Cisco IPICS Server Administration Guide

Release 4.5(1)

Americas 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: 408 527-0883

Text Part Number: OL-23584-02

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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 © 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xix

Introduction xix

Audience xix

Organization xix

Related Documentation xxi

Cisco IPICS Documentation xxi

Cisco Unified Communications Manager Documentation xxi

Cisco Unified Communications Manager Express Documentation xxi

Cisco Unified IP Phone 7900 Series Documentation xxi

Session Initiation Protocol Documentation xxii

Cisco Security Agent xxii

Cisco IOS Documentation xxii

Obtaining Documentation, Obtaining Support, and Security Guidelines xxii

CHAPTER 1 **Introducing Cisco IPICS** 1-1

Getting Started 1-1

Cisco IPICS Terminology 1-3

Cisco IPICS Overview 1-3

Cisco IPICS Server 1-4

IPICS Dispatch Console 1-4

LMR Gateways 1-5

RMS 1-5

UMS 1-5

Networking Components 1-6
Cisco Unified Communications Manager Functionality 1-6
Audio Clients 1-6
Cisco IPICS Roles 1-7
Linux User Roles 1-8
Cisco IPICS Administration Console 1-8
Cisco IPICS Server Usage Guidelines 1-9
Browser Guidelines 1-10
Accessing the Administration Console 1-11
Exiting the Administration Console 1-12
Entering Required Information in Administration Console Windows 1-12
Using Search Windows 1-12
Navigating Item Lists 1-13
Getting Help in the Administration Console 1-14
Viewing Information about Cisco IPICS 1-14
Administration Console Timeout 1-14
Cisco IPICS Splash Screen 1-15
Splash Screen Installation Files 1-16
Installing and Configuring the Splash Screen 1-17
Uninstalling the Splash Screen 1-18

CHAPTER 2 **Performing Cisco IPICS System Administrator Tasks 2-1**
Managing PTT Channels and Channel Groups 2-2
Understanding the Channels Window 2-3
Adding a PTT Channel 2-5
Viewing and Editing Channel Details 2-5
Changing the Status of a PTT Channel 2-14
Understanding Association Attribute Behaviors 2-14
User-Channel Association Example 2-15

Associating PTT Channels to Ops Views 2-16
Associating Users to PTT Channels 2-17
Associating Radio Control Signals to PTT Channels 2-18
Viewing Channel Associations 2-19
Deleting a PTT Channel 2-20
Understanding the Channel Groups Window 2-20
Adding a Channel Group 2-22
Viewing and Editing Channel Group Details 2-23
Viewing Channel Group Associations 2-25
Removing a PTT Channel from a Channel Group 2-25
Associating Ops Views to Channel Groups 2-26
Deleting a Channel Group 2-27
Managing Locations 2-27
Predefined Cisco IPICS Locations 2-27
Location Associations 2-28
Summary of Access Types and Connections 2-31
Understanding the Locations Window 2-31
Adding a Location 2-32
Viewing or Editing a Location 2-32
Deleting a Location 2-33
Managing the Multicast Pool 2-33
Understanding the Multicast Pool Window 2-34
Guidelines for Using IP Multicast Addresses with Cisco IPICS 2-36
Adding Multicast Addresses 2-36
Viewing and Editing Multicast Address Information 2-37
Deleting a Multicast Address 2-38
Managing the RMS 2-39
Understanding the RMS Window 2-39
Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS 2-41

Editing or Viewing RMS Details 2-42
Deactivating or Activating an RMS 2-44
Adding an RMS 2-45
Viewing and Configuring Loopbacks 2-46
Viewing Detailed Information about a Loopback 2-46
Enabling DSOs in a Loopback 2-47
Disabling DSOs in a Loopback 2-47
Removing a Loopback 2-48
Deleting an RMS 2-48
Managing the RMS Configuration 2-49
Managing the UMS 2-50
Understanding the UMS Window 2-50
Viewing and Editing UMS Details 2-52
Enabling or Disabling a UMS 2-55
Repairing the UMS or Viewing a Mixing Session 2-55
Adding a UMS 2-56
Deleting a UMS 2-57
Managing Incidents 2-58
Understanding the Incidents Window 2-59
Viewing Incident Details 2-60
Changing the Status of an Incident 2-62
Downloading Archived Incidents 2-62
Deleting an Incident 2-63
Managing Licenses 2-63
Understanding the License Management Window 2-64
Understanding Time-bound License Behavior 2-68
Uploading a License File 2-68
Viewing Active Users 2-69
Managing Activity Logs 2-71
Understanding the Activity Log Management Window 2-72

Viewing and Downloading Activity Logs 2-73
Downloading Archived Activity Logs 2-74
Managing Activity Log Options Per Ops View 2-75
Managing Cisco IPICS Options 2-77
Managing IDC Versions 2-86
Understanding the IDC Versions Window 2-87
Uploading IDC Versions to the Cisco IPICS Server 2-88
Changing the State of IDC Versions 2-88
Deleting IDC Versions 2-89
Managing IDC Alert Tones 2-89
Creating an IDC Alert Tone Set 2-90
Adding IDC Alert Tone Sets 2-91
Viewing or Editing IDC Alert Tone Sets 2-92
Associating an Alert Tone Set to an Ops View 2-92
Deleting IDC Alert Tones 2-93
Managing the IDC Installer 2-93
Using the IDC Installer Window 2-94
Generating the IDC Installer 2-94
Managing IDC Regions 2-95
Understanding the IDC Regions Window 2-95
Adding IDC Regions 2-96
Viewing or Editing IDC Regions 2-97
Deleting IDC Regions 2-97
Configuring LDAP 2-98

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

Managing Users 3-1
Understanding the Users Window 3-2
Adding a User 3-4

Managing User Information 3-6
Managing General Information for a User 3-6
Managing Address Information for a User 3-7
Managing Roles for a User 3-8
Managing Dial Login Information for a User 3-9
Managing an End Device for a User 3-10
Managing Communications Preferences for a User 3-13
Associating Resources with a User 3-18
Associating PTT Channels with a User 3-18
Associating Phones with a User 3-19
Associating Policies with a User 3-20
Associating Radios with a User 3-22
Managing Ops Views for a User 3-24
Choosing an Ops View to Which a User Belongs 3-24
Associating Ops Views with a User 3-25
Managing Prompts for a User 3-25
Viewing Information about VTGs in which a User is a Participant 3-26
Managing User Status 3-26
Changing User Status 3-27
Locking or Unlocking a User Account 3-27
Recovering a Deleted System Administrator User 3-28
Deleting a User 3-28
Managing User Groups 3-29
Understanding the User Groups Window 3-29
Adding a User Group 3-31
Adding Members to a User Group 3-32
Managing Ops Views for a User Group 3-32
Choosing an Ops View to which a User Group Belongs 3-33
Associating Ops Views with a User Group 3-33
Changing the Name of a User Group 3-34

Viewing Information about VTGs in Which a User Group is a Participant 3-34
Deleting a User Group 3-35

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

Logging in to Cisco IPICS 4-1
Managing Your User Profile 4-2
Managing Communications Preferences 4-7
Viewing, Adding, Editing, or Deleting Notifications Preferences 4-8
Viewing, Adding, Editing, or Deleting Radio Preferences 4-9
Specifying the Order of Radio Preferences 4-10
Viewing or Updating IDC Dialer Preference 4-10
Viewing, Adding, Editing, or Deleting Dial Preferences 4-11
Specifying the Order of Dial Preferences 4-12
Managing User Associations 4-12
Viewing User Associations 4-15
Downloading the IDC 4-16

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

Managing VTGs 5-2
Understanding the Virtual Talk Groups Window 5-2
Managing Inactive VTGs 5-4
Guidelines for Managing Inactive VTGs 5-5
Adding a New VTG 5-6
Modifying a VTG 5-9
Deleting a VTG 5-11
Managing Active VTGs 5-11
Guidelines for Managing Active VTGs 5-11
Changing the Status of a VTG 5-12
Adding Participants to and Removing Participants from an Active VTG 5-13

Muting or Unmuting an IDC User in an Active VTG 5-15
Enabling or Disabling the Latch Feature in the User Details Window 5-17
Notifying and Dialing Out to Participants, and Setting IDC Attributes in an Active VTG 5-19
Reactivating a VTG 5-22
Using the Search Utility 5-23
Best Practices for Managing VTGs 5-25

CHAPTER 6 **Using the Cisco IPICS Policy Engine 6-1**
Policy Engine Overview 6-2
Policy Activities Available for Cisco IPICS Roles 6-2
Understanding the Policies Window 6-3
Adding a Policy 6-4
Managing Actions for a Policy 6-5
Understanding Notification Actions 6-6
Adding or Updating an Action for a Multi-Purpose Type Policy 6-8
Adding or Updating an Action for an Invitation Type Policy 6-11
Deleting an Action 6-12
Managing Triggers for a Policy 6-12
Adding, Viewing, or Updating a Trigger 6-13
Deleting a Trigger 6-14
Associating Users with a Policy 6-15
Activating a Policy Manually 6-16
Deleting a Policy 6-16
Viewing Information about Executing or Executed Policies 6-17
Viewing Information about Scheduled Policies 6-18
Re-Activating a Policy or an Action 6-19
Using the Policy Engine Telephony User Interface 6-20
Accessing the TUI 6-21

Guidelines for using the TUI 6-21
General Guidelines 6-21
Menu Guidelines 6-22

CHAPTER 7 **Configuring and Managing Cisco IPICS Operational Views 7-1**
Managing Cisco IPICS Ops Views 7-1
Understanding the Ops Views Window 7-2
Creating New Ops Views 7-3
Assigning Ops Views Resources 7-4
The Benefits of Using Ops Views 7-4
Understanding Ops Views Attributes 7-4
Understanding Ops Views User Roles 7-6
Understanding Ops Views Caveats 7-7
Understanding VTG and Sub-VTG Caveats 7-8
Understanding How Ops Views Affect VTGs 7-10
VTG Caveats 7-11
Performing Ops Views Tasks 7-11
Adding Ops Views 7-11
Viewing Resources That Belong To and are Accessible To Ops Views 7-15
Viewing Ops Views License Details 7-16
Managing Ops Views License Usage and Limits 7-16
Configuring Licenses for Ops Views Usage 7-18
Allocating Dial Ports for the Dial-In/Invite and Notification Features 7-18
Associating a User or User Group to an Ops View 7-20
Associating a Channel or Channel Group to an Ops View 7-20
Deleting Ops Views 7-21

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 8-3
Configuring the Number and Size of Dial Engine Trace Files 8-4
Configuring Trace Levels for Dial Engine Trace Files 8-4
Performing Advanced Tracing Activities 8-6
Obtaining Trace Files 8-7
Interpreting Trace Files 8-7
Managing Prompts 8-7
Managing Languages for Prompts 8-8
Viewing a List of Languages 8-8
Adding a Language 8-9
Renaming a Language 8-9
Deleting a Language 8-9
Managing Standard Script Prompts 8-10
Viewing a list of Standard Script Prompts 8-10
Uploading Standard Script Prompts 8-11
Managing Customized Script Prompts 8-11
Viewing a List of Customized Script Prompts 8-12
Uploading Customized Script Prompts 8-12
Downloading a Customized Script Prompt 8-13
Renaming a Customized Script Prompt 8-14
Deleting a Customized Script Prompt 8-14
Managing Spoken Names Prompts 8-14
Viewing a List of Spoken Names Prompts 8-15
Uploading Spoken Names Prompts 8-16
Downloading a Spoken Names Prompt 8-17
Recording a Spoken Name Prompt 8-18
Changing Information about a Spoken Names Prompt 8-20
Deleting a Spoken Names Prompt 8-20
Managing Dial Engine Scripts 8-21
Viewing a List of Dial Engine Scripts 8-21

Adding a Dial Engine Script 8-22
Viewing or Changing Information about a Custom Dial Engine Script 8-22
Deleting a Custom Dial Engine Script 8-23
Configuring SIP 8-24
Managing Cisco Unified Communications Manager for IP Phone Notifications 8-25
Viewing a List of Cisco Unified Communications Managers for IP Phone Notifications 8-25
Adding a Cisco Unified Communications Manager for IP Phone Notification 8-26
Viewing or Changing Information about a Cisco Unified Communications Manager Configured for IP Phone Notification 8-26
Deleting a Cisco Unified Communications Manager for IP Phone Notification 8-27
Configuring Text to Speech 8-28
Configuring Dial Engine Parameters 8-28
Managing Direct Dial Numbers 8-29
Viewing a List of Direct Dial Numbers 8-30
Designating a Dial Prefix for Direct Dial Numbers 8-30
Adding a Direct Dial Number 8-31
Viewing or Changing Information about a Direct Dial Number 8-31
Deleting a Direct Dial Number 8-32
Configuring the SIP Provider 8-32
Configuring Cisco Unified Communications Manager as the SIP Provider 8-32
Configuring a Cisco Unified Communications Manager Express as the SIP Provider 8-35

CHAPTER 9 **Managing Radios and Radio Descriptors 9-1**

Managing Radios 9-1
Tone Control Radio Overview 9-2

Serial Control Radio Overview 9-3
ISSI Gateway Overview 9-3
Understanding How Buttons Display on the IDC 9-4
Radio Frequency Channels 9-4
Configuring Channel Selectors and Control Sequences 9-4
Channel Selector Configuration 9-4
Tone Sequence Configuration (Tone Control Radios) 9-5
Caveats for Configuring Default Tone Sequences (Tone Control Radios) 9-6
Understanding the Radios Window 9-7
Adding a Radio 9-8
Viewing and Editing Radio Details 9-14
Associating a User to a Radio From the Radios Window 9-15
Enabling or Disabling a Radio 9-17
Deleting a Radio 9-18
Accessing and Using the Serial Radio Control Interface 9-18
Managing Radio Descriptors 9-21
Tone Descriptors 9-21
Tone Radio Descriptors 9-22
Radio Descriptor Format 9-23
Serial Radio Descriptors 9-25
Step 1: Create the Header 9-25
Step 2: Create the Body 9-25
ISSIG Descriptors 9-31
Caveats for IDC Operation 9-34
Understanding the Descriptors Window 9-35
Adding Descriptors 9-36
Updating Radio and Tone Descriptors 9-37
Deleting Radio and Tone Descriptors 9-38

CHAPTER 10 **Configuring and Managing Cisco IPICS High Availability** 10-1

Overview 10-1

Defining the Active and Standby Servers 10-1

Remote Server Locations Using Secure Communication 10-2

Server Failover Due to Local Critical Process Failure 10-2

Server Failover Due to Lost Heartbeat Message 10-2

Affect of Failover on IDCs and Connected Devices 10-2

Manually Failover and Recovering from a Split Brain Scenario 10-3

Configuring Cisco IPICS Servers for HA 10-3

Unconfiguring HA 10-6

HA Affect on the IDC Connections 10-6

HA Affect On Connected Devices 10-8

Synchronizing the Server Time on HA Servers 10-8

Performing a Manual Failover 10-9

Resolving a Split Brain Scenario 10-10

Overview of Reconciliation Methods 10-10

Method 1: Force the Secondary Server into Standby State 10-10

Method 2: Reconfigure High Availability 10-12

Method 3: Workaround 10-13

Reestablishing HA Configuration After Prolonged Server Downtime 10-14

CHAPTER 11 **Performing Cisco IPICS Database Backup and Restore Operations** 11-1

Overview of Cisco IPICS Database Backup and Restore Operations 11-1

Backing up the Cisco IPICS Server Database 11-2

Managing Database Backups from the Database Management Window 11-2

Performing a Manual Database Backup 11-3

Understanding Naming Conventions for Backup Directories 11-6

Changing the Default Settings for a Scheduled Database Backup 11-6

Guidelines for Choosing a Destination for Database Backups 11-8

Caveats for Remote Host Database Backups 11-9
Restoring Data from a Database Backup 11-9
Options for Using the Restore Procedure 11-10
Performing the Restore Procedure 11-10
Checking the Restore Status in the Database Log 11-12
Downloading and Viewing the Backup and Restore Logs 11-14
Troubleshooting Cisco IPICS Backup and Restore Procedures 11-15
Backing Up Data to a Remote Host Without scp Support 11-16
Restoring Data from a Remote Host Without scp Support 11-17
Unable to Log In to the Administration Console After Restoring Data 11-18
Unable to Retrieve a Database Backup from a Remote Host After Reinstalling Cisco IPICS 11-19
Cannot Access the Administration Console to Back Up and Restore the Cisco IPICS Database 11-20
Using CLI to Manually Back Up the Cisco IPICS Database 11-20
Using CLI to Manually Restore the Cisco IPICS Database 11-22

CHAPTER 12 **Understanding Cisco IPICS Serviceability and Diagnostic Information** 12-1
Understanding the Serviceability Drawer 12-1
Viewing the Information in the Dashboard Window 12-1
Understanding the System Dashboard 12-2
Understanding the Channel Dashboard 12-3
Understanding the Incident Dashboard 12-3
Understanding the Virtual Talk Group Dashboard 12-4
Understanding the User Dashboard 12-4
Understanding the License Dashboard 12-5
Understanding the RMS/UMS Dashboard 12-6
Viewing Cisco IPICS Server Diagnostic Information 12-6
Downloading the Server Diagnostic Information 12-8
Viewing the Cisco IPICS System Logs 12-9

Understanding the System Log Severities 12-10
Searching the System Logs By ERROR or WARNING Messages 12-11
Downloading System Logs 12-12
Viewing the Cisco IPICS RCS Logs 12-13
Understanding the RCS Log Severities 12-13
Searching the RCS Logs By ERROR or WARNING Messages 12-14
Downloading RCS Logs 12-15

APPENDIX A **Configuring the Cisco IPICS RMS Component** A-1
Configuring Security Features A-1
Connecting and Configuring T1/E1 Controllers A-4
RMS Connectivity Guidelines A-4
RMS IP Address Selection Guidelines A-6
Configuring T1/E1 Controllers, Interfaces, and Voice Parameters A-7

APPENDIX B **Using Cisco IPICS for External Notifications** B-1
Requirements for Implementing External Notifications B-1
Dial Engine B-1
Recipient List B-2
Message File B-3
Invoking External Notifications B-3
Invoking an External Notification by Sending an HTTP Request B-3
Invoking an External Notification by Posting a CAP XML File B-4
Retrieving External Notification Results B-5
Reviewing External Notification Results B-8
XML File Parameters for External Notifications B-8

APPENDIX C **Configuring System Event E-Mail Notifications** C-1
Understanding System Event E-Mail Notifications C-1

Enabling System Event E-Mail Notifications C-1

Disabling System Event E-Mail Notifications C-2

Changing System Event Trigger Values C-3

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

Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager D-1

Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager Express D-3

Moving the Logout Softkey Location on a Cisco Unified IP Phone D-3

Subscribing to the Cisco IPICS Service D-3

Using the Cisco IPICS Service on a Cisco Unified IP Phone D-4

APPENDIX E **Generating SSL Certificates** E-1

APPENDIX F **Multicast Recording** F-1

Overview F-1

Voice Recording F-1

Talker ID F-1

Radio Metadata F-2

Telephone F-2

APPENDIX G **Frequently Asked Questions** G-1

GLOSSARY

INDEX

Preface

Introduction

Cisco IPICS Server Administration Guide provides the information that you need to understand, configure, manage, and use the Cisco IP Interoperability and Collaboration System (*Cisco IPICS*), release 4.5(1).

