(conf-voi-serv)# **allow-connections sip to sip**

This command specifies that connections between SIP endpoints are allowed.

c. Router(conf-voi-serv)# **sip**

FCS DRAFT -- CISCO CONFIDENTIAL

This command enables Session Initiation Protocol (SIP) configuration mode.

d. Router(conf-serv-sip)# **bind control source-interface Loopback0**
Router(conf-serv-sip)# **bind media source-interface Loopback0**

These commands bind the source address for signaling and media packets to the IP address of the loopback interface.

e. Enter the following command to return to privileged EXEC mode:

Router(conf-serv-sip)# **end**

Step 13 Return to configuration mode by entering the following command:

Router# **configure terminal**

Step 14 To enable multicast routing for each interface that routes multicast traffic, enter the following commands:

a. Router(config)# **interface** <*interface*>

where:

<*interface*> specifies the interface that you want to enable Protocol Independent Multicast (PIM).

b. Router(config-if)# **ip pim sparse-mode**

Configure this command for each interface that routes multicast traffic. This command enables PIM sparse mode on the interface.

Step 15 To create a voice class that will be applied to all voice configurations, enter the following commands based on your connectivity:

a. When you use T1 connectivity, enter these commands:

Router(config)# **voice class permanent 1**
Router(config-class)# **signal timing oos timeout disabled**
Router(config-class)# **signal keepalive disabled**
Router(config-class)# **signal sequence oos no-action**

where:

1 specifies the unique number that you assign to the voice class.

b. When you use an E1-only interface card or a T1/E1 combination interface card specifically for E1 connectivity, enter all of the following commands:

FCS DRAFT -- CISCO CONFIDENTIAL

```
Router(config)# voice class permanent 1
Router(config-class)# signal timing oos timeout disabled
Router(config-class)# signal keepalive disabled
Router(config-class)# signal sequence oos no-action
Router(config-class)# signal pattern idle transmit 0000
```

where:

1 specifies the unique number that you assign to the voice class.

Note Make sure that you enter only the first four commands when you use T1 connectivity; when you use an E1-only interface card or a T1/E1 combination interface card specifically for E1 connectivity, you must also enter the **signal pattern idle transmit 0000** command as documented in Step 15.

Be aware that the **signal pattern idle transmit 0000** command is a global command that is supported for use only with E1-only interface cards and T1/E1 combination interface cards that you configure for E1 mode. (This command is not supported for use with other interface cards, such as T1-only cards.) When you configure this command, it affects all interface cards in the router; therefore, make sure that all interface cards are either E1-only interface cards or T1/E1 combination cards in E1 mode and that you do not mix T1-only, E1-only, and T1/E1 combination card types in the same router when you use this command.

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)# **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.

Step 17 Configure the list of codecs that Cisco IPICS will support by entering the following commands:

FCS DRAFT -- CISCO CONFIDENTIAL

```
Router(config)# voice class codec 1
Router(config-class)# codec preference 1 g729r8
Router(config-class)# codec preference 2 g711ulaw
```

These commands enable voice-class configuration mode, assign an identification tag number for a codec voice class, and specify the preferred codecs to use on a dial peer.

Step 18 Create the following inbound dial peer by entering the following commands:

Note Although Cisco IOS supports other values for some of the fields in this configuration, Cisco recommends that you configure the values that are shown below to ensure consistency.

```
Router(config)# dial-peer voice 555 voip
Router(config-dial-peer)# voice-class codec 1
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# incoming called-number .
Router(config-dial-peer)# no vad
Router(config-dial-peer)# dtmf-relay rtp-nte
```

These commands configure the voice dial peer and turn off voice activity detection (VAD) on the default SIP PMC connection.

Step 19 Create the following outbound dial peer to configure the voice dial peer for direct dial calls to the SIP provider by entering the following commands:

Note This step is optional; if you do not use the PMC direct dial feature, you do not need to configure this dial peer.

Although Cisco IOS supports other values for some of the fields in this configuration, Cisco recommends that you configure the values that are shown below to ensure consistency.

```
Router(config)# dial-peer voice 556 voip
Router(config-dial-peer)# destination-pattern 9T
Router(config-dial-peer)# voice-class codec 1
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# session target ipv4:<Cisco Unified CallManager or
```

FCS DRAFT -- CISCO CONFIDENTIAL

Cisco IOS SIP Provider IP address>
Router(config-dial-peer)# **session transport tcp**
Router(config-dial-peer)# **dtmf-relay rtp-nte**

where:

Cisco Unified CallManager or Cisco IOS SIP Provider IP address specifies the IP address of your SIP provider.

Note These commands configure the voice dial peer that enables the PMC direct dial feature and specifies the RTP-based mechanism to transport DTMF tones for SIP calls. In this configuration, the dial peer is set to 9T. If you need to use a different dial plan for the PMC direct dial capability, you can change this dial peer or add additional dial peer entries to allow for other destination patterns, as needed.

For more information about configuring the PMC direct dial feature, see the "Managing the Direct Dial Feature" section on page 8-37. For information about using the PMC direct dial feature, refer to the *Cisco IPICS PMC Installation and User Guide*.

Step 20 Configure the digest authentication credentials that the RMS should use when it is challenged by the SIP provider on direct dial call attempts by entering the following commands:

Note This step is optional; if you do not use the PMC direct dial feature, or if you do not use Cisco Unified CallManager as your SIP provider, you do not need to configure these credentials.

Router(config)# **sip-ua**
Router(config-sip-ua)# **authentication username** <*username*> **password** <*password*>
Router(config-sip-ua)# **exit**

where:

username and *password* match the configured username and password for the Application User in Cisco Unified CallManager and are used to authenticate this user. For more information, see the "Configuring Cisco Unified CallManager as the SIP Provider" section on page 8-42.

FCS DRAFT -- CISCO CONFIDENTIAL

Step 21 Enter the following command to reset the router command prompt:

Router(config)# **no prompt**

Step 22 Execute the following command to display the contents of the current, running configuration file and verify that the output reflects the modifications that you performed in this procedure:

Router# **show running-config**

Step 23 Execute the following command to save your changes:

Router# **copy running-config startup-config**

Step 24 If you reconfigured a T1/E1 combination interface card from T1 to E1 mode, you may need to reset the loopback cable. To determine if you need to reset the loopback cable, take one of the following actions:

- Check the LEDs on the interface card to see if the LP LED is amber.

  This LED should be off during normal operation.

- Enter the following CLI command to determine if there are alarms or errors displayed by the controller:

  Router# **show controllers e1**

  The command output should display the e1 in an "up" state with no alarms, as shown in the following sample output:

  ```
  e1 3/0 is up
  No alarms detected
  ```

  If the output displays the e1 in a "down" state, as shown in the following example, continue with Step 21:

  ```
  e1 3/1 is down
  alarm-trigger is not set
  ```

Step 25 To resolve this problem, disconnect the loopback cable from the router; then, reconnect it.

The LP LED should now be off.

Step 26 Verify that the e1 is up by entering the **show controllers e1 command, as shown above.** The command output should display the e1 controllers in an "up" state, with no alarms detected, as shown in the following sample output:

```
e1 3/0 is up
No alarms detected
```

FCS DRAFT -- CISCO CONFIDENTIAL

```
e1 3/1 is up
No alarms detected
```

Note Cisco IPICS supports the use of Land Mobile Radio (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. For detailed LMR gateway configuration information, refer to the Land Mobile Radio over IP documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/lmrip/

FCS DRAFT -- CISCO CONFIDENTIAL

Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device

Cisco IPICS provides the Cisco IPICS service, which allows several Cisco Unified IP Phone models to communicate on PTT channels and participate in channels and VTGs.

Before a user can access the Cisco IPICS service, Cisco IPICS must be configured as a phone service for Cisco Unified CallManager or for Cisco Unified CallManager Express. In addition, users in a deployment that includes Cisco Unified CallManager must subscribe to the Cisco IPICS service by using the Cisco Unified CallManager User Options application.

The total number of Cisco Unified IP Phones, LMR and multicast ports, PMC clients, dial users, and ops views cannot exceed the number that is specified in your Cisco IPICS license. For more information about licenses, see the "Managing Licenses" section on page 2-72.