This preface contains the following sections:

- Audience, page xix
- Organization, page xix
- Related Documentation, page xxi
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xxii

Tip If you use Cisco IPICS only for communicating with other users and do not require any other introductory material, go to Chapter 4, "Performing Cisco IPICS User Tasks," which provides information about logging into Cisco IPICS, downloading and setting up your IPICS Dispatch Console, 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 a*ll 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 5, “Performing Cisco IPICS Dispatcher Tasks”	Describes the tasks that the dispatcher can perform in the Admin Console.
Chapter 4, “Performing Cisco IPICS User Tasks”	Discusses how a user interacts with the Admin Console. Topics covered include logging in, downloading the IDC application, and setting up a user profile.
Chapter 7, “Configuring and Managing Cisco IPICS Operational Views”	Explains the Cisco IPICS operational view functions.
Chapter 6, “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, “Managing Radios and Radio Descriptors”	Explains how Cisco IPCIS uses radios and radio descriptors, and provides information about configuring and managing these items.
Chapter 10, “Configuring and Managing Cisco IPICS High Availability”	Explains the operation of Cisco IPICS high availability and explains how to configure and manage high availability.
Chapter 11, “Performing Cisco IPICS Database Backup and Restore Operations”	Describes the procedures that you perform to back up and restore the Cisco IPICS database.
Chapter 12, “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, “Using Cisco IPICS for External Notifications”	Describes how to set up Cisco IPICS for external notifications and how to invoke external notifications.
Appendix C, “Configuring System Event E-Mail Notifications”	Describes how to configure Cisco IPICS to send e-mail notifications to the system administrator when major system events occur.
Appendix D, “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 E, “Generating SSL Certificates”	Explains how to create an SSL certificate on a Cisco IPICS server to allow access from a Cisco IPICS Mobile Client.
Appendix F, “Multicast Recording”	Describes how third party voice recording systems can be set up to record multicast voice traffic from Cisco IPICS.
Appendix G, “Frequently Asked Questions”	Provides answers to frequently asked questions regarding Cisco IPICS.

Related Documentation

The following sections describe other Cisco IPICS documentation and documentation for related Cisco products.

Cisco IPICS Documentation

For more information about Cisco IPICS and the IDC application, see the latest releases of the following documentation:

- *Cisco IPICS Server Installation and Upgrade Guide*—This document describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system.
- *IPICS Dispatch Console User Guide*—This document describes how to install, configure, manage, and operate the IDC application
- *Release Notes for Cisco IPICS*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.
- *Cisco IPICS Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.

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

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

Cisco Unified Communications Manager Documentation

For information about Cisco Unified Communications Manager, see the documentation at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Express Documentation

For information about Cisco Unified Communications Manager Express, see the documentation at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html?q=&task=default

Cisco Unified IP Phone 7900 Series Documentation

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

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html?q=&task=default

Session Initiation Protocol Documentation

The dial engine, which controls the dial-in and dial-out functionality of the policy engine, uses the Session Initiation Protocol (SIP). For information about SIP, see the documentation at this URL:

http://www.cisco.com/en/US/tech/tk652/tk701/tk587/tsd_technology_support_sub-protocol_home.html?q=&task=default

Cisco Security Agent

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

http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html?q=&task=default

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, see the documentation at this URL:

http://www.cisco.com/en/US/products/ps6441/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

CHAPTER 1

Introducing Cisco IPICS

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

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

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

This chapter includes the following sections:

- Getting Started, page 1-1
- Cisco IPICS Terminology, page 1-3
- Cisco IPICS Overview, page 1-3
- Cisco IPICS Roles, page 1-7
- Linux User Roles, page 1-8
- Cisco IPICS Administration Console, page 1-8
- Cisco IPICS Splash Screen, page 1-15

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. Depending on your deployment, you may not need to perform each of these procedures.

For information about installing Cisco IPICS, see *Cisco IPICS Server Installation and Upgrade Guide* for release 4.5.

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	See the "Cisco IPICS Overview" section on page 1-3	❑
2. Learn about the roles that Cisco IPICS users can have	See the "Cisco IPICS Roles" section on page 1-7	❑
3. Learn about the Cisco IPICS Administration Console, including how to access this application	See the "Cisco IPICS Administration Console" section on page 1-8	❑
Set Up and Configure Cisco IPICS		
1. Configure RMS components, if needed	See Appendix A, "Configuring the Cisco IPICS RMS Component"	❑
2. Configure UMS components, if needed	See the "Managing the UMS" section on page 2-50	❑
3. Configure the ISSIG, if needed	See the "ISSI Gateway Overview" section on page 9-3	❑
4. Configure locations	See the "Managing Locations" section on page 2-27	❑
5. Configure the multicast pool	See the "Managing the Multicast Pool" section on page 2-33	❑
6. Configure radios and radio descriptors	See Chapter 9, "Managing Radios and Radio Descriptors"	❑
7. Create push-to-talk channels	See the "Managing PTT Channels and Channel Groups" section on page 2-2	❑
8. Determine user roles and add users	See the "Managing Roles for a User" section on page 3-8	❑
9. Create VTG templates	See the "Managing Inactive VTGs" section on page 5-4	❑
10. Ensure that the server is hosting the current version of the IDC	See the "Managing IDC Versions" section on page 2-86	❑
11. Configure the Cisco IPICS policy engine, if needed	See Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"	❑
12. Create operational views, if needed	See Chapter 7, "Configuring and Managing Cisco IPICS Operational Views"	❑
13. Set up Cisco Unified IP Phones, if needed	See Appendix D, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device"	❑
14. Configure Cisco IPICS for external notification actions, if needed.	See Appendix B, "Using Cisco IPICS for External Notifications"	❑
15. Configure high availability, if needed	See Chapter 10, "Configuring and Managing Cisco IPICS High Availability"	❑
16. Generate SSL certificates, if needed	See Appendix E, "Generating SSL Certificates"	❑

Cisco IPICS Terminology

This document uses a variety of terms to describe Cisco IPICS features and functions. Table 1-2 describes some of the common terms that you may see throughout this document.

Table 1-2 Cisco IPICS Terms

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

Cisco IPICS Overview

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

- Cisco IPICS server—Provides the core functionality of the Cisco IPICS system. For more information, see the "Cisco IPICS Server" section on page 1-4.
- IPICS Dispatch Console (IDC)—Standalone PC-based software application that provides PTT functionality so that users with a variety of communication devices can participate in the event. For more information, see the "IPICS Dispatch Console" section on page 1-4.
- LMR gateways—Provides radio network interoperability and application integration. For more information, see the "LMR Gateways" section on page 1-5.
- RMS—Enables a Cisco Dispatch Console to remotely attach to a VTG or channel, enables channels to be joined in VTGs, and performs other mixing functions. For more information, see the "RMS" section on page 1-5.

- UMS—An alternative to the RMS. For more information, see the "UMS" section on page 1-5.
- Networking components—Include switches, routers, firewalls, mobile access routers, and wireless access points and bridges. For more information, see the "Networking Components" section on page 1-6.
- Cisco Unified Communications Manager functionality—Provide voice interoperability between radio and non-radio networks. For more information, see the "Cisco Unified Communications Manager Functionality" section on page 1-6.
- Audio clients—Devices such as land mobile radios (LMRs) and Cisco Unified IP Phones that let users participate in VTGs. For more information, see the "Audio Clients" section on page 1-6.
- Cisco IPICS Mobile Client—Standalone application that runs on an Apple iPhone, provides access to an incident VTG and supporting media, and allows users to add journals, videos and pictures to an incident. For more information, see *Cisco IPICS Mobile Client for Apple iPhone Reference Guide*.

Cisco IPICS Server

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

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

IPICS Dispatch Console

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

You install the IDC on your PC after downloading the software from the Cisco IPICS server. For more information, see the "Downloading the IDC" section on page 4-16. After you install the application for the first time, Cisco IPICS automatically alerts you when new versions become available.

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

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

LMR Gateways

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

RMS

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

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

Table 1-3 lists which IPICS features are supported by RMS, UMS, or both.

Table 1-3 RMS and UMS Feature Support

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

UMS

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

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

- Improved multicast voice quality
- Creation of VTGs that are composed of diverse end points
- Bridges multicast and unicast users
- Proxy mixing for resource-constrained end points
- G.711 and G.729 transcoding services so that local IDCs, remote IDCs, and IP phones can participate in the same VTG

See Table 1-3 for a list of IPICS features that are supported or not supported by UMS.

Networking Components

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

Cisco Unified Communications Manager Functionality

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

Audio Clients

Audio clients are devices through which users participate in VTGs. They include IDC clients, LMR gateways, various models of the Cisco Unified IP Phone, mobile clients such as the Apple iPhone, and dial-in devices.

Cisco IPICS Roles

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

Table 1-4 describes the Cisco IPICS roles.

Table 1-4 Cisco IPICS Roles

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

Linux User Roles

Cisco IPICS supports the Linux user roles that Table 1-5 describes.

Table 1-5 Linux User Roles

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

Cisco IPICS Administration Console

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

This section includes the following topics:

- Cisco IPICS Server Usage Guidelines, page 1-9
- Accessing the Administration Console, page 1-11
- Exiting the Administration Console, page 1-12
- Entering Required Information in Administration Console Windows, page 1-12

- Using Search Windows, page 1-12
- Navigating Item Lists, page 1-13
- Getting Help in the Administration Console, page 1-14
- Viewing Information about Cisco IPICS, page 1-14
- Administration Console Timeout, page 1-14

Cisco IPICS Server Usage Guidelines

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

- The Cisco IPICS Administration Console contains the following tabs:
  - Server tab—Provides access to drawers and windows in which you perform Cisco IPICS administration and management activities. These activities include configuring and managing Cisco IPICS components, uploading licenses, managing the database, monitoring activity logs, setting system performance options, and monitoring system performance. You can also perform VTG, user, and IDC management operations.
  - Policy Engine tab—Provides access to drawers and windows in which you perform policy engine and dial engine administration and management activities. These activities include creating and managing policies, configuring SIP and dial engine parameters, managing prompts, and monitoring policy engine services, and managing tracing for the dial engine.
- Many of the Administration Console windows let you enter a variety of information. You might enter information by typing in fields, choosing from drop-down lists, or checking check boxes, depending on the window. An asterisk (*) next to a field, drop-down list, or check box indicates required information. You must provide this information before you can save your changes and exit the window.
- Most windows contain a **Save** button and a **Cancel** button. The **Save** button saves any changes that you make in a window and often closes the window. The **Cancel** button discards any changes that you have made and often closes the window.
- Many Cisco IPICS resources, such as channels, users, and VTGs, display in lists in the Administration Console. These lists include check boxes that you can check to select resources for which to perform certain functions. Most resource lists include a check box at the top of the list that allows you to select all resources at one time.
- Many of the Administration Console windows include drop-down lists. Some of these lists become available only after you perform certain functions. If you do not perform the required function, the drop-down list is dimmed to indicate that it is not available.
- For some resources, separate windows display in which you can take the following actions:
  - To move an item from one list to another list, click the item to highlight it and then click > or <, or double-click the item.
  - To move several items from one list to another list at one time, Shift+click or Ctrl+click to select the items and then click > or <.
  - To move all items from one list to another list at one time, click >> or <<.
- Cisco IPICS provides connection support for both multicast and unicast communications. Make sure that users are aware of the appropriate location information to use when they log in to Cisco IPICS.
- When configuring IP multicast addresses, Cisco strongly recommends that you configure IP multicast addresses that are only in the 239.192.0.0 to 239.251.255.255 range. This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in

a local domain. This address range is less likely to cause an addressing conflict in an existing multicast domain. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-36.

- When adding users, channels, user groups, channel groups, or VTGs, be aware that names within each category must be unique. For example, no two user names can be the same, and no two channel names can be the same, but a user name and a channel name can be the same.
- Users who are in the same multicast domain are also in the same Cisco IPICS location.
- To ensure that each Cisco IPICS server has use of resources on a dedicated RMS component, Cisco IPICS does not support the use of the same RMS component with use multiple Cisco IPICS servers. (In a high availability deployment, the primary and secondary Cisco IPICS server use the same RMS component because only one server is active at a time.)
- Cisco IPICS supports more than one RMS component 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 6, "Using the Cisco IPICS Policy Engine."
- All all time stamps that appear in the Cisco IPICS server Administration Console web interface in Greenwich Mean Time (GMT).

Browser Guidelines

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

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

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

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

Accessing the Administration Console

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

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

Procedure

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

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

The Authentication window displays.

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

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

User names and server hostnames are not case-sensitive.

Step 3 Click **Log In**.

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

You can perform a variety of activities in the User Details window. Table 1-6 describes these activities.

Table 1-6 User Details Window Activities

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

Exiting the Administration Console

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

Entering Required Information in Administration Console Windows

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

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

Using Search Windows

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

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

The following guidelines apply to Search or Search Results windows:

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

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

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

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

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

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

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

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

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

- To view the results in a results list at the bottom of a Search or a Search Results window, see the "Navigating Item Lists" section on page 1-13.

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

- To exit a Search or a Search Results window, take one of these actions:
  - Click the **OK** button—The window closes and then results that you checked are entered in the window that you return to.
  - Click the **Cancel** button—The window closes and the results that you checked are not in the window that you return to.

Navigating Item Lists

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

To view items in these lists, follow these guidelines:

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

- You can navigate pages of information in a list by using the following navigation controls at the bottom of the list:
  - Page field—To go to a specific page, enter the page number and press **Enter**.
  - |< (First Page button)—Displays the first page in the list. This button is not available when the first page is displayed.
  - < (Previous Page button)—Displays the previous page in the list. This button is not available when the first page is displayed.
  - > (Next Page button)—Displays the next page in the list. This button is not available when the last page is displayed.
  - >| (Last Page button)—Displays the last page in the list. This button is not available when the last page is displayed.

Getting Help in the Administration Console

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

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

Viewing Information about Cisco IPICS

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

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

Administration Console Timeout

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

To change the timeout period of your Cisco IPICS session or to disable it so that there is no timeout period, navigate to **Administration > Options** in the Administration Console and modify the value of the Cisco IPICS Session Timeout Period option. See the "Managing Cisco IPICS Options" section on page 2-77 for more information.

Cisco IPICS Splash Screen

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

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

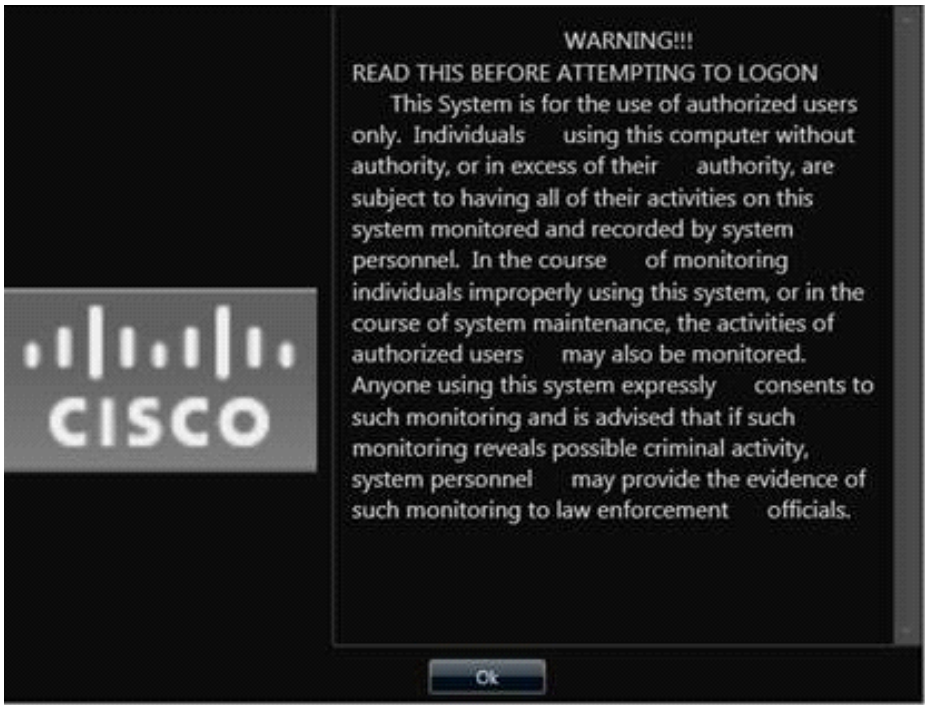
- IDC
- IPICS Administration Console
- Shell / CLI / SSH

Table 1-7 provides examples of how the splash screen can appear in the different clients:

Table 1-7 Customized Splash Screen Examples

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

Table 1-7 Customized Splash Screen Examples (continued)

Client	Default
IDC	

Splash Screen Installation Files

The splash screen feature is not configured from any GUI. Instead, the system administrator invokes a shell script called splash-install to configure it. Table 1-8 describes the files in the /opt/cisco/splash directory that are used to install and configure the splash screen.

Table 1-8 Contents of /opt/cisco/splash Directory

File	Purpose
splash-install	The splash installer
splash-reverse	The splash uninstaller
splash-reverse.sql	(Internal file. Do not edit.)
splash.png	The default splash image is a Cisco logo. Feel free to customize this file. It will get copied to the appropriate place on the IPICS server when the splash-install scripts runs. Keep the filename “splash.png”. If you rename it, or need to use a jpg instead, then you will need to also modify “splash_screen_url” found in the splash.sql file, and re-run splash-install. Suggested image dimensions: 300 x 300
splash.sql	(Internal file. Editing should not be necessary.)

Table 1-8 Contents of /opt/cisco/splash Directory (continued)

File	Purpose		
	Config_name	**Config_value**	**Description**
	splash_screen_message	(splash-install will insert the content of splash.txt here)	Optional customizable splash screen text. If present, IDC and browser will display the splash screen upon startup.
	splash_screen_url	/ipics_server/images/splash.png	Optional customizable splash screen image. If present, IDC and browser will display the splash screen upon startup. A relative URL is recommended (not beginning with http://hostname). If you use an absolute URL, it must be accessible by the IPICS server (e.g. if server is behind a firewall, images on external Internet sites won't work, so you may need to copy the image to the IPICS server.)
	splash_screen_timeout	0	Unused
splash.txt	The customizable splash screen text. The default value is as follows: WARNING!!! READ THIS BEFORE ATTEMPTING TO LOGON This System is for the use of authorized users only. Individuals using this computer without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.		

Installing and Configuring the Splash Screen

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

Procedure

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

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

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

cd /opt/cisco/splash

Step 3 Customize as needed:

a. Modify splash.txt as needed.

b. Replace splash.png with desired image.

- Keep the filename as splash.png.
- The suggested image dimensions are 300 x 300

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

run ./splash-install

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

- 268: Unique constraint (ipicsdba.config_pk) violated.
- 100: ISAM error: duplicate value for a record with unique key.

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

Step 6 Test by logging into the following clients:

a. IPICS Administration Console

b. IDC

c. SSH

Step 7 If you are not satisfied with the results:

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

run ./splash-reverse

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

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

Note

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

Uninstalling the Splash Screen

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

Procedure

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

ssh root@<ipics-server-address>

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

cd /opt/cisco/splash

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

run ./splash-reverse

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

CHAPTER 2

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 and radio channels. The system administrator also manages the Cisco IPICS licenses and IDC versions, monitors the status of the system, reviews log files, as needed, and creates operational views.

In addition, the system administrator is responsible for managing radios and radio descriptors, managing optional high availability, and performing backup and restore operations. For more information, see Chapter 9, "Managing Radios and Radio Descriptors," Chapter 10, "Configuring and Managing Cisco IPICS High Availability," and Chapter 11, "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 2-27
- Managing the Multicast Pool, page 2-33
- Managing the RMS, page 2-39
- Managing the UMS, page 2-50
- Managing Incidents, page 2-58
- Managing Licenses, page 2-63
- Viewing Active Users, page 2-69
- Managing Activity Logs, page 2-71
- Managing Activity Log Options Per Ops View, page 2-75
- Managing Cisco IPICS Options, page 2-77

- Managing IDC Versions, page 2-86
- Managing IDC Alert Tones, page 2-89
- Managing the IDC Installer, page 2-93
- Managing IDC Regions, page 2-95
- Configuring LDAP, page 2-98

For information about managing operational views in the Ops Views window, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

For information about managing database backup and restore operations in the Database Management window, see Chapter 11, "Performing Cisco IPICS Database Backup and Restore Operations."

Managing PTT Channels and Channel Groups

A PTT channel, also referred to as a channel, is a communications path that allows users to communicate with each other. A Cisco IPICS channel defines and describes the specific content stream of the channel regardless of the source of that content. Channel connections distinguish one content stream from another, and are determined by location.

A channel carries traffic to and from a VTG, a land mobile radio (LMR) gateway, an IDC, and an IP phone. Remote IDC users can connect to a channel by using a unicast SIP connection to an RMS component.

A channel can also refer to a radio control interface (radio or radio channel), which also has an audio stream. For information about managing radios in Cisco IPICS, see Chapter 9, "Managing Radios and Radio Descriptors."

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 2-5
- Viewing and Editing Channel Details, page 2-5
- Changing the Status of a PTT Channel, page 2-14
- Understanding Association Attribute Behaviors, page 2-14
- Associating PTT Channels to Ops Views, page 2-16
- Associating Users to PTT Channels, page 2-17
- Associating Radio Control Signals to PTT Channels, page 2-18
- Viewing Channel Associations, page 2-19
- Deleting a PTT Channel, page 2-20

Channel Group Management Tasks

- Adding a Channel Group, page 2-22
- Viewing and Editing Channel Group Details, page 2-23

- Viewing Channel Group Associations, page 2-25
- Removing a PTT Channel from a Channel Group, page 2-25
- Associating Ops Views to Channel Groups, page 2-26
- Deleting a Channel Group, page 2-27

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 2-20.

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 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; then, click **Go**.
Ops View drop-down list	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 indicates the unique identifier that is assigned to the channel.	See the "Viewing and Editing Channel Details" section on page 2-5 and the "Adding a PTT Channel" section on page 2-5

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 2-16
Secure field	This field indicates whether the channel is secure.	See the "Viewing and Editing Channel Details" section on page 2-5
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 2-5 and the "Adding a PTT Channel" section on page 2-5
Users field	This field indicates whether the channel is allowed to be associated to users to affect all endpoints such as the IDC 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 2-14
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 2-5
Delete button	Click this button to delete the specified channel(s).	See the "Deleting a PTT Channel" section on page 2-20
Change Status drop-down list	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 2-14
Associations button	Click this button to view associations for the specified channel.	See the "Associating Users to PTT Channels" section on page 2-17, the "Viewing Channel Associations" section on page 2-19, and the "Associating Radio Control Signals to PTT Channels" section on page 2-18
Display Controls		
Rows per page drop-down list	Specifies the number of rows of channels that are included in a channels list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays channels on a specific page.	
|< (First page) button	Displays the first page of the channels list.	
< (Previous page) button	Displays the previous page of the channels list.	
> (Next page) button	Displays the next page of the channels list.	
>| (Last page) button	Displays the last page of the channels list.	

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 "Adding a Location" section on page 2-32.

To add a new channel, perform the following procedure:

Procedure

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

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 2-5.

Step 4 Enter appropriate information in the Ops Views fields as described in Chapter 7, "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 the **Configuration > Channels** window.

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 2-2 provides descriptions of the fields in the General tab.

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

Table 2-2 General Tab Fields in Channels Window

Field	Description
Channel Information	
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 use it, or for a particular geographic region (for example *Fire Department* or *North Area*). **Note** The IDC truncates the channel name if the name includes more characters than the IDC can display.
Short Name	This field represents the condensed name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: ". , _ ' # ( ) / :_".
Description	(Optional) This field allows you to enter a description for this channel.
Secure Channel	This drop-down list 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, an active IDC user is associated with this channel, or if a user has activated this channel via an IP phone or PSTN phone. To make the field editable, either disable the channel, or deactivate the VTG in which the channel is a participant.
Allow association to users	This check box allows you to indicate whether this channel is available to all Cisco IPICS users. Use this option 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), the channel does not display as available to users in the User window and it is not available on the IDC. In addition, the User tab, in the channel Association window, does not display. **Note** If you change the channel status such that a channel that was previously associated with a user is no longer associated with a user, Cisco IPICS automatically removes the channel associations from the users. This check box is checked by default upon creation of the channel.

Table 2-2 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. Use this setting to prevent certain channels from being included in a VTG. For example, an IDC user who interacts with a another user may wish to hear all the call progress tones that the other user's handset generates, to give feedback when a radio channel is available. These types of progress tones can be assigned to this 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 its use 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 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.
Status *Display only*	This field displays one the following channel states: • Active—Channel in use by an active VTG. • Enabled—Channel is available (channel can be connected to a VTG) and IDC clients can use the channel. • Disabled—Channel is not in use and IDC 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 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Media Connection Assignments	
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. Choose one of the following options from the drop-down list: • **Multicast**—If you choose a multicast connection type, you must also configure the location, IP address, port. and codec fields for the multicast connection. For more information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-36. • **Tone Remote Radio**—If you choose a tone remote radio device type, you must also choose a radio from the Radio drop down list and a channel selector from the Channel Selector drop-down list. The Tone Remote Radio options appear only if you have configured one or more tone control radios and have enabled one or more channel selectors for a tone control radio. For more information, see the "Tone Control Radio Overview" section on page 9-2. • **Pooled Radio**—If you choose a pooled radio device type, you must also choose a descriptor from the Descriptor drop down list and a channel selector from the Channel Selector drop-down list. The Pooled Radio options appear only if you have enabled one or more serial control radios to serve as a pooled resource and have enabled one or more channel selectors for a pooled radio. For more information, see the "Serial Control Radio Overview" section on page 9-3. • **ISSIG**—If you choose an ISSIG (ISSI Gateway) device type, you must also configure the Multicast address for the channel media (media address) and the port for channel media. You must also choose the ISSI Gateway and selector (P25 group on which to talk) to use for the channel. The ISSIG options appear only if you have configured one or more ISSI Gateways.

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

Field	Description
Location	This field displays when you choose a multicast connection type from the Type drop-down list. Channels or users who are associated with the same location are reachable within a multicast network boundary. Therefore, users who are in the same multicast domain are also in the same Cisco IPICS location. Remote, SIP-based users are not in the same location as multicast users. Remote users connect by establishing connectivity with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user. **Note** Channels achieve media connectivity by being mapped to a multicast address and port in a location. A channel can be assigned to multiple locations. In this case, a channel can have more than one media connection. The media connection 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 12-1 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 2-27 for more detailed information about how to configure locations.
Address	This field displays when you choose a multicast connection type from the Type drop-down list. 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 2-36. Two channels in the same location cannot have the same multicast address. See the "Managing Locations" section on page 2-27 for more detailed information about locations.
Port	This field displays when you choose a multicast connection type from the Type drop-down list. This field specifies the multicast address port number, in the corresponding location, that is used to connect to this channel. **Note** This value must be an even number in the range of 21000 through 65534. Cisco IPICS does not allow the configuration of ports below 21000 or any odd ports.

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

Field	Description
Codec	This drop-down list allows you to choose the codec (G.711 or G.729) that is used by this connection. Use G.711 if this connection should be available to Cisco Unified IP Phone users or if it is part of a VTG. Use G.711 or G.729 if this connection is available to IDC users. G.729 requires digital signal processor (DSP) resources for transcoding. **Note** You cannot edit the codec and media connection attributes if users who are associated to the channel are logged in to an IP phone or an IDC. For more information about codecs, see the *Solution Reference Network Design (SRND) for Cisco IPICS* document.
Radio	This drop-down list displays when you choose a tone remote radio device type from the Type drop-down list. It allows you to choose a configured tone control radio.
Descriptor	This drop-down list displays when you choose a pooled radio device type from the Type drop-down list. It allows you to choose a serial control radio that has been enabled to serve as a pooled device.
Channel Selector	This drop-down list displays when you choose a pooled radio or tone remote radio device type from the Type drop-down list. It allows you to choose a channel selector. **Note** You cannot configure multiple channels on the same radio with the same channel selector. However, a channel can have more than one radio connection for a given radio. That is, a radio has more than one control sequence to tune to the same content. For more information about radios, see Chapter 9, "Managing Radios and Radio Descriptors." Each channel can have a specific set of signaling (over-the-air) tones that need to be broadcast over the radio. When a user is associated with the channel, any signaling tones that are defined for that channel are available for use by the IDC. **Tip** When you define channel selectors, consider the different actions that users may want to perform on the channel, such as tuning the radio or beginning a transmission over-the-air. These actions determine the commands that are sent to the radio when the user invokes the action by pressing the button on the channel. For more information about the IDC, see *Cisco IPICS Dispatch Console User Guide*.

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

Field	Description
Ops Views	
Belongs To	This drop-down list 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 2-16 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 7, "Configuring and Managing Cisco IPICS Operational Views."
Accessible To	This drop-down list 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 2-16 for information about how to associate ops views to channels. **Note** This option appears only after you save a channel. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	Click this button to make this channel accessible to other ops views. **Note** This button does not display if there are no additional ops views configured in Cisco IPICS. See the "Associating PTT Channels to Ops Views" section on page 2-16 for more information. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

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

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

Table 2-3 IDC Tab Fields in Channels Window

Field	Description
IDC	
RX Mute During PTT	The following values affect how the receive mute functionality is configured on the IDC for this channel. • None—When PTT is engaged on this channel, this channel is not muted when it receives traffic. • All—When PTT is engaged on this channel, incoming audio traffic is muted on all resources. • Channel—When PTT is engaged on this channel, incoming audio is muted for this channel only. This value is the default.

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

Field	Description
Enable Voice Activity Detection (VAD)	When you enable VAD on Cisco IPICS, the IDC only sends voice traffic when it detects a voice packet on this channel. When this attribute is set to true (attribute check box is checked) on a channel, VAD is used by the IDC when communicating with the channel. By default, this attribute is set to false (attribute check box is not checked).
Allow Latch	When set to true (attribute check box is checked) on a channel, the user can use latch to lock in the channel. By default, this attribute is set to false (attribute check box is unchecked).
Listen Only	When set to true (attribute check box is checked), the user can hear, but cannot talk, on the channel.
Channel Color	This attribute specifies a color tag that you can choose from a drop-down list. This setting 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. **Note** If you do not want the channel to be tagged with a color, you can choose **Not colored** from the drop-down list.
Channel Region	From the drop-down list, choose the region in which this channel should appear on the IDC. For information about configuring IDC regions, see the "Managing IDC Regions" section on page 2-95.

Step 4 To view channel associations, choose a channel in the Channels window, then click the **Associations** button that displays at the bottom of the window.

Step 5 To view channel associations, from the Associations window take one 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 to this channel display. The Users window lists information about each of the users who are associated to the channel.

Table 2-4 describes the items in the Users window.

Table 2-4 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.
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 end devices.

Table 2-4 Items in the Users Window (continued)

Item	Description
Disable Audio field	This field indicates whether audio is disabled on end devices.
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 are appended with a superscript (1) if they are configured as a customized value. See the "Understanding Association Attribute Behaviors" section on page 2-14 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 2-17.

- Click the **Virtual Talk Groups** tab—This tab displays the VTGs in which this channel participates.
- Click the **Signals** tab—This tab lets you associate signals to channels.

  For more detailed information, see the "Associating Radio Control Signals to PTT Channels" section on page 2-18.

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

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

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

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

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

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 (IDC, 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.

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

In addition, a channel can be in the *active* state. Cisco IPICS puts a channel into this state automatically when it is in use by an active VTG in the system. When a channel is in the active state, you must deactivate the referencing VTG or disable the channel before you can change any of its media connection assignments.

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

A channel can be configured as enabled or disabled.

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 the **Configuration > Channels** window.

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**; 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.

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 IDC 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 2-15.

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 are 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 2-15 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 2-17.

User-Channel Association Example

The following example describes different user-channel association scenarios that can be 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 User A is not allowed to latch on Channel A on the IDC. 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 > IDC** window. Because the association settings have not been customized, Cisco IPICS automatically updates the User A-Channel A association. The IDC 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 IDC 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 IDC 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 overrides the custom IDC 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 IDC.

See the "Viewing and Editing Channel Details" section on page 2-5 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 2-17.

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

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 7, "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 the **Configuration > Channels** window.

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

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 an IDC or a Cisco Unified IP Phone that has been configured for use with Cisco IPICS.

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 2-5 for more information.

To associate users to channels, perform the following procedure:

Procedure

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

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 who 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—Choose from a list of locations

  See the "Managing Locations" section on page 2-27 for detailed information about how to configure locations.
- Role drop-down list—Choose from a list of Cisco IPICS roles
- Ops View drop-down list—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria; 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 change the status of an end device for a user, see Step 7 in the "Viewing and Editing Channel Details" section on page 2-5.

Step 7 To delete a user from this channel association, check the check box to the left of the user and click **Delete**.

Step 8 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.

Associating Radio Control Signals to PTT Channels

You can associate specific radio control functions to channels in the channel Associations window. When you associate signals to channels, the specific functions that the signals perform appear as options on the IDC for that channel.

Each channel can be associated with one or more signals. Users who are associated with channels can send signals from the IDC.

You can associate signals with a channel that is not associated with a radio, such as another type of tone-controlled device. For example, you could have a Cisco IPICS PTT channel that includes an LMR gateway that is connecting to a tone-controlled device that is not a radio, such as a device that opens a gate. This type of device can interpret tones and perform specific actions.

When the IDC plays the RFC 2833 and RFC 2198 signals, the LMR gateway detects these signals (in this example, the open gate signal) and converts them into audio. This audio gets sent to the devices that open the gate that triggers them to activate. No radio is present in this scenario. The devices are directly connected to the E&M interface on the LMR gateway.

Unlike alerting tones that cannot be restricted to a specific channel, you can associate signals directly with specific channels. This flexibility gives you the ability to control the appearance of and the ability to play out signals to the appropriate channel(s).

To associate signals to channels, perform the following procedure:

Procedure

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

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 appears dimmed if you do not check a channel or if you check more than one channel.

Step 3 In the Associations window, click the **Signals** tab.

This tab shows a list of the signals that are associated with the channel, and includes the short name, description, and where it originated.

Step 4 Click **Add**.

The Search Signals window displays. This window allows you to search for additional signals to associate to the channel.

Step 5 To add a signal, check the check box to the left of the signal name; then, click **OK**.

Step 6 To delete a signal from this channel association, check the check box to the left of the signal name and click **Delete**.

Step 7 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.

Step 8 To view the users who are associated with the channel, click the **Users** tab.

To associate users to the channel, see the "Associating Users to PTT Channels" section on page 2-17.

Viewing Channel Associations

You can view channel associations by performing the following procedure:

Procedure

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

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 appears 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 2-17.

- **Virtual Talk Groups**—View the VTGs in which this channel participates.
- **Signals**—View the radio signals that are associated with this channel and associate other signals to the channel.

Note To associate other signals to the channel, see the "Associating Radio Control Signals to PTT Channels" section on page 2-18.

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.

Note This procedure deletes a channel even if it is in use by a VTG. If you delete an in-use channel, it becomes unavailable immediately.