This appendix includes the following topics:

- Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager, page B-2
- Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager Express, page B-3
- Subscribing to the Cisco IPICS Service, page B-4
- Using the Cisco IPICS Service on a Cisco Unified IP Phone, page B-5

Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager

This section describes how to configure the Cisco IPICS service in Cisco Unified CallManager. After you configure Cisco IPICS as an available service, IP phone users can subscribe to the service by using the Cisco Unified CallManager User Options web site. When users subscribe to the Cisco IPICS service, the Cisco Unified IP Phone Services menu displays Cisco IPICS as an option.

For additional information about Cisco Unified CallManager Administration and about setting up phone services, refer to the Cisco Unified IP Phone Services configuration information in *Cisco Unified CallManager Administration Guide* for your Cisco Unified CallManager version. You can find the Cisco Unified CallManager documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

To configure Cisco IPICS as an available service in Cisco Unified CallManager, perform the following procedure:

Procedure

Step 1 From Cisco Unified CallManager Administration, take one of these actions:

- For Cisco Unified CallManager 3.x or 4.x—Choose **Feature > Cisco IP Phone Services**.
- For Cisco Unified CallManager 5.x—Choose **Device > Device Settings > Phone Services**.

Step 2 In the page for configuring IP phone services, enter the following information:

a. In the **Service Name** field, enter **Cisco IPICS**.

This field specifies the name that displays for the service on the Cisco Unified IP Phone.

b. In the **Service Description** field, enter **Access to the Cisco IPICS System**, or a similar description.

This field contains a description of the content that the Cisco IPICS service provides. You can enter any appropriate description.

c. Cisco Unified CallManager 5.x only: In the ASCII Service Name field, enter **Cisco IPICS**.

   This field designates the name of the service to display if a phone cannot display Unicode.

d. In the **Service URL** field, enter the following URL, where *ipics server IP address* is the IP address of the Cisco IPICS server:

   http://<*ipics server IP address*>**/ipics_server/servlet/IPPhoneManager**

   This field specifies the URL of the Cisco IPICS server on which the Cisco IPICS service is located.

Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager Express

To configure Cisco IPICS as an available service in Cisco Unified CallManager Express, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IOS router that runs Cisco Unified CallManager Express.

Step 2 Type this command to access the enable prompt:

```
Router> enable
```

Step 3 Enter the following commands to define the IP address of the server that provides the service:

```
Router# configure terminal
Router(config)# telephony-service
Router(config-telephony)# url services http://
<ipics server IP address>/ipics_server/servlet/IPPhoneManager
```

(replace *ipics server IP address* with the IP address of the Cisco IPICS server)

Step 4 Press **Ctrl-Z** to return to the enable prompt.

Step 5 Enter this command to save your configuration:

```
Router# write running-config startup-config
```

Step 6 Log out of the Cisco IOS router.

Subscribing to the Cisco IPICS Service

Cisco Unified IP Phone users in a deployment that includes Cisco Unified CallManager must subscribe to the Cisco IPICS service before they can access the service from a phone.

The information in this section does not apply to users in a deployment that includes Cisco Unified CallManager Express. Cisco Unified CallManager Express supports one active service and users are subscribed to that service automatically.

Before a user can subscribe to the Cisco IPICS service, the service must be configured as described in the "Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager" section on page B-2.

To subscribe to the Cisco IPICS service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco Unified CallManager User Options web site.

For more information about accessing the Cisco Unified CallManager User Options web site, and for additional information about the phone features for your phone model, refer to the Cisco Unified IP Phone documentation at the following URL:

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

Step 2 From the Cisco Unified CallManager User Options Menu, choose your device type or profile from the drop-down list.

Step 3 From the Cisco Unified CallManager User Options Menu, choose **Configure your Cisco IP Phone Services**.

Cisco Unified CallManager displays a list of subscribed services and allows you to choose from a list of available services.

Step 4 Choose the **Cisco IPICS** service from the Available Services drop-down list, then click **Continue**.

Step 5 To subscribe to the Cisco IPICS service, click **Subscribe**.

The information that is configured in Cisco Unified CallManager Administration, such as the service description, the IP address of the Cisco IPICS server, and the path to the service, displays in this window.

Step 6 Click **Log Off**.

Using the Cisco IPICS Service on a Cisco Unified IP Phone

This section describes how to use the Cisco IPICS service from a Cisco Unified IP Phone. Before a user can access the Cisco IPICS service from a Cisco IP Phone, the prerequisites that are described in Table B-1 must be met:

Table B-1 Prerequisites for Using the Cisco IPICS Service

Prerequisite	Reference
Cisco IPICS service must be configured.	See the "Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager" section on page B-2 or the "Configuring Cisco IPICS as a Phone Service for Cisco Unified CallManager Express" section on page B-3.

Table B-1 Prerequisites for Using the Cisco IPICS Service

Prerequisite	Reference
Login credentials must be configured for the user.	A Cisco IPICS user can configure personal login credentials as described in the "Managing Your User Profile" section on page 5-2. A Cisco IPICS operator can configure login credentials for a user as described in the "Managing Dial Login Information for a User" section on page 3-13.
Users in a Cisco Unified CallManager environment must subscribe to the Cisco IPICS service.	See the "Subscribing to the Cisco IPICS Service" section on page B-4.

In addition, users should be aware of the following guidelines:

- To obtain help with using the Cisco IPICS service on a Cisco Unified IP Phone, press the **Help** softkey.
- Channels returned from Cisco IPICS to a Cisco Unified IP Phone must have a multicast connection defined in the Default Location field in the Dial Login tab for the user. (For more information about this tab, see the "Managing Dial Login Information for a User" section on page 3-13.) Channels that do not meet this requirement do not display on the phone.
- A Cisco Unified IP Phone receives a list composed of associated channels in alphabetized order, followed by a list of associated VTGs in alphabetical order.
- A Cisco Unified IP Phone does not receive direct two-way channels or direct dial channels because these channels require SIP unicast connections.
- A phone that is logged into the Cisco IPICS service logs out automatically after 30 minutes of inactivity.

- A Cisco IPICS user can be logged in to the Cisco IPICS service with the same login credentials on two or more phones simultaneously. In this case, the following information applies:
  - The user can send and receive audio on all of the phones.
  - If the user presses a key on any phone that causes the phone to interact with the server (for example, the **Back**, **Latch**, or **Help** softkey), all phones log out except the last one that was logged into.
- If a phone loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service, the service retains its current state and the user can continue to use the PTT functionality for the channel or VTG that is currently selected. However, the phone cannot connect to other channels or VTGs until connectivity to the server is re-established.
- When the Cisco Unified Wireless IP Phone 7921 is connected to an active Cisco IPICS channel or VTG, the phone goes into continuous listening mode. In this mode, the phone remains in an active receive state even if Cisco IPICS is not transmitting audio. In this state, the phone continues to draw power from the battery, which limits the battery life to approximately eight hours of talk time. (When the channel or VTG is deactivated, the phone enters standby mode to conserve power.) To ensure that you have adequate an power supply for your Cisco Unified Wireless IP Phone 7921, Cisco recommends that you maintain a backup battery for use with your phone. For more information about the Cisco Unified Wireless IP Phone 7921, refer to the Cisco Unified IP Phone documentation that is available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/index.htm
- You can customize the softkeys on the Cisco Unified Wireless IP Phone 7920/7921 to enable direct access to the Services menu. For details, refer to the Cisco Unified CallManager documentation at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/
- The PTT button on the Cisco Unified Wireless IP Phone 7921 does not require any special configuration. A user can use either this button or the PTT softkey to communicate in a VTG or a channel. The PTT button cannot be used to latch a channel. To latch a channel, you must press the **Latch** softkey.

To access the Cisco IPICS service from a Cisco Unified IP Phone, perform the following procedure:

Procedure

Step 1 Access the Services menu on the phone.

The procedure for accessing the Service menu varies by phone model. Refer to your Cisco IP Phone documentation for specific instructions.

Step 2 Choose the **Cisco IPICS** service, then press the **Select** softkey.

Step 3 Enter your digit ID and digit password (PIN), then press the **Submit** softkey.

Cisco IPICS displays the list of channels and VTGs that have been assigned to you and activated for your use.

The Cisco IPICS operator configures the digit ID and digit password (PIN). For more information, see the "Managing Dial Login Information for a User" section on page 3-13.

Step 4 Press the **Update** softkey to receive any new channels and VTGs.

The channels and VTGs that display in the menu are those that are available when the Cisco IPICS service starts. To view an updated list of channels, you must press the **Update** softkey. The Cisco IPICS server does not automatically download channel or VTG information to the phone until you press this softkey.