Procedure

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

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 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 2-5 describes the fields in the Channel Groups window.

Table 2-5 Fields in the Channel Groups Window

Field	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; then, click **Go**.
Ops View drop-down list	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 2-23 and the "Removing a PTT Channel from a Channel Group" section on page 2-25
Ops View field	Ops view to which the channel group belongs	See the "Associating Ops Views to Channel Groups" section on page 2-26
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 2-25
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 2-27

Table 2-5 Fields in the Channel Groups Window (continued)

Field	Description	Reference
Associations button	Displays the Associations window for a channel group	See the "Associating Ops Views to Channel Groups" section on page 2-26 and the "Viewing Channel Group Associations" section on page 2-25
Display Controls		
Rows per page drop-down list	Specifies the number of rows of channel groups that are included in a channel groups list page	See the "Navigating Item Lists" section on page 1-13
Page field	Displays channel groups on a specific page	
|< (First page) button	Displays the first page of the channel groups list	
< (Previous page) button	Displays the previous page of the channel groups list	
> (Next page) button	Displays the next page of the channel groups list	
>| (Last page) button	Displays the last page of the channel groups list	

Adding a Channel Group

A channel group enables you to organize channels. You may find it useful to create and name channel groups according to location (for example, South Area Fire Department PTT Channel) or function (for example, Maintenance PTT Channel).

To create a channel group, perform the following procedure:

Procedure

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

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 copy an existing channel group, check the check box next to the existing channel group; then click **Copy**.

Note The **Copy** button appears 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 2-23, 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, see the "Managing VTGs" section on page 5-2.

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 2-22.

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

Procedure

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

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 2-6 provides a description of the fields in the General tab.

Table 2-6 General Tab Fields in Channel Groups Window

Field	Description
Channel Group Information	
Channel Group Name	Unique 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 7, "Configuring and Managing Cisco IPICS Operational Views."
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 7, "Configuring and Managing Cisco IPICS Operational Views."

Table 2-6 General Tab Fields in Channel Groups Window (continued)

Field	Description
Edit button	Click this button to associate ops views to the channel group. See the "Associating Ops Views to Channel Groups" section on page 2-26 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 2-7 provides a description of the fields in the Members tab.

Table 2-7 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
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—Allows you to choose from a list of ops views

Step 6 To search for a channel, enter your search criteria; 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 2-25.

Viewing Channel Group Associations

To view channel group associations, perform the following procedure:

Procedure

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

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 2-8 provides descriptions of the fields in the Associations window.

Table 2-8 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 an inactive VTG

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 the **Configuration > Channel Groups** window.

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 2-23.

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 7, "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 the **Configuration > Channel Groups** window.

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; then, click **>** or **<**, or double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the ops views; 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, 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 the **Configuration > Channel Groups** window.

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.

If two or more users are connected to the same multicast network (or domain), they are in the same location but not necessarily in the same physical place. If two or more users are in the same location and are using the same multicast channel, they can talk to each other without the need for additional resource configuration.

This section includes the following topics:

- Predefined Cisco IPICS Locations, page 2-27
- Location Associations, page 2-28
- Summary of Access Types and Connections, page 2-31

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. The designation of ALL is the sum total of all defined locations.

Note The ALL defines the scope or reachability of a multicast address. For this reason, the ALL location applies 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. The Cisco IPICS server assumes that the multicast address associated with a channel or VTG that is designated with the ALL location can reach all multicast locations. However, this assumption is not always accurate.

- 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 IDC users. When an IDC user chooses the REMOTE location from the Location drop-down list, 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 IDC 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 IDC 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 IDC 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 IDC user activates the channel or VTG, the IDC 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 IDC 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: IDC 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: IDC 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: IDC 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.
- IDC—During the login process, the IDC user chooses the 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 IDC 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—Cisco Unified IP Phones support only 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 2-9 shows a summary of the Cisco IPICS access types and connections, as they pertain to locations.

Table 2-9 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.
IDC (remote login)	Unicast	All channels and VTGs are unicast calls to the appropriate RMS.
IDC (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.
IDC (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.

The following section provide additional information about location-related management tasks that you can perform:

- Understanding the Locations Window, page 2-31
- Adding a Location, page 2-32
- Viewing or Editing a Location, page 2-32
- Deleting a Location, page 2-33

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 the **Configuration > Locations** link in the Administration Console.

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

Table 2-10 describes the items in the Locations window.

Table 2-10 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 2-32
Add button	Allows you to add a new location in Cisco IPICS	See the "Adding a Location" section on page 2-32
Delete button	Allows you to delete a location	See the "Deleting a Location" section on page 2-33

Adding a Location

You can add locations to Cisco IPICS as needed To do so, perform the following procedure:

Procedure

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

Step 2 To add a location, 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 IDC may truncate the location name if the name includes more characters than the IDC can display.

Tip Remember to assign location names that make sense to you.

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 the **Configuration > Locations** window.

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: . , – ‘ # ( ) / :_ .

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

To add a location, see the “Adding a Location” section on page 2-32. To delete a location, see the “Deleting a Location” section on page 2-33.

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.

You also 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 the **Configuration > Locations** window.

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 2-36
- Viewing and Editing Multicast Address Information, page 2-37
- Deleting a Multicast Address, page 2-38

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 2-36.

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 2-34.

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 2-36 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 2-11 describes the items in the Multicast Pool window.

Table 2-11 Fields in the Multicast Pool Window

Field	Description	Reference
Address	This field specifies the multicast address and port.	See the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-36
Location	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 2-37 and the "Deleting a Multicast Address" section on page 2-38 See the "Managing Locations" section on page 2-27 for more detailed information about locations.
Status	Either of the following designations can display in this field: • Active—Address is assigned to an active channel/VTG/radio. • Idle—Address is not assigned to an active channel/VTG/radio.	
Connection Type	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 Radio—Multicast address is assigned to a radio.	
Used By	This field specifies the name of the active channel, VTG, or radio 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 2-36
Delete button	Click this button to delete a multicast address.	See the "Deleting a Multicast Address" section on page 2-38

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, see 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, go 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 is no longer available for use by active VTGs.

Before you add a multicast address, configure locations, as described in the "Managing Locations" section on page 2-27.

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

Procedure

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

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 2-36.

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 2-38.

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 the **Configuration > Multicast Pool** window.

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 2-12.

Table 2-12 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 2-36.

Table 2-12 Multicast Address Details Area Fields (continued)

Field	Description
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. • Used by Radio—Address is assigned to a radio.
Status *Display only*	This field can include either of the following states: • Active—Address is assigned to an active channel/VTG/radio. • Idle—Address is not assigned to an active channel/VTG/radio.
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 2-27 for more detailed information about locations.
Used By *Display only*	Name of the active channel, VTG, or radio 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 the **Configuration > Multicast Pool** window.

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 IDC 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 2-41
- Adding an RMS, page 2-45
- Viewing and Configuring Loopbacks, page 2-46
- Deleting an RMS, page 2-48
- Managing the RMS Configuration, page 2-49

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 2-39.

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 the **Configuration > RMS** window in the Administration Console.

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 Appendix A, "Configuring the Cisco IPICS RMS Component."

Table 2-13 describes the items in the RMS window.

Table 2-13 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 2-41 and the "Adding an RMS" section on page 2-45 See the "Managing Locations" section on page 2-27 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 2-46
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.	
Add button	Choose this button to add an RMS component.	See the "Adding an RMS" section on page 2-45
Delete button	Choose this button to delete an RMS component.	See the "Deleting an RMS" section on page 2-48
Configuration drop-down list	Provides the ability to merge, update, or show configuration information for an RMS component.	See the "Managing the RMS Configuration" section on page 2-49

Table 2-13 Items in the RMS Window

Item	Description	Reference
Display Controls		
Rows per page drop-down list	Specifies the number of rows of RMS components that are included in a RMS components list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays RMS components on a specific page.	
|< (First page) button	Displays the first page of the RMS components list.	
< (Previous page) button	Displays the previous page of the RMS components list.	
> (Next page) button	Displays the next page of the RMS components list.	
>| (Last page) button	Displays the last page of the RMS components list.	

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 2-77.)

Tip Because the RMS comparator mechanism can interject delays, you can disable it by navigating to the **Administration > Options** window 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 2-49. For more complete configuration and deployment details, see *Solution Reference Network Design (SRND)* (latest version).

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 the **Configuration > RMS** window.

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 2-14. For information about how to deactivate a VTG, "Changing the Status of a VTG" section on page 5-12.

Step 4 To view or update the information in the General tab, see Table 2-14.

Table 2-14 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 2-27 for detailed information about locations.
Description	This field specifies a description for the RMS.

Table 2-14 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 deactivates 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" section on page 5-12. • 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.
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 lists 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 2-46.

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 2-49.

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 2-77.

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 2-42.

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 IDC 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" section on page 5-12.

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 the **Configuration > RMS** window.

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 occurs in the Cisco IPICS database, but is not 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 2-27

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

Procedure

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

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 2-14.

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, choose a location that is defined by the IP address that you entered for the router.

See the "Managing Locations" section on page 2-27 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 2-46.

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 2-49.

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 2-46
- Enabling DS0s in a Loopback, page 2-47
- Disabling DS0s in a Loopback, page 2-47
- Removing a Loopback, page 2-48

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 2-39.

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/radio 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 the **Configuration > RMS** window.

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 the **Configuration > RMS** window.

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; 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 the **Configuration > RMS** window.

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 2-41 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 2-45 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 the **Configuration > RMS** window.

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, take any of the following actions:

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

  After you click the **Update** button, wait approximately 90 seconds while the system goes through its checks and resets the RMS, then refresh your browser window to see current information.
- 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.

Managing the UMS

The unified media service (UMS) is a component that performs audio mixing functions similar to those performed by the RMS. For more information, see the "UMS" section on page 1-5.

The following sections describe the sections that a Cisco IPICS system administrator can perform for the UMS:

- Understanding the UMS Window, page 2-50
- Viewing and Editing UMS Details, page 2-52
- Enabling or Disabling a UMS, page 2-55
- Repairing the UMS or Viewing a Mixing Session, page 2-55
- Adding a UMS, page 2-56
- Deleting a UMS, page 2-57

You perform the UMS management tasks in the UMS window, which is located in the Configuration drawer. For more information about this window, including how to access it, see the "Understanding the UMS Window" section on page 2-50.

Understanding the UMS Window

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

To display the UMS window, navigate to the **Configuration > UMS** window in the Administration Console.

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

Table 2-15 describes the items in the UMS window.

Table 2-15 Items in the UMS Window

Item	Description	Reference
Name field	This field specifies a unique name that is assigned to the UMS.	See the "Viewing and Editing UMS Details" section on page 2-52 and the "Adding a UMS" section on page 2-56.
Location field	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this UMS.	See the "Managing Locations" section on page 2-27 for detailed information about configuring locations.

Table 2-15 Items in the UMS Window (continued)

Item	Description	Reference
IP Address field	This field specifies the IP address of the UMS.	See the "Viewing and Editing UMS Details" section on page 2-52 and the "Adding a UMS" section on page 2-56.
Configuration Port field	This field specifies the port on the UMS that the Cisco IPICS server uses to configure and control the UMS.	
High Availability Port field	This field specifies the port on the UMS that is used for HA heartbeats.	
SIP Connection Port	This field specifies the port on the UMS that remote clients use to communicate with the UMS.	
Mode	This field shows the current HA mode of the UMS ("Primary" or "Secondary"). Displays "Primary" for a standalone UMS.	
HA Status field	This field shows the HA status of the UMS ("Active," "Standby," "Initializing," "Out of Service," or "Unknown").	
Status field	This field shows the operational status of the UMS ("Enabled" or "Disabled"). The Cisco IPICS server excludes disabled UMS components when attempting to fulfill an audio mixing request.	
Number of Voice Ports in User field	The first value in this field shows how many VTGs and remote channels are being mixed on this UMS. The second value shows the maximum number of VTGs and remote channels that can be mixed at one time on this UMS.	
Add button	Choose this button to add a UMS component.	See the "Adding a UMS" section on page 2-56.
Delete button	Choose this button to delete a UMS component.	See the "Deleting a UMS" section on page 2-57.
Change Status drop-down list	Choose **Enable** to enable the UMS, or choose **Disable** to disable the UMS. Some operations, such as tearing down HA for the Cisco IPICS server, require that the UMS be disabled.	See the "Enabling or Disabling a UMS" section on page 2-55.

Table 2-15 Items in the UMS Window (continued)

Item	Description	Reference
Configure drop-down list	Choose **Update** to repair various UMS communication issues and update the UMS with the latest configuration from the Cisco IPICS server. Choose **Show** to see the current mixing sessions on the UMS.	See the "Repairing the UMS or Viewing a Mixing Session" section on page 2-55.
Display Controls		
Rows per page drop-down list	Specifies the number of rows of UMS components that are included in a UMS components list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays UMS components on a specific page.	
|< (First page) button	Displays the first page of the UMS components list.	
< (Previous page) button	Displays the previous page of the UMS components list.	
> (Next page) button	Displays the next page of the UMS components list.	
>| (Last page) button	Displays the last page of the UMS components list.	

Viewing and Editing UMS Details

You can view and edit information for any UMS in your Cisco IPICS network.

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

Procedure

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

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

The Configuration window for the selected UMS displays.

Step 3 View or update the information in the Configuration window, as described in Table 2-16.

Table 2-16 Fields in the Configuration Page of the UMS Window

Field	Description
Basic Configuration Tab	
UMS Name	This field specifies the name of the UMS. The name can include alphanumeric characters only.
UMS IP Address	This field specifies the IP address of the UMS. The Cisco server requires this address to send mixing requests to the UMS. Remote Clients also connect to this address in their SIP connections.

Table 2-16 Fields in the Configuration Page of the UMS Window (continued)

Field	Description
Location	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this UMS. A UMS must be configured with the same location that is configured for the channels that it serves. A UMS cannot be configured with the same location as an existing RMS. See the "Managing Locations" section on page 2-27 for detailed information about locations.
UMS Admin Password	This fields specifies the password for the Linux OS user "ipicsadmin" on the UMS.
Configuration Port	This field specifies the port on the UMS that the Cisco IPICS server uses to configure and control the UMS.
SIP Connection Port	This field specifies the port on the UMS that remote clients use to communicate with the UMS.
Save	Click this button to exit the UMS Configuration Page and save any changes that you made.
Cancel	Click this button to exit the UMS Configuration Page without saving any changes that you made.
Advanced Configuration Tab	
HA Enabled	Check this check box to make the Paired UMS field available so that HA for the UMS can be enabled. If unchecked, HA for the UMS is disabled. **Note** When HA is enabled, the active UMS and standby UMS maintain a heartbeat between them to continuously confirm the status and availability of each other. After a specified number of heartbeats are missed, an HA failure is declared and failover quickly occurs in the background. Within 5 seconds the audio fails over to the backup UMS, with minimal perceptible voice loss.
Mode *Display only*	This field shows the current HA mode of the UMS ("Primary" or "Secondary"). Displays "Primary" for a standalone UMS.
Paired UMS	Choose the UMS to use as the secondary UMS in an HA deployment. Each UMS must be in the same location to be paired. Before you can set up UMS HA, you must add both UMSs individually, and then select the paired UMS.
Heartbeat Port	This field specifies the port on the UMS that is used for HA heartbeats. The default value is 4000.
Heartbeat Interval (secs)	This field specifies the number of seconds between UMS-to-UMS heartbeats. Each heartbeat checks to confirm the status and availability of the partner server. Valid values are 5 through 600. The default value is 5.
Missed Heartbeat Count	This field specifies the number of missed heartbeats before the active UMS fails over to the standby UMS. Valid values are 5 through 30. The default is 5 (25 seconds if the Heartbeat interval is 5 seconds). The transition process takes approximately 10 seconds.

Table 2-16 Fields in the Configuration Page of the UMS Window (continued)

Field	Description
Save	Click this button to exit the UMS Configuration Page and save any changes that you made.
Cancel	Click this button to exit the UMS Configuration Page without saving any changes that you made.
UMS HA Status Tab	
Note This tab appears only after you save UMS configuration.	
UMS High Availability Mode *Display only*	This field indicates whether HA for the UMS is configured: • Enabled—HA for the UMS is configured • Disable—HA for the UMS is not configured
Standby UMS HA Status *Display only*	This field indicates whether the standby UMS is ready to go to active mode. Values are "Ready" or "Not Ready."
UMS Name *Display only*	This field shows the name of the UMS.
Operational State *Display only*	This field shows the operational status of the UMS ("Enabled" or "Disabled"). The Cisco IPICS server excludes disabled UMS components when attempting to fulfill an audio mixing request.
HA Status *Display only*	This field shows the status of the UMS: • Active—The UMS is ready to mix audio. • Standby—The UMS is ready for failover. • Initializing—The UMS is initializing. • Out of Service—The UMS is reachable, but is either unable to initialize or is in the process of restarting. • Unknown—The UMS is not reachable or there is a SSL certificate problem. The normal UMS operating state is Active or Standby.
Failover Now	Click this button to perform a manual failover from the active UMS to the standby UMS.
Go Standby	Click this button to force one of the UMSs into standby state. After network connectivity is restored, use this button to recover from a *split brain* scenario. For related information, see Chapter 10, "Configuring and Managing Cisco IPICS High Availability."
Refresh	Click this button to update the information on this tab with current information.
Voice Resource List Tab	
Port Number *Display only*	This fields shows an arbitrary identifier for an audio mixing session.
Voice Resource Status *Display only*	Reserved for future use.
Operational Status *Display only*	Displays the current operating status of the voice resource.

Table 2-16 Fields in the Configuration Page of the UMS Window (continued)

Field	Description
Source *Display only*	Channel or VTG of the connection that the voice resource is making.
Destination *Display only*	Channel, user, or VTG of the connection that the voice resource is making.
Refresh	Click this button to update the information on this tab with current information.

Enabling or Disabling a UMS

When you disable a UMS, it goes into the Disabled state and is not available to fulfill audio mixing requests until you enable it. You should disable a UMS when you make certain changes to it, as described in the "Viewing and Editing UMS Details" section on page 2-52.