Step 5 To participate in a channel or VTG, use the Navigation button to scroll to the channel or VTG in which you want to participate, then press the **Select** softkey.

When you choose a channel or VTG, it becomes active on your Cisco Unified IP Phone.

Step 6 To talk on the channel or VTG, press and hold the **PTT** softkey.

If you want to latch, or lock in, the channel or VTG, press the **Latch** softkey on the Cisco Unified IP Phone. You can disengage the latch by pressing the **Stop** softkey. (On some phone models, you must press the **More** softkey to see **Latch**.)

Step 7 When you are done talking, release the **PTT** softkey to return to listen-only mode.

Step 8 When you are done using the Cisco IPICS service, press the **Logout** softkey.

On some phone models, you must press the **More** softkey to see **Logout**.

Frequently Asked Questions

This appendix contains frequently asked questions about Cisco IPICS, and provides answers to these questions:

Q. Does Cisco IPICS allow multiple Cisco IPICS servers to use the same RMS?

A. No, Cisco IPICS does not support the use of multiple Cisco IPICS servers for the same RMS. Each server must have the use of resources on a corresponding RMS to ensure proper functionality.

Q. Does Cisco IPICS support more than one RMS in the same location.

A. Yes.

Q. What makes a channel remote?

A. A channel is remote when it is in a different multicast domain than the user who is accessing it.

Q. What does the designation “REMOTE” mean for a PMC location?

A. 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 more detailed information about locations, see the “Managing Locations” section on page 2-38.

Q. If I only have one router in a location and my channel is defined as ALL, will the channel be accessible to a user?

A. Yes. However, if a router location is defined as ALL, a channel that is not also configured as ALL will not be accessible to users or VTGs that the router supports.

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. For more detailed information about locations, see the "Managing Locations" section on page 2-38.

Q. How many resources (voice ports, multicast addresses) do I need?

A. The following guidelines apply to the use of resources:

- Every channel that is active in a VTG uses one DS0 pair (also called a loopback)
- Every sub-VTG in a VTG uses one DS0 pair
- Every SIP connection uses one DS0 pair per channel or VTG per user, per location
- Local channels do not use any DS0 pairs
- G.729, which is used for a SIP connection, requires DSP resources
- A dial connection uses two DS0 pairs (for two multicast addresses) for the first dial user, and then one DS0 per subsequent dial user

The following items do not use voice resources:

- A user with an associated channel (the system only uses resources when the user logs in from a remote location)
- A VTG that includes only users
- User Groups
- Channel Groups

Q. Why would a VTG suddenly become active or inactive unexpectedly?

A. If a VTG unexpectedly becomes active or inactive, it could be because the VTG can be associated to a policy and the policy can execute, which could change the status of the VTG.

Q. What is the difference between the *Belongs To* attribute and the *Accessible To* attribute for an ops view?

A. The Belongs To attribute determines the ops view to which the resource belongs, or that the ops view owns. After a new ops view is created, the system administrator can associate resources, such as channels or users, to the ops view. The operator creates an operator user who belongs to that ops view and who can manage the ops view resources that are visible within the specific ops view.

The Accessible To attribute specifies that the resource is accessible to, or visible to, the ops view(s). Users only have access to the resources that are accessible to the ops view to which they belong. See "Configuring and Managing Cisco IPICS Operational Views" for more information about these attributes.

Q. What codecs does the dial engine support?

A. The dial engine supports only G.711 u-law. This codec is not configurable.

Q. How are license ports and DS0 loopback port resources counted in Cisco IPICS release 2.0(1)?

A. A single LMR (LMR Port) license is used when a channel is enabled.

A single PMC license is used each time that a PMC user logs in to the system. If a PMC user logs in multiple times, a license is used for each login occurrence.

A single IP phone license is used each time that an IP phone user (PMC xml client) logs in to the system.

A single Multicast (Multicast Port) license is used when a VTG is activated.

A single PSTN (Dial User) license is used in each of the following scenarios:

- One license is used for an active inbound call
- One license is used for an active outbound call

A single DS0 loopback pair is used in the following scenarios:

- For each remote channel on a PMC
- For each channel in an active VTG

- For each instance of an active VTG that is accessed by a dial-in or dial-out user, regardless of the number of users who are connected to the VTG

A single Ops View license is used for each configured ops view.

Q. Will an IP phone keep working if it loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service?

A. If a phone loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service, the service retains its current state and the user can continue to use the PTT functionality for the channel or VTG that is currently selected. However, the phone cannot connect to other channels or VTGs until connectivity to the server is re-established.

Q. In the case of a notification action that is in the form of an e-mail, sms, or page and a dial notification to a large number of users (for example, 100 users), what is the sequence of notification events?

A. The dial engine uses a scalable, multi-threaded dial-pool implementation for dialing out to users. Ports from the available dial pools are used by the currently executing policy notification/invite actions. If there are fewer dial ports available than what is needed, the other policy actions are put in a waiting state until more ports become available.

A call is considered successful when the call recipient authenticates. If there is no authentication, the system moves to the next dial preference that is listed in the Dial Preferences for the user in the user profile until either the call is successful or every number has been tried by the system. For detailed information, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 6-29 and the "Managing Communications Preferences for a User" section on page 3-23.

Q. During a dial-out to users, does a dispatcher get notified about numbers that have not yet been reached and is there any way to determine how long it should take to reach all the participants in a VTG?

A. Dialed numbers display in the **Policy Execution Status > Executed/Executing Policy** window, showing which numbers have been reached and which are still in progress.

For each available port, the user must authenticate by entering a digit ID/PIN and then the notification message is played. Whenever errors occur, such as the user entering an incorrect digit ID or PIN and/or a timeout occurring when

the user is not reached, the dial-out notification takes longer to complete. The total time for dial-out notification depends on these factors. For more information, see the "Viewing Information about Executing or Executed Policies" section on page 7-22.

Q. How do you integrate the dial engine into an existing network that runs an earlier version of Cisco Unified CallManager and does not have native SIP trunk support?

A. This integration can be accomplished by using a Cisco IOS router that runs Cisco Unified CallManager Express as the SIP provider and configuring an H.323 Intercluster Trunk (ICT) between the Cisco Unified CallManager and the SIP provider. For detailed information, refer to the *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*.

A

action — A discrete function that is performed through a policy. Discrete functions include activate VTG, notification, VTG add participant, dial-out, and invite to VTG.

activate VTG — An action that activates a preconfigured VTG; can also specify a duration. At the end of the specified duration, the VTG is deactivated. If no duration is specified, the VTG must be manually deactivated by the dispatcher from the VTG Management drawer in the Cisco IPICS administration console.

activated — A state that indicates that the SIP (unicast) or multicast channel is fully operational. When a channel/VTG on the PMC is enabled and activated, all of the PMC buttons are operational.

activating — A state that becomes effective when you click the **Activate** button on the PMC. The Activate button appears highlighted while the other PMC buttons remain in an inactive state as the system attempts to activate and connect.

activation button — This button toggles activate and deactivate functionality on the PMC. Click this button on the PMC to activate a channel (to call out); click it again to deactivate the channel.

active virtual talk group — A virtual talk group (VTG) becomes active when Cisco IPICS commits global resources, such as a multicast address and any necessary dial-in peers, so that the participants in the VTG can communicate with each other.

Administration Console — The graphical user interface (GUI) in the Cisco IPICS server software through which authorized Cisco IPICS users can manage and configure Cisco IPICS resources, events and VTGs.

alert tone buttons Buttons on the PMC that can play out alert tones on one channel or multiple channels.

all talk button Allows you to simultaneously talk on all of the channels that you selected.

autonomous system A radio system under one administrative control; also known as a management domain. This system is usually mapped to an agency.

B

backward compatibility The ability of newer radio equipment to operate within an older system infrastructure or to directly intercommunicate with an older radio unit. The term usually applies to digital radios that are also capable of analog signal transmission.

bandwidth The difference between the highest and lowest frequencies that are available for network signals. The term also describes the rated throughput capacity of a specific network medium or protocol. Bandwidth specifies the frequency range that is necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth.

base station A land station in the land mobile radio service. In the personal communication service, the common name for all the radio equipment that is located at one fixed location and used for serving one or several calls.

C

CAI common air interface. The standard for the digital wireless communications medium that is employed for P25-compliant radio systems and equipment. The standard for P25 Phase I incorporates Frequency Division Multiple Access (FDMA) technology.

call delay The delay that occurs when there is no idle channel or facility available to immediately process a call that arrives at an automatic switching device.

call setup time The time that is required to establish a circuit-switched call between users or terminals.

carrier A wave that is suitable for modulation by an information-bearing signal.

CAS channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.

channel A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. *See* PTT channel.

channel capacity The maximum possible information transfer rate through a channel, subject to specified constraints.

channel folder A logical grouping of channels

channel select check box Provides the ability to select or deselect the specified channel on the PMC for audio transmission.

channel spacing The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.

Cisco Unified CallManager The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified CallManager extends enterprise telephony features and functions to packet telephony network devices, such as Cisco Unified IP Phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco IPICS Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.

Cisco IPICS policy engine Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco IPICS server Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco Unified IP Phone A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.

Cisco Security Agent Provides threat protection for server and desktop computing systems (endpoints) by identifying, preventing, and eliminating known and unknown security threats.

CLI command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.

codec coder-decoder.

1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.

2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm that is used to compress/decompress speech or audio signals.

conference of conferences A conference that consists of two or more VTGs.

conventional radio system A non-trunked system that is similar to telephone party-line in that the user determines availability by listening for an open channel.

COR carrier operated relay. A signal from a receiver that indicates that the receiver is receiving a signal and that the receiver is not squelched.

coverage In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area.

D

delay time The sum of waiting time and service time in a queue.

decrypt Cryptographically restore ciphertext to the plaintext form it had before encryption.

decryption Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.

dial engine scripts Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.

dial-in A phone call that is dialed in to the policy engine.

dial-in floor control A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users.

dial number The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.

dial out invite An action that invites selected user(s) to the selected VTG.

A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.

dial peer Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.

digit ID A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.

digital modulation technique A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.

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

DS0 digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.

dynamic regrouping A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.

E

E & M recEive and transMit (or ear and mouth). The E&M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&M interface provides the most common form of analog trunking.

1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&M also is available on E1 and T1 digital interfaces.

2. A type of signaling that is traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.

encipher To convert plain text into an unintelligible form by using a cipher.

encode To modify information into the required transmission format.

encryption Application of a specific algorithm so as to alter the appearance of data and make it incomprehensible to unauthorized users.

event An active VTG in the Cisco IPICS solution.

F

FDM frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency.

FDMA frequency-division multiple access. A a channel access method in which different conversations are separated onto different frequencies. FDMA is employed in narrowest bandwidth and multiple-licensed channel operations.

FLEXlm Cisco software that enforces licensing on certain systems; FLEXlm ensures that Cisco IPICS software will work only on the supported and licensed hardware.

floor control The standard mechanism for Push-to-Talk speaker arbitration.

frame A logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment also describe logical information groupings at various layers of the OSI reference model.

frequency For a periodic function, frequency represents the number of cycles or events per unit of time.

frequency assignment Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.

frequency hopping The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.

frequency modulation Modulation technique in which signals of different frequencies represent different data values.

frequency sharing The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.

G

gateway Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway 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.

GRE generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers.

H

H.323 Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol.

high-band frequency Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.

Hoot ‘n’ Holler (Hootie) A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.

Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.

I

inactive VTG A VTG that is stored for use. The Cisco IPICS server stores inactive VTGs so that they can be automatically activated by a policy or manually activated by a dispatcher.

incident management framework A software framework that includes an adaptable GUI to facilitate resources, such as users, radio channels, cameras, and sensor information, for delivery that is based upon policy or incident needs.

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.

informix user ID 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** (superuser from root).

interference The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.

interoperability The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.

invitation policy A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.

invite to VTG A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.

ipicsadmin user ID 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 ID 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** (superuser from root).

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.

ipics user ID 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.

IPSec IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

K

keepalive A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.

key The parameter that defines an encryption code or method.

kilohertz (kHz) A unit of frequency that denotes one thousand Hz.

L

latch The PMC functionality that allows a Cisco IPICS user to lock in a PTT channel.

linear modulation A radio frequency transmission technique that provides the physical transport layer of a radio system. This technology is compatible in digital and analog system environments and supports channel bandwidths of 5 kHz to 50 kHz.

LMR Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel.

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.

location In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server.

low-band frequency Lower frequency levels in the VHF band, typically 25–50 MHz.

M

megahertz (MHz) A unit of frequency denoting one million Hz.

modulation The process, or result of the process, of varying a characteristic of a carrier in accordance with an information-bearing signal.

multicast Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network.

multicast address A single address that may refer to multiple network devices.

multicast address/port Cisco IPICS uses this type of connection to enable the PMC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and RMS components.

multicast pool Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.

multiplexing The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

multipurpose policy A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.

multiselect buttons Provides the ability to select or deselect all channels on the PMC for audio transmission.

mute The functionality that enables a dispatcher to mute a PMC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.

mutual aid channel A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.

N

narrowband channels Channels that occupy less than 20 kHz.

National Public Safety Planning Advisory Committee The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.

National Telecommunication and Information Administration The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government's use of the radio spectrum.

network An interconnection of communications entities.

NAT Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.

not activated A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No PMC buttons appear highlighted.

notification An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.

O

offline mode When the connection to the server goes offline, the PMC enters offline mode. Offline mode enables continuous communication during periods of server downtime. Using offline mode requires at least one successful login to the server.

operator The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.

ops view operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

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.

OTAR over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

P

packet A logical grouping of information that includes a header that contains control information. Usually also includes user data.

packet switching The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

PIM Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

PIM dense mode One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

PIM sparse mode One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.

PMC Push-to-Talk Management Center. A standalone PC-based software application that simulates a handheld radio to enable PTT functionality for PC users. This application enables Cisco IPICS PMC end-users, dispatch personnel, and administrators to participate in one or more VTGs at the same time.

PMC ID The unique ID that the Cisco IPICS server generates for each PMC to track requests between the PMC and the server and to verify and manage concurrent PMC usage for licensing requirements.

policy Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.

policy channel A channel that can be set up by the dispatcher and configured as a designated channel; that is, a channel that is always open to enable your interaction with the dispatcher.

policy execution status An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy,

portalization A web programming paradigm for customizing the interface and functionality of a client application.

protocol A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.

PTT Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy.

PTT channel A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel.

PTT channel button The button on the PMC that you click with your mouse, or push, and hold to talk. You can use the latch functionality on this button to talk on one or more channels at the same time.

PTT channel group A logical grouping of available PTT channels that can be used for categorization.

Q

QoS quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.

queue Represents a set of items that are arranged in sequence. Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive.

queuing delay In a radio communication system, the queuing delay specifies the time between the completion of signaling by the call originator and the arrival of a permission to transmit to the call originator.

R

radio channel Represents an assigned band of frequencies sufficient for radio communication. The bandwidth of a radio channel depends upon the type of transmission and its frequency tolerance.

radio equipment Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.

receive indicator The indicator on the PMC that blinks green when traffic is being received.

remote connection Cisco IPICS uses this type of connection to provide SIP-based trunking into the RMS component, which is directly tuned into the multicast channel.

RF radio frequency. Any frequency within the electromagnetic spectrum that is normally associated with radio wave propagation. RF generally refers to wireless communications with frequencies below 300 GHz.

RF repeater An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

RMS router media service. Component that enables the Cisco IPICS PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.

The RMS mixes multicast channels in support of VTGs and it also mixes PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

root user ID 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.

RTP Real-Time Transport Procotol. Commonly used with IP networks to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services.

S

scanning A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.

script prompts The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.

secure channel A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as a PMC or Cisco Unified IP Phone.)

An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.

service delivery area *See* coverage.

signal The detectable transmitted energy that carries information from a transmitter to a receiver.

skin Skins form the appearance of the PMC. In Cisco IPICS, skins are customizable and available in various options, including 4-channel and 8-channel mouse and touch screen formats.

speaker arbitration The procedure that is used to determine the active audio stream in a Push-to-Talk system.

spectrum The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:

High HF 25–29.99 MHz
Low VHF 30–50 MHz
High VHF 150–174 MHz
Low UHF 406.1–420/450–470 MHz
UHF TV Sharing 470–512 MHz
700 MHz 764–776/794–806 MHz
800 MHz 806–824/851–869 MHz.

spoken names The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded.wav files that can be uploaded into the system.

squelch An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.

stored VTG Also referred to as inactive VTG.

subscriber unit A mobile or portable radio unit that is used in a radio system.

system administrator The Cisco IPICS 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.

system architecture The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.