Note You cannot deactivate a UMS if any VTGs are active or if the UMS is configured for HA. When the UMS becomes disabled, Cisco IPICS no longer uses any of its voice ports. To deactivate a VTG, see the "Changing the Status of a VTG" section on page 5-12.

When you enable a UMS component, it becomes available for use by Cisco IPICS.

To enable or disable a UMS, perform the following procedure:

Procedure

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

Step 2 Check the check box next to the link of the UMS that you want to enable or disable.

Step 3 From the Change Status drop-down list, choose **Enable** to enable the UMS, or choose **Disable** to disable the UMS.

Repairing the UMS or Viewing a Mixing Session

This section explains how to repair a UMS and view a mixing session that a UMS is handling.

Repairing a UMS fixes various UMS communication issues and updates the UMS with the latest configuration from the Cisco IPICS server. Perform this action in these situations:

- A UMS is in a split brain situation and there is no network issue causing this situation
- After a database restore
- After recovering from a hardware failure of a Cisco IPICS server or a UMS
- When a UMS is out of sync with the Cisco IPICS server

To repair a UMS or view a mixing session, perform the following procedure:

Procedure

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

Step 2 Check the check box next to the link of the UMS that you want to update or view information about.

Step 3 From the Configure drop-down list, choose either of these options:

- **Update**—Repairs various UMS communication issues and updates the UMS with the latest configuration from the Cisco IPICS server.

  Repair is a lengthy process and takes more time if you have server HA or UMS HA configured. In some cases, it may take up to 5 minutes to repair a UMS. Be aware that services on the UMS restart during this process.

- **Show**—Displays the current mixing sessions on the UMS.

Adding a UMS

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

- The UMS application must be installed on a dedicated server. See *Cisco IPICS Installation Guide* for UMS installation instructions.
- The UMS cannot be in the same location (multicast domain) as an RMS component.
- At least one location must be defined, as described in the "Managing Locations" section on page 2-27.
- You cannot add a UMS to a Cisco IPICS server if it is already in use by another Cisco IPICS server.
- The UMS must be running the same Cisco IPICS software release as the Cisco IPICS server.
- The UMS must be reachable when you add it to the Cisco IPICS server.

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

Procedure

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

Step 2 Click **Add**.

The UMS Configuration window displays.

Step 3 The UMS Configuration window, take these actions:

Note For detailed descriptions of the UMS fields, see Table 2-16.

f. In the UMS Name field, enter a unique name for the UMS.

a. In the UMS IP Address field, enter the IP address of the server on which the UMS is installed.

b. From the Location drop-down list, choose a location for the UMS.

See the "Managing Locations" section on page 2-27 for more detailed information about locations.

c. In the UMS Admin Password field, enter the password that you entered for the ipicsadmin user when you installed the UMS.

d. In the Configuration Port field, the port on the UMS that the Cisco IPICS server uses to configure and control the UMS.

   Cisco recommends that you use the default port 5555.

e. In the SIP Connection Port field, enter the port on the UMS that remote clients use to communicate with the UMS.

   Cisco recommends that you use the default port 5060.

f. Click **Save**.

   Cisco IPICS determines whether it can access the UMS. This process can take up to one minute and the message "This will take a minute. Please wait..." appears during this time. If the UMS is accessible, Cisco IPICS displays the UMS List page. If the UMS is not accessible, a message informs you of the possible reason.

Step 4 (Optional) If you are configuring a UMS for high availability, take these actions:

a. Click the name of the UMS that you want to configure as the primary UMS.

b. Click the Advanced Configuration tab.

c. Check the HA Enabled check box.

d. From the Paired UMS drop-down list, choose the UMS that is to be the secondary UMS.

e. In the Heartbeat Port field, enter the port number on the UMS that is used for HA heartbeats.

   Cisco recommends that you use the default port 4000.

f. In the Heartbeat Interval (secs) field, enter a number between 5 and 600 that defines the number of seconds between heartbeats. Each heartbeat checks to confirm the status and availability of the partner server.

   Cisco recommends that you use the default value of 5.

g. In the Missed Heartbeat Count field, enter a number from 5 to 30 that defines the number of missed heartbeats before the active role is transitioned to the secondary server.

   Cisco recommends that you use default value of 5.

h. Click **Save**.

Deleting a UMS

Deleting a UMS removes all of its resources from Cisco IPICS and makes the UMS unavailable to Cisco IPICS. This process can take up to 2 minutes and requires that the UMS be reachable.

To delete a UMS, perform the following procedure:

Procedure

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

Step 2 Check the check box next to the **UMS** 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 **U**MS, click **Cancel**.

Managing Incidents

An incident is an event that you identify in Cisco IPICS and for which various users can coordinate responses by using the IDC. An incident can be any event, such as a fire or other situation, that requires a response.

The following section uses these incident-related terms:

- Active incident—The incident is ongoing and the IDC functionality is available for coordinating it. In addition, mobile client users can access the incident.
- Deactive incident—The incident is closed and the IDC functionality is not available for coordinating the incident. In addition, mobile client users cannot access the incident. (A deactive incident can be reactivated, if needed.)
- Incident VTG—A talk group that consists of the users, channels, and radios that are associated with an incident. When an incident VTG is active, its participants can communicate with each other. When it is inactive, they cannot.

For detailed information about coordinating incidents by using the IDC, see *IPICS Dispatch Console User Guide* for this release.

As a Cisco IPICS system administrator, you can perform the following incident management tasks, which allow you to obtain information and manage system resources:

- Understanding the Incidents Window, page 2-59
- Viewing Incident Details, page 2-60
- Changing the Status of an Incident, page 2-62
- Downloading Archived Incidents, page 2-62
- Deleting an Incident, page 2-63

You perform the incident management tasks in the Incidents window, located in the Configuration drawer of the Administration Console. For more information about this window, including how to access it, see the "Understanding the Incidents Window" section on page 2-59.

Note A user with the Cisco IPICS Dispatcher role or All role creates incidents in the IDC. For more information, see *IPICS Dispatch Console User Guide* for this release.

Understanding the Incidents Window

The Incidents window lists information about each incident that is configured in Cisco IPICS and is not yet archived.

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

Note You can specify the number of rows of incidents that display per results page by choosing from the Rows per page drop-down list 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 various incident management functions. To display the Incidents window, access the Configuration drawer, then click **Incidents**.

Table 2-17 describes the items in the Incidents window.

Table 2-17 Items in the Incidents Window

Item	Description	Reference
Filter		
Incident ID field	This field allows you to display only the incident with the ID that you enter.	To limit the display of incidents or to display a certain incident, enter the desired search criteria in the filter field; then, click **Go**.
Incident Name field	This field allows you to display only incidents with names that include the character string that you enter (characters are not case-sensitive).	
Started Before fields	These fields allows you to display only incidents that were activated before the date and time that you specify. To specify a date, click the Started Before field, then choose a date. To specify a time, choose the hour (24-hour format) and minute from the “at” drop-down lists.	
State field	This field allows you to display only incidents that are active or only incidents that are inactive.	
Incident VTG field	This field allows you to display only incidents that have an active incident VTG or only incidents that have an inactive incident VTG.	
Ops View field	This field allows you to display only incidents that belong to the designated ops view.	
Go button	Click this button to display incidents by the filters that you choose.	
Clear Filter button	Click this button to remove filter selections and display an empty list of incidents. Click the **Incidents** link again to display the full list of entries.	

Table 2-17 Items in the Incidents Window (continued)

Item	Description	Reference
Incident Information		
ID field	This field indicates the unique identifier that Cisco IPICS assigned to the incident	—
Name field	This field indicates the name that is assigned to the incident.	See *IPICS Dispatch Console User Guide* for this release.
Ops View field	This field indicates the ops view to which the incident belongs. An incident belongs to the same ops view as that of the user who created it.	—
Activated field	Indicates the date and time that the incident was activated.	See *IPICS Dispatch Console User Guide* for this release.
State field	This field indicates whether the incident is active or inactive.	See the "Changing the Status of an Incident" section on page 2-62.
Incident VTG field	This field indicates whether the incident VTG is active or inactive, if the incident includes an incident VTG.	See *IPICS Dispatch Console User Guide* for this release.
Delete button	Click this button to delete the specified incident(s).	See the "Deleting an Incident" section on page 2-63.
Change Status drop-down list	Choose from the Activate or Deactivate option to change the status of an incident.	See the "Changing the Status of an Incident" section on page 2-62.
Download Archived Incident(s) button	Click this button to obtain archived incidents.	See the "Downloading Archived Incidents" section on page 2-62.
Display Controls		
Rows per page drop-down list	Specifies the number of rows of channels that are included in a channels list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays channels on a specific page.	
|< (First page) button	Displays the first page of the channels list.	
< (Previous page) button	Displays the previous page of the channels list.	
> (Next page) button	Displays the next page of the channels list.	
>| (Last page) button	Displays the last page of the channels list.	

Viewing Incident Details

You can view information for any incident. To do so, perform the following procedure:

Procedure

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

Step 2 In the ID column, click the link for the incident for which you want to view information.

Information for the selected incident displays. Table 2-18 describes this information.

Table 2-18 Information for Incidents

Field	Description
Incident Information	
ID	This field shows the unique identifier that Cisco IPICS assigned to the incident.
Name	This field shows the name that was assigned to the incident in the IDC.
Description	This field shows the description that was entered for the incident in the IDC.
State	This field shows whether the incident is active or inactive.
Current Participants	Tabs that show the following information: • User tab—Shows the Cisco IPICs user name, first name, and last name of each user who is a participant in the incident. • Channel tab—Shows the name, description, and status (Enabled or Disabled) of each channel that is used in the incident. • Radio tab—Shows the name, description, and status (Enabled or Disabled) of each radio that is used in the incident. • Photo tab—Shows the name, description, and URL of each photograph that has been uploaded for the incident. To delete a photograph from the incident, check the check box to the left of the photograph and click **Delete**. • Video tab—Shows the name, description, and URL of each video that has been uploaded for the incident. To delete a video from the incident, check the check box to the left of the video and click **Delete**. • VTG tab—Shows the name, description, and status (Active or Inactive) of each incident VTG that has been created for the incident. • Journal tab—Shows the name, description or message, type, and creation date of each journal entry that has been created for the incident. Type indicates that a user created the entry.
Incident VTG	This field shows whether the incident VTG for the incident is active or inactive.
Ops View	This field indicates the ops view to which the incident belongs.
Address	Reserved for future use.
Created	This field shows the date and time that the incident was created.
Activated	This field shows the date and time that the incident was activated.
Deactivated	This field shows the date and time that the incident was deactivated. If the incident is still active, this field displays “(Still Active).”

Step 3 To exit the display of incident details, click **Done**.

Changing the Status of an Incident

Cisco IPICS allows you to change the status of an incident. An incident status can be either of the following:

- Active incident—The incident is available on the IDC. You can use the IDC to add or remove resources and perform other activities for an active incident.
- Inactive incident—The incident is closed and the incident is not available on the IDC or to mobile client users cannot access the incident.

To determine the current status of an incident, access the Configuration drawer, click **Incidents**, and look at the information in the State column for the incident.

To change the status of an incident, perform the following procedure.

Procedure

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

Step 2 Check the check box next to each incident for which you want to change the state, then choose the desired action (**Activate** or **Deactivate**) from the Change Status drop-down list.

Step 3 In the pop-up window that prompts you to confirm the action, click **OK**.

Downloading Archived Incidents

Cisco IPICS automatically archives an incident 30 days after it is deactivated (by default) or after the retention period that you configured. (For information about configuring archives, see the description of the Incident Archive pane options in Table 2-25 on page 2-77.) The system stores information about each archived incidents in a unique XML file. The XML files contain information about users, channels, radios, VTGs, journal entries, images, and videos that are part of the incident.

You can download the incident archive, which contains the XML files for all archived incidents. This process copies the zipped archived incident file to your local disk.

When an incident is archived, the system deletes it from the Cisco IPICS database, and it no longer appears in the list of incidents in the Incidents window. If the incident includes images or video clips that are stored on the Cisco IPICS server disk, and these items are not referenced by another incident the archiving process deletes these items from the disk.

To download an archived incident, To delete an incident, perform the following procedure:

Procedure

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

Step 2 Click the **Download Archived Incident(s)** button.

This button is enabled only after the system creates and archive file.

Step 3 In the File Download dialog box, click Save, and follow the on-screen prompts to save the archive file in a location of your choice.

By default, the archive file name is ipics_incident_archive.zip.

Deleting an Incident

If an incident is no longer needed, you can delete it from Cisco IPICS. You can delete a single incident or you can delete several incidents at one time.

When you delete an incident, it goes into the *pending deletion* state. The system archives incidents in this state the next time it runs the archiver, then deletes the incidents from the Cisco IPICS database. When an incident is in this state, it does not appear in the IDC nor in the Incidents page in the Cisco IPICS Administration Console.

To delete an incident, perform the following procedure:

Procedure

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

Step 2 If an incident that you want to delete is active, deactivate is as described in the "Changing the Status of an Incident" section on page 2-62.

Step 3 Check the check box next to each incident that you want to delete.

Step 4 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 5 To confirm the deletion, click **OK**.

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

Managing Licenses

The Cisco IPICS license determines the number of concurrent LMR ports, multicast ports, dial users, Cisco Unified IP Phone users, Silver IDC users, Platinum IDC users, mobile endpoint users, and ops views that are available for your system. Licenses also determine whether the policy engine is enabled on your system, and whether high availability is enabled on your system.

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, see *Cisco IPICS Server Installation and Upgrade Guide* for this release.

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 2-68.

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 2-64.

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 2-68 for information about uploading licenses.

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

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, the update may not succeed and cause Cisco IPICS to display an error. If you receive an error, refresh your browser window and retry the operation.

The License Management window contains the following tabs:

- Summary Tab
- Usage Per Ops View Tab
- Installed License Files Tab

Summary Tab

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. Table 2-19 describes the information in this tab.

If your system includes high availability, the high availability license resides on the secondary server only. The other licenses reside on the primary server only.

Table 2-19 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. **Note** Each radio channel that you add in Cisco IPICS uses one LMR license. However, each unique channel that you configure within a radio channel, does not use a separate LMR license. Cisco IPICS uses only one LMR license per radio. 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, the single channel uses two licenses. If one of the multicast addresses is removed, the system releases one of the licenses so that the port only uses one license.

Table 2-19 Summary Tab Fields in the License Management Window (continued)

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 uses a license when a policy triggers (activates) that VTG; therefore, 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.
Concurrent Cisco Unified IP Phone Users	A Cisco Unified IP Phone user who is logged in to Cisco IPICS consumes one Cisco Unified IP Phone license. Cisco IPICS release the license when the user logs out. If you use all of the Cisco Unified IP Phone licenses, no more Cisco Unified IP Phone users can dial in.
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 are 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 are not able to access the policy engine windows.
Concurrent Dispatch Console Silver Users	An IDC Silver user who is logged in to Cisco IPICS consumes one IDC Silver license. Cisco IPICS release the license when the user logs out. If you use all of the IDC Silver licenses, no more IDC Silver users can log in.
Concurrent Dispatch Console Platinum Users	An IDC Platinum user who is logged in to Cisco IPICS consumes one IDC Platinum license. Cisco IPICS release the license when the user logs out. If you use all of the IDC Platinum licenses, no more IDC Silver users can log in.
Concurrent Mobile Endpoint Users	A mobile endpoint user who is logged in to Cisco IPICS consumes one mobile endpoint license. Cisco IPICS release the license when the user logs out. If you use all of the mobile endpoint licenses, no more mobile endpoint users can log in.
Concurrent EndtoEnd P25 Vocoders	The number of concurrent connections to end-to-end P25 channels that your Cisco IPICS system is licensed to use on the IDC. An IDC user uses a license each time a P25 channel is powered up in EndtoEnd mode. **Note** The IDC supports a maximum of 4 concurrent P25 channels in EndtoEnd mode per user session. If a user is logged in from 2 IDC consoles at the same time, only one IDC can join P25 channels in EndtoEnd mode.
Concurrent Gateway Vocoders	The number of P25 channels that can be concurrently enabled at any time on the Cisco IPICS server. The Cisco IPICS server uses a license each time a P25 channel is enabled on that server.

Table 2-19 Summary Tab Fields in the License Management Window (continued)

Field	Description
Concurrent UMS Servers	The number of UMSs that can be configured and enabled in the Administration Console.
Concurrent ISSI Gateway Servers	The number of ISSI Gateway servers that can be configured and enabled in the Administration Console.
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.
Cisco UMS High Availability License	License usage does not apply to this field. This field indicates whether you have a base license for UMS high availability.
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**.
High Availability License	License usage does not apply to this field. This field displays whether you have a high availability license for Cisco IPICS.

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 7, "Configuring and Managing Cisco IPICS Operational Views" for more information about ops views.

Usage Per Ops View Tab

The **Usage Per Ops View** tab provides license information per ops view. This tab displays types of licenses, the ops view, current license usage, and the allocated ports. Table 2-20 describes the information in this tab.

Table 2-20 Usage Per Ops View Tab in the License Management Window

Field	Description
License Type	
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

Table 2-20 Usage Per Ops View Tab in the License Management Window (continued)

Field	Description
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
Cisco Unified IP Phone Users	Ops View—Ops view to which this license belongs Current Usage—Number of Cisco Unified IP Phone ports in use for this ops view Allocated Ports—Number of Cisco Unified IP Phone ports that have been allocated to this ops view
Dial Users	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
Dispatch Console Silver Users	Ops View—Ops view to which this license belongs Current Usage—Number of IDC ports that are in use for this ops view Allocated Ports—Number of IDC ports that have been allocated to this ops view
Dispatch Console Platinum Users	Ops View—Ops view to which this license belongs Current Usage—Number of IDC ports that are in use for this ops view Allocated Ports—Number of IDC ports that have been allocated to this ops view
Mobile Endpoint Users	Ops View—Ops view to which this license belongs Current Usage—Number of mobile endpoint users that are in use for this ops view Allocated Ports—Number of mobile endpoint users that have been allocated to this ops view

Installed License Files Tab

The **Installed License Files** tab provides information about the license files installed on the IPICS server. It displays the file name, file size (in bytes), and modify date for each license file. Table 2-21 describes the information in this tab.