T

T1 Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.

T1 loopback Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.

talk group A VTG or a channel.

A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.

TCP Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TDMA time division multiple access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval (“slot” or “slice”) for the transmission of each channel; that is, the channels take turns to use the link.

terminal A device capable of sending, receiving, or sending and receiving information over a communications channel.

throughput The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.

TIA/EIA-102 standards A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.

tone control The process of sending a 2175 Hz inband tone with voice transmission to control receiving radios remotely. An inband tone can be used to control functions such as frequency selection and channel monitoring.

transmit indicator On some of the PMC skins, this indicator blinks red when traffic is being transmitted.

trigger A time-based event that invokes a policy on a scheduled basis, without manual intervention.

trunk A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.

trunked (system) Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.

trunked radio system Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel.

TUI telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.

U

user The Cisco IPICS user may set up personal login information, download the PMC application, customize 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 Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.

unicast Specifies point-to-point transmission, or a message sent to a single network destination.

V

VAD Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the PMC only sends voice traffic when it detects your voice.

virtual channel A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the PMC application or a supported Cisco Unified IP Phone model.

voice interoperability Voice interoperability enables disparate equipment and networks to successfully communicate with each other.

voice replay A feature that allows the PMC user to replay buffered audio on a per channel basis.

VoIP Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality.

volume indicator The volume indicator on the PMC that shows the current volume level on the channel in a graphical format.

volume up/down buttons The buttons on the PMC that let you control the volume level.

VOX Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation.

VTG virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.

VTG add participant An action that adds selected participant(s) to the selected VTG.

VTG template Before becoming active, a VTG is in an inactive state as a VTG template. The server stores VTG templates so that they can be automatically activated by a policy or manually activated by a dispatcher. Also known as a preconfigured VTG.

W

wavelength The representation of a signal as a plot of amplitude versus time.

wideband channel Channels that occupy more than 20 kHz.

Symbols

* (asterisk), in Cisco IPICS Administration Console windows 1-9, 1-13

A

About, in Administration Console 1-16
accessing
  Active Users window 2-79
  Activity Log Management window 2-85
  Activity Log Options window 2-90
  Channel Groups window 2-28
  Channels window 2-4
  Dial Engine drawer 8-1
  Download PMC window 5-2
  License Management window 2-72
  Locations window 2-45
  Multicast Pool window 2-48
  My Profile window 5-2
  Ops View window 6-3
  Options window 2-92
  PMC Installer window 2-122
  PMC Versions window 2-107
  Policy Management drawer 7-1
  RMS window 2-57
  Skins window 2-119
  User Groups window 3-42
  Users window 3-3
  Virtual Talk Groups window 4-2
action
  activate VTG 7-8
  definition 7-1
  deleting 7-15
  dial-out 7-8, 7-13
  in multi-purpose type policy 7-10
  invite to VTG 7-8, 7-10
  managing 7-8
  notification 7-8
  overview 7-8
  re-activating 7-26
  VTG add participants 7-8, 7-12
activating
  policy 7-21
  RMS 2-63
  VTG 4-19, 7-10
active
  channel state in Channel window, described 2-13
  multicast address 2-50, 2-54
  VTG 4-2

VTG guidelines 4-17

active users

fields, described 2-80

viewing 2-79

viewing information for 2-79

activity log

described 2-84

downloading 2-85

managing 2-83

managing activity types per ops view 2-89

options per ops view 2-89

types 2-89

understanding the Activity Log Management window 2-84

viewing 2-85

viewing and downloading 2-85

viewing and downloading archived 2-88

activity log retention period, setting described 2-94

adding 2-120

alert tone set 2-115

a sequence of multicast addresses to multicast pool 2-52

channel 2-7

channel group 2-30

locations 2-45

multicast address to multicast pool 2-51

RMS 2-64

skins 2-120

user 3-6

user group 3-43

VTG template 4-10

address

e-mail, of user 3-12

information for user 3-11

multicast address 2-49

of user, in user profile 5-6

street, of user in Users window 3-11

Address Information tab 3-11

Administration Console

accessing 1-11

Authentication window 1-11

client system requirements 1-11

displaying current data 1-10

exiting 1-13

logging in 1-11

logging out 1-13

obtaining information about 1-16

online help 1-16

overview 1-7

refreshing 1-10

timeout 1-16

advanced PMC permissions 3-19

advanced PMC permissions, field described 5-9

alerting tones

See alert tones

alert tones

adding 2-115

associating ops views 2-117

creating alert tone sets 2-113
deleting 2-118
managing 2-112
viewing or editing alert tone sets 2-117
allow association to users field, described 2-11
allow latch
field in user profile 5-9
for channel 2-17
in PMC tab 3-19
allow use in VTGs field, described 2-12
all role, described 1-7, 3-12
associating
alert tones to ops views 2-117
channel with user 3-28
ops views with user group 3-47
ops view with user 3-35
phone with user 3-31
policy with user 3-32, 7-19
user with policy 3-32, 7-19
user with user 3-30
Associations tab 3-22
audio, disable 3-19
audio client 1-6
authentication log file 3-18, 3-20
Authentication window 1-11

B

backup and restore operations
overview 9-1
performing 9-1
browser
guidelines for using 1-10
memory issues 1-11
pop-up windows, disabling blocking 1-10
refreshing windows 1-10
busy channel 2-6

C

calculating DSPs A-17
changing status of VTG template 4-19
channel
active status 2-13
adding 2-7
adding to VTG template 4-9
allow association to users, field described 2-11
allow latch, described 2-17
allow use in VTGs field, described 2-12
associated ops view, field described 2-16
associating to ops views 2-23
associating user with 3-28
associating with user 2-24
available 3-48
busy 2-6
changing status 2-20
channel color, field described 2-18
channel name, described 2-9

deleting 2-27
deleting from a channel group 2-35
described 2-2
disabled status 2-13
disabling 2-20
editing information 2-8
enabled status 2-13
enable latch, field described 2-17
enable VAD, field described 2-17
enabling 2-20
inactive status 2-13
in VTG template 4-8
listen only, field described 2-18
location 2-14
location, field described 2-14
mixing secure and non-secure in VTG 4-9
multicast address 2-15
multicast address, field described 2-15
multicast address port 2-15
multicast address port, field described 2-15
not present 2-7
preferred codec, described 2-10
removing 2-27
removing from a channel group 2-35
RX mute during PTT, field described 2-17
search for in VTG window 4-35
secure 2-6
secure, field described 2-10
status 2-13
type 2-14
type, field described 2-14
unavailable 2-7
unavailable for VTG 4-32
viewing associations 2-26
viewing information 2-8
Channel dashboard
elements 10-5
overview 10-5
channel group
adding 2-30
adding to VTG template 4-9
associated ops view, field described 2-32
associated VTG 2-35
associated VTG status 2-35
associating ops views to 2-36
channels in 2-2
deleting 2-37
deleting a channel from 2-35
described 2-2
editing information 2-31
name 2-32
removing 2-37
removing a channel from 2-35
viewing associations 2-34
viewing information 2-31
channel name 2-9
channel statistics log file 3-18, 3-20
Cisco IOS documentation xxii

Cisco IPICS
Administration Console 1-7
database
backing up 9-3
logs 9-19
restoring 9-12
deployment options 1-3
getting started 1-2
hardware components 1-3
initial configuration 1-2
IP multicast address guidelines for 2-51
logging in to 5-1
Login window 5-1
overview 1-1, 1-3
role 1-6
server 1-4
setting up 1-2
software components 1-3
Cisco IPICS policy engine
See policy engine
Cisco IPICS server
Administration Console 1-7
described 1-4
usage guidelines 1-8
Cisco IPICS service
about B-1
configuring for Cisco Unified CallManager B-2
configuring for Cisco Unified CallManager Express B-3
subscribing to B-4
using B-5
Cisco IP Interoperability and Collaboration System
See Cisco IPICS
Cisco Land Mobile Radio (LMR) documentation xxi
Cisco router
configuring as SIP provider 8-46
function in a Cisco IPICS deployment 1-6
Cisco Security Agent documentation xxii
Cisco Unified CallManager
configuring as SIP provider 8-42
configuring Cisco IPICS service for B-2
documentation xxi
function in a Cisco IPICS deployment 1-6
Cisco Unified CallManager Express, configuring Cisco IPICS service for B-3
Cisco Unified CallManager Express documentation xxi
Cisco Unified IP Phone
accessing Cisco IPICS service from B-5
allow latch 3-19
audio 3-19
dial login for 3-13
digit ID 3-14, 5-6
digit password 3-14
disable 3-15
documentation xxi
enable 3-15

latching 3-21
listen only 3-19, 3-21
managing for user 3-15
mute 3-15
subscribing to Cisco IPICS service B-4
unmute 3-15
user in VTG 4-21
using as a PTT device B-1
cluster view daemon, trace file 8-4
codec 2-10, 8-37
communications preferences
configuring 3-24
described 3-23
managing 3-23
configuring
Cisco IPICS 1-2
controllers A-6
RMS A-2
configuring Cisco IOS Express as SIP provider 8-46
configuring RMS security features A-2
connection type, multicast address 2-50, 2-54
controllers
configuring T1/E1 controllers A-5
on RMS 2-62
copying a user 3-6
customized script prompts
codec 8-17
deleting 8-19
described 8-16
downloading 8-18
renaming 8-19
uploading 8-17
viewing list of 8-16
Customized Script Prompts window 8-16

D

Dashboard window, overview 10-2
database
backing up 9-3
choosing a backup destination 9-11
described 9-22
exporting 9-21, 9-23
importing 9-26
manually starting database server 9-36
options
changing 9-9
default 9-9
options for restoring 9-13
restoring 9-12
troubleshooting a backup procedure 9-30
troubleshooting a restore procedure 9-30
Database Management window
overview 9-3
tabs inside of 9-3
deactivated
RMS 2-63
RMS status 2-61

VTG 4-20
DEBUG-level error messages 10-14
debug log file 3-18, 3-20
debug trace level 8-4
default language folder 8-11
deleting
action from policy 7-15
alert tones 2-118
channel 2-27
channel from a channel group 2-35
channel group 2-37
languages 8-13
locations 2-47
multicast address 2-55
PMC versions 2-112
policy 7-22
RMS 2-69
skins 2-121
spoken names prompts 8-29
trigger from policy 7-19
user 3-41
user group 3-50
VTG template 4-16
deployment, of Cisco IPICS 1-3
diagnostic information
downloading 10-11
viewing 10-8
Diagnostics window
diagnostic summary pane, described 10-11
elements 10-8
overview 10-2, 10-8
dial engine
codec 8-37
described 8-1
parameters 8-36
services
obtaining information about 8-2
status 8-3
trace file 8-4
Dial Engine drawer, accessing 8-1
dial engine script
See scripts 8-30
dial-in floor 7-31
dialing out to participants in an active VTG 4-29
dial-in phone
disable 3-15
enable 3-15
listen only 3-19, 3-21
managing for user 3-15
mute 3-15
unmute 3-15
dial login
configuring 3-13
described 3-13
Dial Login tab 3-14
dial-out action 7-8, 7-13
dial preferences
configuring 3-24

described 3-23
order of 3-27
dial prefix 8-39
digit ID 3-14, 5-6
digit password (PIN) 3-14, 5-7
direct dial
adding numbers 8-39
deleting numbers 8-41
described 8-37
dial prefix 8-39
updating numbers 8-40
viewing information about numbers 8-40
viewing list of numbers 8-38
Direct Dial Management window 8-38
direct two-way channels 3-30
disable
audio 3-19
Cisco Unified IP Phone 3-15
dial-in phone 3-15
end device 3-15
listen only 3-21
PMC 3-15
voice activation detection (VAD) 3-21
disable audio, in user profile 5-9
disabled channel 2-13
disabled user 3-38
disable PMC activity log upload, setting
described 2-103
disable RMS comparator, setting
described 2-93
disabling
latch in User Details window 4-26
PMC attributes in an active VTG 4-29
user 3-38
dispatcher role
described 1-7, 3-12
responsibilities 4-1
documentation
Cisco IOS xxii
Cisco Land Mobile Radio (LMR) xxi
Cisco Security Agent xxii
Cisco Unified CallManager xxi
Cisco Unified IP Phones xxi
downloading
activity logs 2-85
archived activity logs 2-88
PMC 5-2
DS0
destination 2-67
disabling 2-68
enabling 2-67
in loopback 2-67
source 2-67
status 2-67
ds0 groups
configuring ds0 groups A-6
dspfarm
calculating DSPs A-17
checking configuration A-16

DSP resource pool A-17
enabling A-18
DSPs A-17
dump
memory trace 8-8
threads trace 8-8

E

E1 timeslots A-7
e-mail
address of user 3-12
notification preference 3-23, 3-24
enable
Cisco Unified IP Phone 3-15
dial-in phone 3-15
end device 3-15
listen only 3-21
PMC 3-15
voice activation detection (VAD) 3-21
enabled
channel 2-13
user 3-38
enable voice activity detection (VAD), field described 2-17
enabling
latch in User Details window 4-26
PMC attributes in an active VTG 4-29
user 3-38
end device
audio 3-19
described 3-15
disable 3-15
enable 3-15
listen only 3-19, 3-21
managing for user 3-15
mute 3-15
unmute 3-15
ERROR-level error messages 10-14
event, also called active VTG 4-2
executed policy, information about 7-22
executing policy, information about 7-22
expiration date, of password 3-10

F

floor, for dial-in 7-31

G

G.711 2-10
G.729 2-10
gateway 1-5
General Information tab 3-9, 3-13
Get Logs from PMC 3-20
guidelines
for using IP multicast addresses with Cisco IPICS 2-51
managing active VTGs 4-17
managing VTG templates 4-8

multicast address 2-51
server usage 1-8

H

hardware components, of Cisco IPICS 1-3
help, in Administration Console 1-16
host name, of RMS 2-61

I

icons
in Channels and Channel Groups windows 2-6
in Users window 3-4, 3-46
in Virtual Talk Groups window 4-6
ID, of user 3-7
idle status, for multicast address 2-50, 2-54
IN_SERVICE 8-3
inactive channel 2-13
INFO-level error messages 10-14
Informix database, manually starting 9-36
INITIALIZING 8-3
invitation policy type
adding 7-14
described 7-6
updating 7-14
invitation type policy, actions in 7-8
invite to VTG action 7-8
IP address, of RMS 2-61
IP address selection guidelines A-8
ipics.log
downloading 10-16
error types 10-14
IP multicast address, guidelines for using with Cisco IPICS 2-51

L

languages
adding 8-12
default folder 8-11
default language folder 8-11
deleting 8-13
for prompts 8-11
for scripts 8-11
naming requirement 8-11
of TUI prompts 7-29
renaming 8-12
viewing list of 8-11
Languages window 8-11
latch
allow 3-19
disable 3-21
enable 3-21
license
described 2-72
for policy engine 7-1
managing a Cisco IPICS 2-72
summary 2-73

time-bound, described 2-77
usage per ops view 2-76
License dashboard
elements 10-7
overview 10-6
license file, uploading 2-78
listen only
channel 2-18
field in user profile 5-9
in PMC tab 3-19
LMR gateway 1-5
location
adding 2-45
associations 2-40
deleting 2-47
described 2-38
multicast address 2-50, 2-55
of RMS 2-60
predefined 2-38
RMS 2-65
summary of access types and connections 2-43
user 5-8
viewing or editing 2-46
locking a user account 3-38
log files
downloading 10-16
downloading system 10-16
in System Logs window 10-13
location 3-18, 3-20
managing activity 2-83
obtaining 3-19
PMC 3-15, 3-18
log level, setting 3-20
logs, managing activity 2-83
loopback
configuring 2-66
creating 2-66
disabling DS0 in 2-68
DS0 destination 2-67
DS0 source 2-67
DS0 status 2-67
enabling DS0 in 2-67
number 2-67
on RMS 2-62
removing 2-69
state 2-67
viewing information about 2-66, 2-67

M

Management Information Base (MIB)
network and system status MIBs 10-20
Request for Comments (RFC) documents 10-24
managing activity log options per ops view 2-89
managing PMC from Associations tab 3-21
maximum activity logs, setting described 2-94
MCS servers documentation xxi

member, adding to user group 3-45
merging RMS configuration 2-70
multicast address
  adding address to multicast pool 2-51
  adding a sequence of addresses to multicast pool 2-52
  address 2-54
  address and port 2-49
  assignment 2-51
  channel 2-15
  connection type 2-50, 2-54
  conventions 2-15, 2-51, 2-54
  deleting 2-55
  editing information 2-53
  guidelines 2-51
  in multicast pool 2-47
  location 2-50, 2-55
  port 2-54
  recommended range 2-51
  status 2-50, 2-54
  used by 2-50, 2-55
  viewing information 2-53
multicast communications guidelines 2-51
multicast domain 2-38
multicast pool
  adding multicast address to 2-51
  deleting multicast address from 2-55
  described 2-47
Multi-Purpose type policy
  trigger 7-16
multi-purpose type policy
  actions in 7-8, 7-10
  activating 7-21
  adding 7-9
  described 7-6
  updating 7-9
mute
  Cisco Unified IP Phone 3-15
  dial-in phone 3-15
  end device 3-15
  PMC 3-15
  PMC user in a VTG 4-23
My Profile window, described 1-12