Table 2-21 Installed License Files Tab in the License Management Window

Field	Description
File Name	Name of the installed license file.
File Size	Size (in bytes) of the installed license file.
Modify Date	Date and time when the license file was uploaded to the server.

Understanding Time-bound License Behavior

Time-bound, or evaluation, licenses differ from permanent licenses by the inclusion of a predefined expiration date.

Note Cisco IPICS does not overwrite older license files with newer license files. As a best practice, Cisco recommends that you remove the old license file(s) from the directory where Cisco IPICS stores the license(s).

After you remove the old license(s), restart the server by entering the following command:

*[root]# **service ipics restart***

For more detailed information and guidelines about time-bound licenses, see *Cisco IPICS Server Installation and Upgrade Guide* for this release.

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 is 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/current/webapps/license/**

To upload a license file, perform the following procedure:

Procedure

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

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, see *Cisco IPICS Server Installation and Upgrade Guide* for this release.

Viewing Active Users

As a Cisco IPICS system administrator, you can view the activity for users who are logged in to the system via an IDC, mobile client, Cisco Unified IP Phone, or dial-in, 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 view active users and the associated information for each user, perform the following procedure:

Procedure

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

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

- **Logged-in Users**—Users who are logged in to Cisco IPICS
- **IDC**—Users who connected to Cisco IPICS through an IDC
- **Mobile**—Users who connected to Cisco IPICS through a Cisco IPICS Mobile Client.
- **Cisco Unified IP Phone Users**—Users who are connected to Cisco IPICS via a Cisco Unified 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 2-22 for a description of the fields in the Active Users window.

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 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 2-22 Active Users Window Fields

Field	Description
Logged-in Users	
User	User ID of user who is logged in to Cisco IPICS.
Date	Date and time that the user logged in to the Cisco IPICS system.

Table 2-22 Active Users Window Fields (continued)

Field	Description
IDC Users	
User	User ID of the active IDC user.
IDC ID	Identification of the IDC for the session.
Version	Version of the IDC.
Address	IP address of the IDC client machine.
Location	Cisco IPICS location of the IDC user.
Belongs To	Ops view to which the IDC user belongs.
Last Activity	Date and time of the last IDC activity.
Mobile Users	
User	User ID of the active mobile client user.
Mobile ID	Identification of the mobile client for the session.
Version	Version of the mobile client.
Address	IP address of the mobile client.
Location	Cisco IPICS location of the mobile client.
Last Activity	Date and time of the last mobile client activity.
Cisco Unified IP Phone Users	
User	Name or user ID of the active Cisco Unified IP Phone user.
Digit ID	Digit identification number of the active Cisco Unified IP Phone user.
Location	Location of the active Cisco Unified IP Phone user.
Active	Indicates whether the Cisco Unified IP Phone user is currently active.
Remote	Indicates whether the Cisco Unified IP Phone user is dialed in using a remote connection.
Dialed-in Users	
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.

Table 2-22 Active Users Window Fields (continued)

Field	Description
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, IDC, mobile client, 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 an IDC user, click the **IDC** tab. Check the check box to the left of each IDC user that you want to log out and click **Logout**.

  When you log out an IDC user, all resources, including licenses and RMS resources, are deallocated immediately.

  If the IDC is running in offline mode, multicast audio for the IDC continues to work after you log out an IDC user if the Cisco IPICS server cannot reach the IDC to inform it of the logout and a channel or VTG is active. However, if the IDC was REMOTE (that is, using a unicast SIP call to the RMS), the server tears down the dedicated SIP connection for that IDC upon when you click **Logout** on the IDC tab.
- To log out a mobile client user, click the **Mobile** tab. Check the check box to the left of each mobile user that you want to log out and click **Logout**.

  When you log out a mobile client user, all resources, including licenses and RMS resources, are deallocated immediately.
- 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 clicking **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.

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 2-72 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 2-75.

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 radio—Channels, users, and VTGs that used that radio
- 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 2-73 for more information.

Understanding the Activity Log Management Window

The Activity Log Management window displays each channel, radio, 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, radio, 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, 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 1-7.

For information about viewing and downloading Cisco IPICS activity logs, see the "Viewing and Downloading Activity Logs" section on page 2-73.

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 2-77. For information about downloading archived activity logs, see the "Downloading Archived Activity Logs" section on page 2-74.

For information on the display controls, see the "Navigating Item Lists" section on page 1-13.

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

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, radio, 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 the **Administration > Activity Log Management** window.

Step 2 From the drop-down list 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, 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, 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 or download.

Step 7 In the To field, specify the ending date and time of the activity logs that you want to view 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 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 steps were performed by using Microsoft Office Excel 2007.

- Use Microsoft Excel application to open the .xml file. In the Open XML dialog box, click the **As an XML Table** 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 and take these actions:
  - Right-click the file.
  - Choose **Open With > Choose Program**.
  - Choose **Microsoft Excel** in the Open With dialog box. (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 2-74.

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 in the Administration Console. For more information about the Options window, see the "Managing Cisco IPICS Options" section on page 2-77.

To download archived activity logs, perform the following procedure:

Procedure

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

Step 2 Click the **Archives** tab.

Table 2-23 shows the fields in the Archive Status pane.

Table 2-23 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

Table 2-23 Archive WIndow Fields (continued)

Field	Description
Archive Count *Display only*	Number of log entries that were archived during the last archive
Archived Files drop-down list	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, 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 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 2-24 describes the types of activities that can be logged in by ops views.

Table 2-24 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.
HAACTIONS	Logs are created whenever a high-availability activity occurs.
IDC Activities	Logs are created whenever IDC activities occur in Cisco IPICS.

Table 2-24 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.
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 in the Administration Console 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 the **Administration > Activity Log Options** window.

Step 2 From the Ops View drop-down list, 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; then, click **>** or **<**. Or, double-click the activity type.
- To move several activity types from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the activity types; 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 various options that affect the system and devices.
- **Passwords** tab—Choose this tab to set the password options for users.
- **Client** tab—Choose this tab to set IDC client 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 in the Administration Console 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 IDC 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 2-25, Table 2-26, and Table 2-27 describe the fields in the Options window.

Table 2-25 General Tab in the Options Window

Setting	Description	Default Setting
RMS Pane		
Disable RMS Comparator	The RMS comparator is the mechanism that checks the responsiveness of the RMS and if there have been any changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. Because 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 through 32767.	The default interval between checks specifies 10 minutes.

Table 2-25 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Activity Logs Pane		
Maximum Activity Logs	This setting the maximum amount of database space that may be used by Cisco IPICS activity logs. For more information, see Chapter 12, "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 through 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 through 365.	The default setting specifies 90 days.
Cisco Unified IP Phone Pane		
Cisco Unified IP Phone Timeout Period	This setting specifies whether a Cisco Unified IP Phone times out after a configured period of inactivity, forcing a user to log in again. **Note** To disable the timeout period, set the value to 0. This setting specifies a value in minutes. To change the default, double-click the current value and enter a new value. Valid values: 0 through 99999.	The default setting specifies 30 minutes.
Cisco IPICS Session Pane		
Cisco IPICS Session Timeout Period	This setting specifies whether a Cisco IPICS session times out after a configured period of inactivity, forcing a user to log in again. **Note** To disable the timeout period, set the value to 0. This setting specifies a value in minutes. To change the default, double-click the current value and enter a new value. Valid values: 0 through 99999.	The default setting specifies 30 minutes.
Incident Archive Pane		
Maximum File Size	This field specifies the maximum size of archive file, in MB. When an archive file reaches this size, older information is deleted.	The default setting specifies 50 MB.
Retention Period	This field specifies how many days Cisco IPICS retains an inactive incident before archiving the incident. Until a incident is archived, you can reactivate it from the Incidents window.	The default setting specifies 30 day.

Table 2-25 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Archive File Name	This field specifies the location on the Cisco IPICS server where the archive file is stored, and the name of the archive file.	The default location and file name is /idspri/archive/incident/ipics_incident_archive.zip
Run at	The server time at which Cisco IPICS runs the archive process each day. At this time, Cisco IPICS archives any incidents have been inactive for 30 days (by default) or for the retention period that you configured.	The default time is 00:00 (midnight), server time.
Operator Role Assignments Pane		
Restrict Operator Role assignments	If you check this box, users with the operator role can grant users (including themselves) the operator, dispatcher, or Ops view administrator roles only.	Not checked.
CUCM Settings for IDC Dialer		
CUCM Host Name or IP Address	Host name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express that the IDC uses for the dialer functionality.	—

Table 2-26 Passwords Tab in the Options Window

Setting	Description	Default Setting
User Passwords Pane		
Minimum Password Length	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 4-2. Use the drop-down list to choose a new setting. The minimum length can range from 4 to 20 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 through 20.	The default setting specifies 8 characters.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
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 through 10.	The default setting specifies 4 characters.
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 through 20.	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 through 20.	The default setting specifies 1 character.
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 through 20.	The default setting specifies 1 character.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
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 through 20.	The default setting specifies 1 character.
Password History Count	This setting specifies the number of passwords that Cisco IPICS marks as previously used, and that the user is not able to use again. For example, if the Password History Count is set to 5, the user is not 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 through 999.	The default setting specifies 5 previous passwords.
Password Expiration Pane		
Apply User Password Expiration	This check box specifies whether Cisco IPICS applies the value that is specified in the Password Expiration field. If this check box is unchecked, there is 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.
Password Expiration	This setting specifies the number of days before a Cisco IPICS login password and the digit password expire. For example, if the value is 180 days, the password expires after 180 days from the date that the password was created. To prevent the password from expiring, uncheck the check box in the Apply User Password Expiration setting. The Never Expired message displays in the Password Expiration Date field, in the My Profile window for the user. 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 forces users who log in to Cisco IPICS during that day (after the migration) to change their login passwords. Valid values: 1 through 999.	The default setting specifies 180 days.

Table 2-26 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** To expire passwords quickly, set the value to 1 day. The user will be forced to change the password when logging in to Cisco IPICS the following day. Valid values: 1 through 999.	The default setting specifies 3 days.
User Account Lockout Pane		
Apply User Account Lockout	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 is 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 2-26 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 through 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 is locked. When the user account is unlocked, both invalid attempt counts is 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."	The default setting specifies 5 attempts.
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 through 999.	The default setting specifies 8 hours.

Table 2-27 Client Tab in the Options Window

Setting	Description	Default Setting
Configuration Pane		
Client Update Poll	This setting specifies the frequency that the IDC uses to poll the server for updates. For more information, see *IPICS Dispatch Console 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 through 3600.	The default polling interval specifies 5 seconds.

Table 2-27 Client Tab in the Options Window (continued)

Setting	Description	Default Setting
Logout Client After	This setting configures the number of seconds an IDC client can be offline before the session expires and is forced to log out. **Note** Quick patch VTGs that are created by an IDC client session are associated to the session on the server. They are deleted from the server when the session expires and is forced to log out. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 0 through 99999. A value of 0 specifies that IDC client sessions never expire and are never forced to log out.	The default client logout interval specifies 900 seconds (15 minutes).
Maximum Video Size	This setting configures the maximum video file size that can be uploaded to the IPICS server. This setting specifies a value in MB. To change the default, double-click the current setting and enter a new value. Valid values: 1 through 2048.	The default maximum video size specifies 4 MB.
IDC Activity Logs Pane		
Disable IDC Activity Log Upload	When you check this check box, the IDC does not upload logs to the server. 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 IDC Log Upload Frequency field and the IDC Send Logs on Rollover fields are dimmed.

Table 2-27 Client Tab in the Options Window (continued)

Setting	Description	Default Setting
IDC Log Upload Frequency (IDC to server)	When an IDC client has activity logs ready to upload to the Cisco IPICS server, the IDC application places the logs in a queue. At regular intervals, the IDC 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 IDC 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 upload interval in seconds. To change the default, double-click the current setting and enter a new value. Uploaded IDC log files are archived. Once a day, an archive utility 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 IDC log files, see "Managing an End Device from the IDC Tab" section on page 3-11. Valid values: 60 through 32767.	The default upload frequency specifies 600 seconds (10 minutes).
IDC Send Logs on Rollover	Cisco IPICS defines the IDC UserInterface.log, Authentication.log, and ChannelStatistics.log log files based on a maximum size of 1MB. When any one of these log files reaches the size limit, the system creates a new log file. When you enable this option, the Cisco IPICS server retrieves the log files from the IDC based on file size rollover and renames the uploaded log file to reflect an archive copy. If you do not enable this option, the IDC 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 IDC 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 IDC Log Upload Frequency field). Valid values: true or false.	The IDC uploads files on rollover (the check box is checked).

Table 2-27 Client Tab in the Options Window (continued)

Setting	Description	Default Setting
IDC Activity Log Update	The Cisco IPICS server retrieves activity logs from the IDC clients and updates the database with this information at regular intervals. The information is available for queries from the Activity Log window. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 30 through 32767.	The default update frequency specifies 600 seconds (10 minutes).
User Configuration Overrides		
Patch Secure Channels	This setting allows you to patch a secure channel to any other secure or unsecure channel, or to any incident or VTG. Disallowing this option prevents secure channels from being patched. **Note** Patching a secure channel into an incident is considered secure and is allowed even if patching secure channels is disallowed. You can also configure secure channel patching on a per-user basis. For more information, see the "Managing Your User Profile" section on page 4-2. Valid values: allow or disallow.	Patching secure channels is allowed.
Complex Key Settings	This setting allows or disallows all IDC clients to configure keyboard hot keys (key assignments) for individual PTT buttons and for the All Talk button. You can also configure complex key settings on a per-user basis. For more information, see the "Managing Your User Profile" section on page 4-2. Valid values: allow or disallow.	Complex key settings are allowed.

Managing IDC Versions

The Cisco IPICS server maintains a repository of one or more versions of the IDC. Users can update their IDC clients at their convenience by downloading the current version of the ID utility, as described in the "Downloading the IDC" section on page 4-16.

Note You must perform the IDC configuration procedures that are in this section before users can download and install an IDC on their PC clients.

When you initially install Cisco IPICS, an IDC package is included with the server. You must generate the IDC Installer for that version to be available for download to IDC users.

When subsequent versions of the IDC becomes available, you upload the new IDC package to the Cisco IPICS server making it available for the IDC users to download to their IDC clients.

When you log in to the Cisco IPICS server from the IDC, the IDC determines whether there is a new version to which it can or must update. You configure IDC versions to designate whether an update is required or recommended. For more information about configuring the IDC versions, see the "Changing the State of IDC Versions" section on page 2-88.

As a Cisco IPICS system administrator, you can perform the following IDC version management tasks:

- Uploading IDC Versions to the Cisco IPICS Server, page 2-88
- Changing the State of IDC Versions, page 2-88
- Deleting IDC Versions, page 2-89
- Deleting IDC Versions, page 2-89

You perform the IDC version update tasks in the IDC Versions window. For more information about this window, including how to access it, see the "Understanding the IDC Versions Window" section on page 2-87.

Understanding the IDC Versions Window

The IDC Versions window allows you to specify information about IDC versions to use for IDC updates. It also enables you to upload new IDC versions to the Cisco IPICS server, and it lists information about each of the IDC versions that have been uploaded to the Cisco IPICS server.

To display the IDC Versions window in the Administration Console, navigate to **IDC Management > IDC Versions**.

Table 2-28 describes the items in the IDC Versions window.

Table 2-28 Items in the IDC Versions Window

Item	Description	Reference
Upgrade Package field	This field identifies the IDC version to be uploaded to the Cisco IPICS server.	See the "Uploading IDC Versions to the Cisco IPICS Server" section on page 2-88
Browse button	Click this button to browse to the location that contains the IDC version upgrade package to upload to the Cisco IPICS server.	
Upload button	Click this button to upload a new IDC version to the Cisco IPICS server.	
Priority field	Specifies the order of preference for IDC versions.	
Version field	This field specifies a unique version number that is assigned to the IDC version upgrade package.	
Name field	This field allows you to assign a unique identification to the IDC version upgrade package.	
State field	This field specifies the priority (state) that is assigned to the upgrade package.	See the "Changing the State of IDC Versions" section on page 2-88

Table 2-28 Items in the IDC Versions Window (continued)

Item	Description	Reference
Delete button	Click this button to delete an IDC version from the Cisco IPICS server.	See the "Deleting IDC Versions" section on page 2-89
drop-down list for IDC version states	Choose from this list box to configure the state for the IDC versions.	See the "Changing the State of IDC Versions" section on page 2-88
Change State button	Click this button to change the state of the IDC version.	

Uploading IDC Versions to the Cisco IPICS Server

When you upload a new IDC version, the upgrade package file is copied from a specified location on your PC to the Cisco IPICS server.

To upload an IDC version to the Cisco IPICS server, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Versions** window.

Step 2 To locate the IDC version upgrade package that you obtained from Cisco click **Browse**.

Step 3 In the Choose File window, browse to the IDC 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 IDC version displays in the IDC Versions list.

Note All new IDC versions are saved, by default, in a non-operational state. IDC users cannot download the version until you change the state to Recommended or Mandatory. See the "Changing the State of IDC Versions" section on page 2-88 for more information.

Changing the State of IDC Versions

The IDC Versions window enables you to specify various states for IDC versions. You can use states to designate whether in IDC version is a recommended or required update for an IDC user. IDC states are:

- **Recommended**—When you choose this state, the next time that an IDC client polls the Cisco IPICS server, it compares the IDC version that it is running with the recommended IDC version. If the IDC client does not match the recommended version, the IDC provides the option of upgrading to the recommended version. If a user declines to upgrade, the existing IDC version continues to work.
- **Mandatory—**When you choose this state, the next time that an IDC client polls the Cisco IPICS server, it compares the IDC version that it is running with the recommended IDC version. If the IDC client does not match the mandatory version, the IDC requires upgrading to this version.

- **Not Specified**—When you choose this state, an IDC client does not compare the IDC version that it is running with this IDC version. IDC users cannot update to an IDC version that is in the Not Specified state.

You must upload an IDC version to the Cisco IPICS server before it becomes available in any of the fields in the IDC Versions window.

To change the state of IDC versions for automatic updates, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Versions** window.

Step 2 Check the check box next to the IDC version that you want to change.

Step 3 From the drop-down list, choose the desired state.

Step 4 Click the **Change State** button.