N

name
  of user 3-10
  of user group 3-49
name, of user 3-7
New Users window 3-6
notification action 7-8
notification preferences
  configuring 3-24
  described 3-23
notifying participants in an active VTG 4-29
no voice resources 2-7

O

old digit password, changing 5-7
online help, accessing 1-16
operational, RMS status 2-61
Operational Views
  See ops views
operator role
  described 1-7, 3-12
  responsibilities 3-1
ops view administrator role, described 1-7, 3-12
ops views
  accessible to 6-8
  affecting VTGs 6-16
  allocating dial ports, described 6-29
  assigning to user 6-31
  associated 3-35
  associating channel groups with 2-36
  associating channels 6-32
  associating channels or channel groups 6-32
  associating to channels 2-23
  associating user group with 3-47
  associating user with 3-35
  available 3-35
  belongs to 6-7
  benefits 6-6
  caveats 6-11
  channels 6-32
  creating 6-5
  determining dial port allocation 6-31
  dial port pools 6-29
  overview 6-1
  resources 6-6
  system 6-2
  to which user belongs 3-34
  to which user group belongs 3-47
  understanding VTGs 6-13
  user roles 6-9
  viewing details 6-25
  viewing resources 6-23
Ops View to User Association window 3-35
Options window 2-91
order, of dial preferences 3-27
OUT_OF_SERVICE 8-3

P

pager
  notification preference 3-23, 3-24
PARTIAL_SERVICE 8-3
participant
  adding to VTG 4-21
  in VTG 4-20
  removing from VTG 4-21
password
  Apply User Account Lockout setting 2-101
  Apply User Password Expiration setting 2-98
  changing 5-4
  expiration date 3-10

Failed Password Attempt Expiration Hours setting 2-103

Maximum Invalid Login Attempts Allowed setting 2-102

Minimum Digit Password Length setting 2-95

Minimum Lower Case Letter Count setting 2-96

Minimum Numeric Character Count setting 2-97

Minimum Password Length setting 2-95

Minimum Special Character Count setting 2-97

Minimum Upper Case Letter Count setting 2-96

Password Expiration Notification setting 2-100

Password Expiration setting 2-99

Password History Count setting 2-98

RMS 2-65

user 3-7, 3-10

phone

associated 3-32

associating user with 3-31

available 3-32

Phone Associations window 3-32

phone service B-1

PIN, digit password 3-14

PIN, digit password in user profile 5-7

PMC

adding alert tone sets 2-115

advanced permissions 3-19

allow latch 3-19

audio 3-19

authentication log file 3-18, 3-20

automatic update 2-106

changing the state of versions for updates 2-110

channel statistics log file 3-18, 3-20

creating alert tone sets 2-113

debug log file 3-18, 3-20

deleting versions 2-112

described 1-4

direct two-way channels 3-30

disable 3-15

downloading current version 5-19

enable 3-15

forced update 2-110

information status in VTG 5-9

installer, generating 2-123

latching 3-21

listen only 3-19, 3-21

log files 3-15, 3-18, 3-19, 3-20

log level 3-20

managing for user 3-15

managing the configuration 2-122

mute 3-15

skins 2-119, 2-120

unmute 3-15

updating 2-106

uploading and managing skins 2-119

user interface log file 3-18, 3-20

user in VTG 4-21

voice activation detection (VAD) 3-21

PMC activity log update, setting frequency 2-106

PMC alert tones

See alert tones

PMC installer, generating 2-123

PMC log upload frequency, setting described 2-104

PMC send logs on rollover, setting described 2-105

pmcsetup.exe 2-122

PMC skins

See alert tones

See skins

PMC tab 3-19

PMC update poll, setting described 2-103

PMC versions

changing the state 2-110

uploading 2-109

Policies window

described 7-4

displaying 7-4

policy

action,*See* action

activating 7-21

adding 7-6

associated 3-33

associating user with 3-32, 7-19

available 3-33

definition 7-1

deleting 7-22

deleting action from 7-15

deleting trigger from 7-19

executed 7-22

executing 7-22

invitation type

actions in 7-8

adding 7-14

described 7-6

updating 7-14

Multi-Purpose type

updating 7-9

multi-purpose type

actions in 7-8

adding 7-9

described 7-6

ops view guidelines 7-5

re-activating 7-26

scheduled 7-25

system resources for 7-6

trigger 7-16

type 7-8

viewing information about 7-22, 7-25

Policy Associations window 3-33

policy engine

license requirement 7-1

Policies window 7-4

policy, *See* policy 7-1

roles that can access 8-1
SIP provider 8-41
tracing 8-4
Policy Management drawer, accessing 7-1
pop-up windows 1-10
port
channel 2-15
conventions 2-15, 2-53, 2-54
multicast address 2-54
preferences, system, setting in Options window 2-91
preferred codec 2-10
prompts
customized script, *See* customized script prompts
described 8-1
languages 8-11
languages, *See* language
managing 8-10
repository 8-10
spoken name, *See* spoken name prompts
standard script, *See* standard script prompts
PTT channel
See channel
PTT channel group
See channel group
Push-to-Talk Management Center
See PMC

R

re-activate
action 7-26
policy 7-26
VTG 4-32
recording, spoken names prompts 8-25
recovering, system administrator 3-40
recurrence, of trigger 7-17, 7-18
refreshing, Administration Console 1-10
removing
channel 2-27
channel from channel group 2-35
channel group 2-37
RMS 2-69
user 3-41
user group 3-50
VTG template 4-16
repository 8-10, 8-30
Request for Comments (RFC) documents used with SNMP 10-24
required information, in Cisco IPICS windows 1-8, 1-13
rerecording, spoken names prompts 8-25
restoring a backed-up database 9-12
RMS
activating 2-59, 2-63
adding 2-64
calculating DSPs A-17
configuring A-2

configuring security features A-2
configuring T1/E1 controllers, interfaces, and voice parameters A-9
connectivity guidelines A-6
controller 2-62
controllers A-6
deactivated status 2-61, 2-63
deactivating 2-59, 2-63
deleting 2-69
described 1-5
ds0 groups A-6
dspfarm configuration A-16
E1 timeslots A-7
editing information 2-59
host name 2-61
IP address 2-61
IP address selection
  Ethernet interface A-8
  guidelines A-8
  Loopback0 interface A-8
  Vif1 interface A-9
location 2-60
loopback 2-62
managing 2-56
managing configuration 2-70
merging configuration 2-70
name 2-60
operational status 2-61
removing 2-69
status 2-61
  status of routers in RMS window 2-57
  stopping state 2-63
  stopping status 2-61
  T1 timeslots A-6
  unconfigured status 2-61
  unreachable status 2-61
  updating configuration 2-70
  updating information in Cisco IPICS 2-70
  viewing information 2-59
RMS dashboard
  elements 10-8
  overview 10-7
RMS polling frequency, setting interval 2-93
role
  all 1-7, 3-12
  assigning 3-12
  changing 3-12
  described 1-6, 3-12
  dispatcher 1-7, 3-12, 4-1
  operator 1-7, 3-1, 3-12
  ops view administrator 1-7, 3-12
  system administrator 1-7, 2-1, 3-12
  user 1-6, 5-1
Roles 5-5
router
  See RMS
router media service
  See RMS
RX mute during PTT on channel 2-17

S

scheduled policy, information about 7-25

scripts

- adding 8-31
- changing information about 8-32
- deleting 8-33
- described 8-1
- dial engine 8-30
- IppeDialin 8-30
- IppeDialout 8-30
- IppeRecording 8-30
- languages 8-11
- managing 8-30
- repository 8-30
- system 8-30
- viewing information about 8-32
- viewing list of 8-31

searching in Virtual Talk Groups window 4-34

secure channel 2-6, 2-10

server, Cisco IPICS 1-4

server logs, viewing 10-13

server usage guidelines 1-8

Serviceability drawer, overview 10-1

services, obtaining information about 8-2

setting up Cisco IPICS 1-2

short message service (SMS), notification preference 3-23, 3-24

Simple Network Management Protocol (SNMP)