Deleting IDC Versions

To delete IDCC versions, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Versions** window.

Step 2 Check the check box of the IDC 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 IDC version.

This version of the IDC is completely removed from the server.

If you do not want to delete the IDC version, click **Cancel**.

Managing IDC Alert Tones

IDC 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 Cisco IPICS server. The alert tone set is packaged in a .zip file that you can upload to the server and that IDC users can then download on to their client machines.

An alert tone set is associated with an ops view; therefore, each IDC user can see only one tone set based on the ops view association. For more information about ops views, see Chapter 7, “Configuring and Managing Cisco IPICS Operational Views.”

The IDC alert tone feature requires the use of compatible alerting tone files. These files must be:

- Pulse Code modulation (PCM) .wav files

- 8 bits monaural samples at 8000 Hz sampling rate
- Little Endian, 16-bit mono codec
- Normalized to –2 db
- Begin and end with silence (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 an IDC Alert Tone Set, page 2-90
- Adding IDC Alert Tone Sets, page 2-91
- Viewing or Editing IDC Alert Tone Sets, page 2-92
- Associating an Alert Tone Set to an Ops View, page 2-92
- Deleting IDC Alert Tones, page 2-93

Creating an IDC Alert Tone Set

To provide the alert tones that get downloaded to the IDC, you must first create an IDC 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 IDC is installed, navigate to the following directory:

C:\Program Files\Cisco Systems\Cisco IDC 4.5

Step 2 Create a new empty directory and extract the example-toneset.zip file and all its contents in to the new director.

This file contains a sample alert tone set.

Step 3 Add any desired sound files in .wav format to this directory.

These files must be normalized to –2 db and must be PCM 8KHz signed, Little Endian, 16-bit mono codec.

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 IDC.

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*” represents the .wav file to be played, and “*displayName*” is the text that displays on the IDC.

Step 6 Save the example tone set .xml file and rename the .xml file to a name that identifies the tone set to you.

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 that you do not want from the directory.

Step 8 Navigate to the directory that contains the .xml and .wav files and select all of the .wav files and the .xml file.

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 an IDC user to press a button on the IDC 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 IDC alert tone set to the Cisco IPICS server.

See the "Associating an Alert Tone Set to an Ops View" section on page 2-92 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 IDC Alert Tone Sets

To add a new IDC alert tone set, perform the following procedure.

Tip The Stop alert tone should be included in each tone set that you upload to the Cisco IPICS server. This alert tone allows 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 an IDC Alert Tone Set" section on page 2-90 for information about how to create an alert tone set.

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

Step 2 Click **Add**.

A blank alert tone detail window displays.

Step 3 In the Set Name field, enter a name for the alert tone set.

Step 4 In the Description field, enter a description for the alert tone set.

Step 5 Click the **Browse** button use the File Upload pop-up window to identify the files to upload.

Step 6 Click **Save**.

The tone set gets uploaded to the server and is available for use by IDC 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 7 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 2-92.

Viewing or Editing IDC Alert Tone Sets

To view or edit the IDC alert tone sets that are available for use in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

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 2-92.

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 IDC 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 the **IDC Management > Alert Tones** window.

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; then, click **>** or **<**. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the ops views; 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.

IDC users can now only see the alert tone set that is in the ops view to which they belong.

Note The user(s) that you want to have access to the tone set must be assigned the appropriate permissions in Cisco IPICS to see the tone set, and must also belong to the same ops view to which the tone set is associated.

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

Deleting IDC Alert Tones

To delete IDC tones, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > Alert Tones** window.

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 IDC 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 the IDC Installer

Before an IDC user can download a new IDC version to a clients, you must configure the IDC Installer.

The IDC Installer installs the IDC on IDC client machines. The IDC installer, called idcsetup.exe, downloads to an IDC client when a IDC user clicks the **Download IDC** link in the Home drawer, as described in the "Downloading the IDC" section on page 4-16.

As a Cisco IPICS system administrator, you can upload a new IDC package and generate the IDC Installer as described in the "Generating the IDC Installer" section on page 2-94.

You perform these tasks in the IDC Installer window. For more information about this window, including how to access it, see the "Using the IDC Installer Window" section on page 2-94.

Using the IDC Installer Window

The IDC Installer window contains configuration information that is necessary to generate an IDC installer.

To display the IDC Installer window, navigate to the IDC Management drawer in the Cisco IPICS Administration Console and click the **IDC Installer** link.

The Installer Status field displays the date and time that an idcsetup.exe file was last generated, and displays the IP address defined by the bundled idc.ini file. These files are used to install the IDC.

Generating the IDC Installer

Generating an IDC Installer installs a new IDC version package. It also makes the IDC version package available for download from the **Download IDC** link in the Home drawer (see the "Downloading the IDC" section on page 4-16).

For information about configuring additional IDC options, see the "Managing Cisco IPICS Options" section on page 2-77.

To generate an IDC Installer, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Installer** window.

Step 2 Take one of these actions to specify the IP address that the IDC uses to contact the Cisco IPICS server:

- To specify the IP address of the Cisco IPICS server that you are accessing to generate the IDC installer, choose the radio button that appears next to the IP address.
- To choose a different IP address, click the **Other** radio button and enter the IP address.

  If you use this option, the IP address that you enter should be tested in the network domain that is supported with that server to ensure that NAT or firewall restrictions do not prevent the IDC from connecting to that server.

In a high availability deployment, specify the IP address of the primary server. Information about the secondary server is provided to the IDC automatically so that the IDC properly fails over to the secondary server if the primary server goes down.

Step 3 In the HTTP Port field, enter the port number that is used for non-secure HTTP communication between the IDC and the server.

Step 4 In the HTTPS Port field, enter the port number that is used for secure HTTPS communication between the IDC and the server.

Note Cisco recommends that you use the default HTTP and HTTPS ports that are listed in the IDC Installer Configuration area. The IP address, HTTP port, and HTTPS port fields affect only the IDC installer and do not have an immediate effect on IDC clients that have already been installed on user PCs. If you need to change these values, Cisco recommends that you notify all users that they need to download and reinstall the IDC using the new idcsetup.exe that is generated after you save the changes to these values.

Step 5 From the IDC Version To Be Used For The IDC Installer drop-down list, choose the version number of the IDC that you want the users install.

The drop-down list should be populated with the version numbers of the idcinst.exe files that have been uploaded to the Cisco IPICS server. See the "Managing IDC Versions" section on page 2-86 for more information.

Note There is only one IDC installer and all IDC users who use that installer automatically receive a complete application of that IDC version.

Step 6 Click **Save**.

IDC users can now download a new version of the IDC application, as described in the "Downloading the IDC" section on page 4-16.

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

Managing IDC Regions

An IDC region is a grouping of channels on the IDC. Channels (radios) are divided among regions. Channels, radios, and VTGs are configured to belong to a particular region when they are created. You can configure regions (views) that the IDC displays to a user.

When you configure new regions in the Cisco IPICS server, they are represented by tabs that display in the IDC. The position of the region in the IDC Regions window in the Administration Console determines where the region displays on the IDC.

You create regions in the **IDC Management > IDC Regions** window in the Administration Console. You can configure up to 20 regions.

You can add new IDC regions, as well as edit and delete existing regions, as described in the following procedures:

- Understanding the IDC Regions Window, page 2-95
- Adding IDC Regions, page 2-96
- Viewing or Editing IDC Regions, page 2-97
- Deleting IDC Regions, page 2-97

Understanding the IDC Regions Window

The IDC Regions window allows you to create new IDC regions that display on the IDC. You can also edit and delete existing IDC regions in this window.

The IDC Regions window lists information about each of the IDC regions that have been created in the Cisco IPICS server.

To display the IDC Regions window, navigate to the **IDC Management > IDC Regions** window.

Table 2-29 describes the items in the IDC Regions window.

Table 2-29 Item in the IDC Versions Window

Item	Description	Reference
Name field	This field specifies the name of the IDC regions.	See the "Adding IDC Regions" section on page 2-96 and the "Viewing or Editing IDC Regions" section on page 2-97
Short Name field	This field specifies the shortened name of the regions.	
Position field	This field specifies the position of the regions on the IDC display.	
Add button	Click this button to add a new IDC region to the Cisco IPICS server.	See the "Adding IDC Regions" section on page 2-96
Delete button	Click this button to delete an IDC region.	See the "Deleting IDC Regions" section on page 2-97

Adding IDC Regions

To add a new IDC region, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Regions** window.

Step 2 Click **Add**.

A blank New IDC Region detail window displays.

Note This button is dimmed if 20 regions are already configured. In this case, you must delete a region before you can add a new one.

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

Step 4 In the Short Name field, enter a condensed name for the region.

Tip The short name can be a shortened version of the full name or the same as the region position.

Step 5 From the Position drop-down list, choose a position for the region.

Position indicates where the region appears in the Regions list in the IDC. Position 1 indicates the top position, and 6 indicates the bottom position. If you want to assign a region to a position that is in use, you must delete the in-use region first, as described in the "Deleting IDC Regions" section on page 2-97.

Step 6 (Optional) In the Description field, enter a description of the region.

Step 7 Click **Save**.

The region displays in the list of IDC regions and is available to assign to a channel/VTG while creating/updating channel/VTGs.

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

Viewing or Editing IDC Regions

To view or edit the IDC regions that are available for use in Cisco IPICS, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Regions** window.

Step 2 In the Name column, click the link for the IDC region to view or edit.

A window displays current information about the region that you choose.

Step 3 To edit the information for the region, take any of the following actions:

- In the Name field, enter a new name for the region.
- In the Short Name field, enter a new condensed name for the region.
- From the Position drop-down list, choose the position that the region appears in the Regions list in the IDC.
- In the Description field, enter a new description for the region.

For a description of the fields in this window, see the "Adding IDC Regions" section on page 2-96.

Step 4 Click **Save**.

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

Deleting IDC Regions

To delete IDC regions, perform the following procedure. When you delete an IDC region, any associated channels and VTGs are moved to region 1.

Procedure

Step 1 From the Administration Console, navigate to the **IDC Management > IDC Regions** window.

Step 2 Check the check box to the left of the region that you want to delete.

Step 3 Click **Delete**.

The region that you deleted is no longer available for use by the IDC users.

Configuring LDAP

Cisco IPICS lets you use the Lightweight Directory Access Protocol (LDAP) to authenticate against an Active Directory (AD) server users who access Cisco IPICS.

Note The values that are configured in the AD for a user in the **Display name** field in the General tab and the **User logon name** field in the Account tab must be identical. If they are not, the user cannot log in to Cisco IPICS.

This section describes how to configure the general settings that are required for LDAP authentication of users. In addition, you must make the following settings:

- Create an ops view and enable it for LDAP (or enable the System ops view for LDAP). For instructions, see the "Adding Ops Views" section on page 7-11.
- Configure users that are to use LDAP authentication to belong to the ops view that is enabled for LDAP. For instructions, see the "Choosing an Ops View to Which a User Belongs" section on page 3-24.

To configure general settings for LDAP authentication, perform the following procedure:

Procedure

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

Step 2 In the LDAP Configuration window, take these actions:

a. In the Host Name / IP Address field, enter the host name or the IP address of the LDAP server in your network.

b. In the LDAP Port field, enter the port number on the LDAP server that Cisco IPICS uses to communicate with that server.

Typically, this port number is 389 for non-secure communication or 636 for secure communication. The port number that you enter must match the port number that is configured in the LDAP server.

c. In the LDAP Timeout field, enter the maximum number of seconds that can pass before a connection from Cisco IPICS to the LDAP server fails.

The default value is 30. Valid values are 5 through 180.

d. Check the **Use LDAPS** check box if you want to use secure LDAP.

In this case, Cisco IPICS downloads the SSL certificate from the LDAP server and uses this certificate to encrypts data that is sent between Cisco IPICS and the LDAP server. The certificate is downloaded when you save the configuration settings that you are making.

When this check box is checked, the Certificate Security Configuration fields appear, which show the serial number and expiration date of the LDAP certificate

Step 3 Click **Save**.

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 IDC, 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 7, "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 4, "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 3-1
- Managing User Groups, page 3-29

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
- Communicate through the IDC with associated dial-in users

- Download the IDC installer

This section describes the following user management activities:

- Understanding the Users Window, page 3-2
- Adding a User, page 3-4
- Managing User Information, page 3-6
- Associating Resources with a User, page 3-18
- Managing Ops Views for a User, page 3-24
- Managing Prompts for a User, page 3-25
- Viewing Information about VTGs in which a User is a Participant, page 3-26
- Managing User Status, page 3-26

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 1-12
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 3-4

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 3-6
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 3-24
End Device Status field	Can display these icons: —Audio of the IDC, 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 IDC, 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 3-27 and the "Managing an End Device from the User Management Window" section on page 3-10
Status field	Indicates whether a user is enabled or disabled	See the "Changing User Status" section on page 3-27
Prompt	Indicates whether a spoken name prompt is recorded for the user	See the "Managing Prompts for a User" section on page 3-25
Password Expiration field	Indicates when the password of the user expires	See the "Managing Cisco IPICS Options" section on page 2-77
Account Status field	Shows if a user account is locked or available	See the "Locking or Unlocking a User Account" section on page 3-27
Add button	Provides the ability to add a new Cisco IPICS user	See the "Adding a User" section on page 3-4
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 3-28
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 3-27 and the "Locking or Unlocking a User Account" section on page 3-27
End Device drop-down list	Provides the ability to perform several activities for the IDC, 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 3-10

Table 3-1 Items in the Users Window (continued)

Item	Description	Reference
Associations button	Displays the Associations window for a user	See these sections: • Associating PTT Channels with a User, page 3-18 • Associating Phones with a User, page 3-19 • Associating Policies with a User, page 3-20 • Viewing Information about VTGs in which a User is a Participant, page 3-26
Display Controls		
Rows per page drop-down list	Specifies the number of rows of users that are included in a users list page	See the "Navigating Item Lists" section on page 1-13
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 2-27.

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 the following 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 appears 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.

If you are using LDAP to authenticate against an AD server users who access Cisco IPICS, this User Name must be identical to the value that is configured for the user in these fields in the AD:

- **Display name** in the General tab
- **User logon name** in the Account tab

b. In the First Name field, enter the First name of the user.

Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (').

c. In the Last Name field, enter Last name of the user.

Valid characters include: 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 IDC. (The actual characters in the password are represented by asterisks (*)).

You specify requirements for passwords, including length and character requirements, in the **Administration > Options** window.

Valid characters include: 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 3-7.
In the General tab, assign one or more Cisco IPICS roles to the user.	See the "Managing Roles for a User" section on page 3-8.

Table 3-2 Tasks for Adding a Cisco IPICS User (continued)

Task	Reference
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 3-24.
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 3-9.
In the IDC tab, designate how a user communicates through the IDC, choose whether IDC log files are on or off, and specify debug levels for IDC log files.	See the "Managing an End Device from the IDC Tab" section on page 3-11.
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 3-13.
Associate ops views with the user.	See the "Managing Ops Views for a User" section on page 3-24.

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 3-6
- Managing Address Information for a User, page 3-7
- Managing Roles for a User, page 3-8
- Managing Dial Login Information for a User, page 3-9
- Managing an End Device for a User, page 3-10
- Managing Communications Preferences for a User, page 3-13

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 include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Last Name	Last name of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Password	Password that the user enters when logging in to Cisco IPICS or the IDC. (The actual characters in the password are represented by asterisks (*)). You specify requirements for passwords, including length and character requirements, in the **Administration > Options** window. Valid characters include: 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 include: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :
Address (cont)	Additional street address information. Valid characters include: alphanumeric characters, spaces, and these special characters include: . , – ‘ # ( ) / :
City	City of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
State/Province	State or province of the user. Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Country	Country of the user. Valid characters include: alphanumeric characters, space, and period (.).
Zip/Postal Code	Zip code or postal code of the user. Valid characters include: alphanumeric characters, space, and period (.).
E-mail	E-mail address of the user. Valid characters include: 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 inactive VTGs, activating VTGs to begin conferences, and adding or removing participants in inactive VTGs 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 IDC, 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 IDC 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 above 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 D, "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 6-20.

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 or when accessing the TUI. Valid characters include: 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 **Administration > Options** window. Valid characters include: 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 2-27.

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

An end-device can be an IDC, a Cisco Unified IP Phone, or a 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 3-10—Provides the ability to mute or unmute an end device, disable or enable an end device, and obtain IDC log files
- Managing an End Device from the IDC Tab, page 3-11—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 an End Device from the Associations Tab, page 3-12—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 end device of a user. Not all end devices support all of these activities.

- Mute or unmute the device
- Disable or enable the device
- 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.

Note The setting that you make by using this procedure do not affect the mobile client.

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 End Device Drop-Down List Options

Option	Explanation	Notes
Set Listen Only	Disables the transmission of audio from the IDC or Cisco Unified IP Phone, which restricts a user to listening only.	Affects any IDC or Cisco Unified IP Phone that a user logs in to, and affects any phone from 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 IDC Tab" section on page 3-11 and the "Managing an End Device from the Associations Tab" section on page 3-12.
Unset Listen Only	Enables the transmission of audio from the IDC or Cisco Unified IP Phone.	
Disable Audio	Disables the microphone and speaker on the IDC or a Cisco Unified IP Phone that is logged in to the Cisco IPICS service, which prevents a user from listening and talking.	Affects any IDC 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 the IDC or a Cisco Unified IP Phone that is logged in to the Cisco IPICS service, which allows a user to listen and talk.	

Managing an End Device from the IDC Tab

From the User Management: Users > *Username* > IDC tab, you can perform the following activities for the end device of a user:

- Designate how a user communicates in VTGs
- Obtain IDC log files
- Turn IDC log files on or off and set log levels

To manage the end device of a user from the User Management: Users > *Username* > IDC 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 **IDC** tab.

Step 4 To designate how a user communicates in VTGs, check the appropriate check boxes in the IDC Info area:

- Disable Audio—Disables the microphone and speaker on the IDC. Does not affect a Cisco Unified IP Phone, a phone from which a user dials in to the TUI, or a mobile client.
- Listen Only—Disables the transmission of audio from the IDC, Cisco Unified IP Phone, dial-in phone, which restricts a user to listening only. Does not affect a mobile client.
- Allow Latch—User can use the latch feature on the IDC or Cisco Unified IP Phone.
- Advanced IDC 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 the IDC.
- Allow Complex Key Setting—User can configure keyboard hot keys (key assignments) for individual PTT buttons and for the All Talk button.
- Allow Secure Channel Patch —User can patch a secure channel to any other secure or unsecure channel, or to any incident or VTG.