- configuring an MIB browser 10-25
- configuring an SNMP management console 10-25
- Management Information Base (MIB) objects
  - described 10-18
- support 10-18

SIP, configuring for Policy Engine 8-34

SIP provider

- Cisco IOS 8-46
- Cisco router 8-46
- Cisco Unified CallManager 8-42
- configuring for Cisco IPICS 8-41
- described 8-41

skins

- adding 2-120
- viewing or editing 2-120

SNMP

- *See* Simple Network Management Protocol (SNMP)

software components, of Cisco IPICS 1-3

specifying order 5-13

spoken names prompts

- changing information about 8-28
- deleting 8-29
- described 8-20
- downloading 8-24
- for user 3-36
- recording 8-25
- replacing .wav file 8-25
- rerecording 8-25

uploading 8-22
viewing list of 8-21
Spoken Names window 8-21
standard script prompts
described 8-14
uploading 8-15
viewing list of 8-14
Standard Script Prompts window 8-14
status
channel 2-13
DS0 2-67
multicast address 2-50, 2-54
Status Details window 8-3
stopping, RMS status in RMS window 2-61
sub-VTG 4-8
system administrator role
described 1-7, 2-1, 3-12
responsibilities 2-1
System dashboard, overview 10-3
system logs
downloading 10-16
entry types 10-14
overview 10-13
viewing 10-13
System Logs window
described 10-2, 10-13
log entry types 10-14
system preferences, setting in Options window 2-91
system status, monitoring 10-13

T

T1/E1 controller configuration A-5
T1 timeslots A-6
tab
Address Information 3-11
Associations 3-22
Dial Login 3-14
General Information 3-9, 3-13
PMC 3-19
telephony user interface
See TUI
time out, period for Administration Console 1-16
tone broadcast wave files
See alert tones
trace
advanced activities 8-8
cluster view daemon 8-4
configuring number of trace files 8-5
configuring size of trace files 8-5
debug 8-4
default levels 8-6, 8-8
described 8-4
dial engine 8-4
dump memory trace 8-8
dump threads trace 8-8
facilities 8-4, 8-7
files 8-4
interpreting trace files 8-10

levels 8-4, 8-6

maximum size of all trace files on systems 8-5

obtaining trace files 8-9

recommendations for 8-5

XDebug (extended debug) 8-4

TRACE-level error messages 10-14

trigger

adding 7-16

definition 7-1

deleting 7-19

overview 7-16

recurrence 7-17, 7-18

updating 7-16

viewing 7-16

TUI (telephony user interface)

accessing 7-28

activities 7-27

described 7-27

dial-in floor 7-31

dial login for 3-13

digit ID 3-14

general guidelines 7-29

guidelines for using 7-28

logging in 7-28

menu guidelines 7-30

PIN 3-14

speaking 7-31

type, channel connection 2-14

U

unavailable channel 2-7

unconfigured, RMS status 2-61

understanding 6-29

Activity Log Management window 2-84

channel and channel group icons 2-6

Channels window 2-3

icons in Virtual Talk Groups window 4-6

Ops View window 6-3

RMS window 2-57

Virtual Talk Groups window 4-3

unlocking a user account 3-38

unmute

Cisco Unified IP Phone 3-15

dial-in phone 3-15

end device 3-15

PMC 3-15

unmuting PMC user in a VTG 4-23

unreachable, RMS status 2-61

updating RMS configuration 2-70

uploading

license file 2-78

PMC versions 2-109

standard script prompts 8-15

used by field, for multicast address 2-50

user

adding 3-6

adding communications preferences in user profile 5-10

adding to VTG template 4-9
address
  street, of user 3-11
address information 3-11
associating channels with 2-24
associating channel with 3-28
associating ops view with 3-35
associating phone with 3-31
associating policy with 3-32, 7-19
associating user with 3-30
changing information in user profile 5-2
channel association 5-15
copying 3-6
default location 3-14
deleting 3-41
deleting communications preferences in user profile 5-10
described 3-1, 3-2
dial preferences 5-13
digit ID 3-14
digit password (PIN) 3-14
digit password (PIN) field, described 5-7
disabled 3-38
downloading PMC 5-19
editing communications preferences in user profile 5-10
enabled 3-38
general information 3-9
in VTG template 4-8
list of VTGs in which is a participant 3-36
locking account 3-38
managing associations 5-14
managing communications preferences 5-10
managing profile 5-2
name 3-7, 3-10
ops view for 3-34
password 3-10
PIN 3-14
recovering deleted 3-40
recovering system administrator 3-40
removing 3-41
search for in VTG window 4-35
specifying order of dial preferences 5-13
status 3-38
unlocking account 3-38
viewing associations 5-18
viewing communications preferences 5-10
user associations
  Channels tab, described 5-15
  Phones tab, described 5-17
  Policies tab, described 5-18
  Users tab, described 5-16
  Virtual Talk Groups tab, described 5-17
User dashboard
  elements 10-6
  overview 10-6
User Details window
  activities 1-12
  enabling or disabling latch for PMC user 4-26

user group
adding 3-43
adding members to 3-45
adding to VTG template 4-9
associating ops views with 3-47
changing name of 3-49
deleting 3-50
described 3-1, 3-41
list of VTGs in which is a participant 3-49
naming recommendation 3-44
ops view for 3-47
removing 3-50
User Groups window
accessing 3-42
described 3-42
user interface log file 3-18, 3-20
User Management drawer, accessing 3-1
user name of RMS field, described 2-62
user profile 5-2
account status field, described 5-5
address field, described 5-6
belongs to field, described 5-5
confirm password field, described 5-4
default location 5-8
dial preferences field, described 5-9
digit ID field, described 5-6
first name field, described 5-3
IPICS status field, described 5-5
last name field, described 5-3
new password field, described 5-4
notification preferences field, described 5-9
old digit password field, described 5-7
old password field, described 5-4
password expiration date field, described 5-5
PMC info field, described 5-9
roles field, described 5-5
user name field, described 5-3
user role
described 1-6
responsibilities 5-1
users
phone associations 5-17
user associations 5-16
VTG associations 5-17
Users window
accessing 3-3
described 3-3
using the PMC Installer window 2-122

V

viewing
activity logs 2-85
and downloading archived activity logs 2-88
and editing user associations, My Associations window 5-2
channel associations 2-26
ops view resources 6-23
or editing locations 2-46

or editing PMC alert tone sets 2-117
or editing PMC skins 2-120
user associations 5-18
virtual talk group
See VTG
Virtual Talk Group dashboard
elements 10-6
overview 10-5
voice activity detection
enable field 2-17
enabling on PMC 4-11, 4-14
VTG
activating 4-19
active 4-2, 4-17
adding participants 4-20
adding to VTG template 4-9
best practices 4-37
changing the status of 4-19
Cisco Unified IP Phone user in 4-21
deactivating 4-20
dialing out to participants in active 4-29
disabling latch in User Details window 4-26
disabling PMC attributes in active 4-29
empty 4-8
enabling latch in User Details window 4-26
enabling PMC attributes in active 4-29
guidelines for managing active 4-17
inactive 4-2
in which user group is participating 3-49
list in which user is participating 3-36
managing 4-2
managing active 4-17
multicast address used by 2-47
muting a PMC user 4-23
non-secure channel in 4-9
notifying participants in active 4-29
participant in itself 4-8
participants 4-20
PMC user in 4-21
reactivating 4-32
removing participants 4-20
search for in VTG window 4-35
secure channel in 4-9
seeing as user on Cisco Unified IP Phone B-8
sub-VTG 4-8
template
See VTG template
unavailable channel 4-32
unmuting a PMC user 4-23
VTG add participants action 7-8, 7-12
VTG search utility, using 4-34
VTG template
adding 4-10
adding channel 4-9
adding channel group 4-9
adding user 4-9
adding user group 4-9
adding VTG 4-9

channel in 4-8
deleting 4-16
described 4-2, 4-7
guidelines for managing 4-8
managing 4-7
modifying 4-14
removing 4-16
user in 4-8

W

WARN-level error messages 10-14

X

X, in Activate VTG Details area 4-33
Xdebug (extended debug) trace level 8-4