  Patching a secure channel into an incident is considered secure and is allowed even if patching secure channels is disallowed.

Note The Allow Complex Key Setting and Allow Secure Channel Patch options will take effect only when they are globally allowed. For more information, see "Managing Cisco IPICS Options" section on page 2-77.

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

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

Managing an End Device from the Associations Tab

From the User Management: Users > *Username* > Associations tab, you can perform the following activities for the end device of a user:

- Enable or disable the latch feature for the IDC or the Cisco Unified IP Phone
- Enable or disable Listen Only for the IDC or the Cisco Unified IP Phone
- Enable or disable Voice Activation Detection (VAD) for the IDC

You can perform these activities for any or all channels with which the user is associated.

To manage the IDC or mobile client 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 End Device Status drop-down list, choose the desired option.

Table 3-7 describes these options.

Table 3-7 Change End Device Status Drop-Down List Options

Option	Explanation
Allow Latch	Allows the user to use the latch feature on the IDC or Cisco Unified IP Phone.
Disallow Latch	Prevents the user from using the latch feature on the IDC or Cisco Unified IP Phone.
Set Listen Only	Disables the transmission of audio from the IDC, Cisco Unified IP Phone, or dial-in phone, which restricts a user to listening only.
Unset Listen Only	Enables the transmission of audio from the IDC, Cisco Unified IP Phone, or dial-in phone.
Enable Audio	Enables the microphone and speaker on the IDC or a Cisco Unified IP Phone that is logged in to 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 the IDC or Cisco Unified IP Phone that is logged in to 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 6, "Using the Cisco IPICS Policy Engine" and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

Note Users can update their own preferences in their user profiles. For more information, see the "Managing Communications Preferences" section on page 4-7.

When you specify communication preferences, you can provide the following information:

- Notification Preferences—Specifies how Cisco IPICS contacts a user when a user-associated policy executes. Also used by Cisco IPICS when a dispatcher initiates a notification or dial out to invite you to join an active VTG. Can be any combination of one or more e-mail, Short Message Service (SMS), or pager addresses.
- Radio Preferences—Specifies one or more connect numbers for radios that are used by the IPICS Connect feature.
- IDC Dialer Preference—These fields specify information that is required by Cisco Unified Communications Manager and Cisco Unified Communications Manager Express for the IDC dialer feature.
- Dial Preferences—One or more telephone numbers at which Cisco IPICS contacts a user when a user-associated policy executes. Also used by Cisco IPICS when a dispatcher initiates a dial out to invite you to join an active VTG.

This section includes these topics:

- Viewing, Adding, Editing, or Deleting Communications Preferences, page 3-14
- Changing the Order of Dial Preferences, page 3-17
- Changing the Order of Radio Preferences, page 3-18

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:

- Notification Preferences
  - Type—Method by which the user is notified. Can be Email (specifies that notification is sent to an e-mail address); Pager (specifies that notification is sent to a pager through an e-mail gateway); or SMS (specifies that notification is sent to an SMS through an e-mail gateway)
  - Number/Address (under Notification Preferences)—E-mail address for the corresponding notification type
- Radio Preferences:
  - Type—Type of radio that a user is using
  - Value— IPICS connect number for the radio

- IDC Dialer Preference (used for the IDC dialer feature):
  - IDC Dialer Phone Number—Unique number that the IDC requires to register with Cisco Unified Communications Manager (CUCM) or Cisco Unified Communications Manager Express (CME) when the user logs in. Displays on an end device when the IDC places a call to a device that is configured to display caller ID. This parameter must also be configured in CUCM or CME.
  - End User Name—CUCM or CME end user name that is configured for the user.
  - End User Password—CUCM or CME end user password that is configured for the user.
  - Confirm End User Password—Confirmation of the password in the End User Password field
- Dial Preferences:
  - Type—Description of the location to be dialed, such as Business, Car, or Home
  - Dial Number—Telephone number of the corresponding location type

Step 4 To add, edit, or delete notification preferences, take the appropriate actions in the Notification Preferences area:

- 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 radio preferences, take the appropriate actions in the Radio Preferences area:

- To add a radio preference, follow these steps:
  a. Click **Add**.
  b. From the drop-down list, choose the type of radio that you are configuring the IPICS Connect number for.
  c. In the field next to the drop-down list, enter the IPICS Connect number for the radio.

Note If you choose an ISSIG as the radio type, you must enter a 6-digit hexadecimal value for the P25 subscriber unit ID instead of an IPICS Connect number for the radio. This assigns the IPICS user an P25 subscriber unit ID, and associates the P25 subscriber unit ID to the ISSIG where this user needs to be homed.

d. Click **Done**.

e. Repeat these steps as needed to add more dial preferences.

- To edit a radio preference, follow these steps:
  a. Check the check box next to the radio 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, choose the type of radio for which you are configuring the IPICS Connect number.

  d. In the field next to the drop-down list, enter the IPICS Connect number for the radio.

  e. Click **Update**.
- To delete a radio preference, follow these steps:
  a. Check the check box next to the radio 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 To add or edit IDC dialer preferences, take the appropriate actions in the IDC Dialer Preference area:

a. In the IDC Dialer Phone Number field, enter a unique number that the IDC requires to register with CUCM or CME when the user logs in. Displays on an end device when the IDC places a call to a device that is configured to display caller ID. This parameter must also be configured in CUCM or CME.

b. In the End User Name field, enter the CUCM or CME end user name that is configured for the user.

c. In the End User Password field, enter the CUCM or CME end user password that is configured for the user

d. In the Confirm End User Password field, re-enter the password that you entered in the End User Password field.

Step 7 To add, edit, or delete dial preferences, take the appropriate actions in the Dial Preferences area:

- 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 8 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 9 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**.

Changing the Order of Radio Preferences

You can specify the order of the radios in your radio preferences. This function is reserved for future use.

To specify the order of the radio 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 radio preference type that you want to move to a different position in the list.

Step 4 Click the up arrow button to move the radio 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 radio preferences.

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

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 3-18
- Associating Phones with a User, page 3-19
- Associating Policies with a User, page 3-20
- Associating Radios with a User, page 3-22

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 IDC of the user
- Causes the channels to appear on a Cisco Unified IP Phone when the user accesses the Cisco IPICS 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. For more information, see the "Associating Users to PTT Channels" section on page 2-17.

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 the following 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 Associations button 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 1-12.

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 Phones with a User

When you associate phones (direct dial numbers) with a user, the user can communicate directly with those phones by using the policy engine direct dial feature.

Before You Begin

Configure one or more direct dial numbers for the phones that you want to associate with a user. For information about configuring direct dial numbers, see the "Managing Direct Dial Numbers" section on page 8-29.

To associate phones 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 the following 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 Associations button is dimmed if you do not check a user or if you check more than one user.

Step 3 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 4 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 5 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, press **Shift+click** or press **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 6 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 6-16.
- Activate the policy by calling the policy engine. For related information, see the "Using the Policy Engine Telephony User Interface" section on page 6-20.
- 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 6-15.

Procedure

Step 1 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of the following 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 Associations button is dimmed if you do not check a user or if you check more than one user.

Step 3 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 4 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 5 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, press **Shift+click** or press **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 6 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 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 click the up arrow button or the down arrow button to move it up or down in the list.

Associating Radios with a User

Associating radios with a user causes the radios that you choose to appear as options on the IDC for the user. In addition, you can choose whether channel selectors and controls are accessible for each radio that is assigned to the user.

You must have Cisco IPICS administrator privileges to associate radios with users and to configure channel selector and control privileges.

For information about configuring radios that you can associate with users, see Chapter 9, "Managing Radios and Radio Descriptors."

Note You can also associate radios with a user from the Radios window. For information, see the "Associating a User to a Radio From the Radios Window" section on page 9-15.

Designating Radios to Associate with a User

To associate radios 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 the following 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 Associations button is dimmed if you do not check a user or if you check more than one user.

Step 3 In the Associations window, click the **Radios** tab.

This tab shows a list of the radios that are associated with the user and provides information about each radio.

Step 4 Click **Add**.

The Search Results window appears.

Step 5 In the Search Results window, locate one or more radios 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 1-12.

Step 6 In the Search Results window, check the check box next to each radio that you want to associate with this user and then click **OK**.

The radios that you choose appear in the list of associated radios.

If you want to remove any radio from this list, click the check box next to the radio, click **Delete**, and then click **OK** in the confirmation dialog box that appears.

Designating Radio Permissions

A Cisco IPICS administrator can designate the following permissions for each radio that is associated with a user. The permissions apply only to the radio that you are configuring.

- Channel Selector Permissions—Enables the user to tune to the channels that you specify on the radio that you are configuring.
- Control Function Permissions—Enables the user to use the controls that you specify on the radio that you are configuring.

If you do not designate any channel selectors or controls, the user can listen to channels on the radio, but cannot change (retune) channels or control any radio functions.

To designate permissions for a radio that is associated 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 the following 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 Associations button is dimmed if you do not check a user or if you check more than one user.

Step 3 In the Associations window, click the **Radios** tab.

Step 4 Check the check box next to the radio for which you want to designate permissions.

Step 5 To designate the channels that a user can select from the radio, take these actions:

a. From the Radio Permissions drop-down list, choose **Channel Selector Permissions**.

The User Radio Permissions window displays. This window shows the following information:

- Available Channel Selectors list—Channels that are configured for the radio
- Permitted Channel Selectors list—Channels on which the user can communicate, or on which the user will be able to communicate after you click **Save**

b. Take any of these actions:

- To move a channel from the one list to the other, click the channel to highlight it and then click > or <. Or, double-click the channel.
- To move several channels from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the channels and then click > or <.
- To move all channels from one list to the other at one time, click >> or <<.

c. Click **Save** to save your changes.

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

Step 6 To designate the controls that a user can access on the radio, take these actions:

a. From the Radio Permissions drop-down list, choose **Control Function Permissions**.

The User Radio Permissions window displays. This window shows the following information:

- Available Control Functions list—Controls that are available on the radio
- Permitted Control Functions list—Controls that the user can use, or that the user will be able to use after you click **Save**

b. Take any of these actions:

- To move a control function from the one list to the other, click the channel to highlight it and then click **>** or **<**. Or, double-click the control function.
- To move several control functions from one list to the other at one time, press **Shift+click** or press **Ctrl+click** to select the control functions and then click **>** or **<**.
- To move all control functions from one list to the other at one time, click **>>** or **<<**.

c. Click **Save** to save your changes.

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

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 3-24
- Associating Ops Views with a User, page 3-25

Choosing an Ops View to Which a User Belongs

A user can belong to only 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 the ops views that can access a user, from the User Management drawer in the Cisco IPICS Administration Console, click **Users**; then, 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 the following actions to associate ops views with a user:

- Click the link for the user in the User Name column; then, 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 Associations 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, press **Shift+click** or press **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 8-18.

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 5, "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 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 2 Take either of the following 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 Associations button is dimmed if you do not check a user or if you check more than one user.

Step 3 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 IPICS or removing a user from the system. For detailed information about managing user status, see the following sections:

- Changing User Status, page 3-27
- Locking or Unlocking a User Account, page 3-27
- Recovering a Deleted System Administrator User, page 3-28
- Deleting a User, page 3-28

Changing User Status

A user can have either of these statuses:

- Enabled—User can log in to Cisco IPICS from an end device (IDC, Cisco Unified IP Phone, dial-in phone, and mobile client).
- Disabled—User cannot log in to Cisco IPICS from any end device (IDC, Cisco Unified IP Phone, dial-in phone, and mobile client).

  If you disable a user who is currently logged in to Cisco IPICS, that login session is terminated automatically.

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 the following 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 in to 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 in to 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 assistance, contact Cisco.

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 the following 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 a deleted system administrator user ID 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, 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 3-4.

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 3-29
- Adding a User Group, page 3-31
- Adding Members to a User Group, page 3-32
- Managing Ops Views for a User Group, page 3-32
- Changing the Name of a User Group, page 3-34
- Viewing Information about VTGs in Which a User Group is a Participant, page 3-34
- Deleting a User Group, page 3-35

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 1-12
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 3-31
Ops View field	Ops view to which the user group belongs	See the "Managing Ops Views for a User Group" section on page 3-32
Add button	Provides the ability to add a new user group	See the "Adding a User Group" section on page 3-31
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 3-35
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 3-34
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 1-13
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 the following 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 appears 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 unique 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 3-32
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 3-32.

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.

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 IDC, Cisco Unified IP Phone, dial-in phone, and mobile client of the user is disabled, so user cannot talk or listen in a channel or VTG
  - —Microphone of the IDC, Cisco Unified IP Phone, dial-in phone, and mobile client 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 1-12.

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 3-33
- Associating Ops Views with a User Group, page 3-33

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 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 the following 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; 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 appears 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, press **Shift+click** or press **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 5, “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 the following actions:

- In the User Group Name column, click the link for the user group; 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; 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.

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**.

CHAPTER 4

Performing Cisco IPICS User Tasks

All Cisco IPICS users are assigned a user role in the system. 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 IDC client application to your PC.

The user role may be your only role, or you may have one or more additional roles, such as system administrator, ops view administrator, dispatcher, or operator.

This chapter contains information about the Cisco IPICS user functionality and includes the following sections:

- Logging in to Cisco IPICS, page 4-1
- Managing Your User Profile, page 4-2
- Managing User Associations, page 4-12
- Downloading the IDC, page 4-16

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 automatically converts 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 4-2.

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 3-1.

To access your user profile, navigate to **My Profile** from the Home drawer. See the "Managing Your User Profile" section on page 4-2 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 4-12 for more information about managing user associations.

To download the IDC client application to your PC, click the **Download IDC** link from the Home drawer. See the "Downloading the IDC" section on page 4-16 for more information about downloading the IDC client application.

Managing Your User Profile

Your user profile, also referred to as *My Profile*, includes your name, password, default location, communications preferences, 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 the following information tabs: General, Address, Dial Login, IDC, and Communications. 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 4-1 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 3-1 and the "Managing User Groups" section on page 3-29.

Table 4-1 General Tab Fields

Field	Description
User Name	*Display only.* This field specifies the user name that was 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 4-1 General Tab 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.
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** Cisco IPICS displays 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.
Account Status	*Display only*. This field specifies the status of the user account.
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.
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 7, “Configuring and Managing Cisco IPICS Operational Views.”

Step 3 Table 4-2 describes the fields in the Address tab.

Table 4-2 Address Tab Fields

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 (@)

Step 4 Table 4-3 describes the fields in the Dial Login tab.

Table 4-3 Dial Login Tab Fields

Field	Description
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.
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

Table 4-3 Dial Login Tab Fields (continued)

Field	Description
Digit Password (PIN)	This field specifies the password that you enter when you access the Cisco IPICS service from a Cisco Unified IP Phone or personal identification number (PIN) that you enter when you access 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 your entry in the Digit Password field.
Default Location	By default, this field specifies the location that displays on your IDC. Choose a location from the drop-down list. **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. For more information about locations, see the "Managing Locations" section on page 2-27.

Step 5 Table 4-4 describes the fields in the IDC tab.

Table 4-4 IDC Tab Fields

Field	Description
IDC 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 IDC Permissions—Specifies whether you are enabled for the following features on the IDC: – Channel multiselect for voice and tone transmissions – Alert tones transmissions – DTMF tones transmissions – All Talk channel transmissions • Allow Complex Key Setting—Allows you to configure keyboard hot keys (key assignments) for individual PTT buttons and for the All Talk button. • Allow Secure Channel Patch —Allows you to patch a secure channel to any other secure or unsecure channel, or to any incident or VTG. Disallowing this option prevents secure channels from being patched. Patching a secure channel into an incident is considered secure and is allowed even if patching secure channels is disallowed. **Note** The Allow Complex Key Setting and Allow Secure Channel Patch options will take effect only when they are globally allowed. For more information, see "Managing Cisco IPICS Options" section on page 2-77. For more information about the IDC, see *IPICS Dispatch Console User Guide* for this release.

Step 6 Table 4-5 describes the fields in the Communications tab.

Table 4-5 Edit Communications Tab Fields

Field	Description
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 4-7.
Radio Preferences	This field specifies the IPICS Connect number for radios that support this feature. To manage your radio preferences, see the "Managing Communications Preferences" section on page 4-7.

Table 4-5 Edit Communications Tab Fields (continued)

Field	Description
IDC Dialer Preference	These fields specify information that is required by Cisco Unified Communications Manager and Cisco Unified Communications Manager Express for the IDC dialer feature. To manage your IDC dialer preferences, see the "Managing Communications Preferences" section on page 4-7.
Dial Preferences	This field specifies one or more telephone numbers. To manage your dial preferences, see the "Managing Communications Preferences" section on page 4-7.

Step 7 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 invite you to join an active VTG. For more information about notifications, see Chapter 6, "Using the Cisco IPICS Policy Engine."

When you specify communication preferences, you can provide the following information:

- Notification Preferences—Specifies how Cisco IPICS contacts you when a user-associated policy executes. Also used by Cisco IPICS when a dispatcher initiates a notification or dial out to invite you to join an active VTG. Can be any combination of one or more e-mail, Short Message Service (SMS), or pager addresses.
- Radio Preferences—Specifies one or more direct connect numbers for Nextel radios. This information is used by the IPICS connect feature.
- IDC Dialer Preference—These fields specify information that is required by Cisco Unified Communications Manager and Cisco Unified Communications Manager Express for the IDC dialer feature.
- Dial Preferences—One or more telephone numbers at which Cisco IPICS contacts you when a user-associated policy executes. Also used by Cisco IPICS when a dispatcher initiates a dial out to invite you to join an active VTG.

Note A Cisco IPICS operator can configure user notification preferences. For more information, see the "Managing Communications Preferences for a User" section on page 3-13.

This section includes the following topics:

- Viewing, Adding, Editing, or Deleting Notifications Preferences, page 4-8
- Viewing, Adding, Editing, or Deleting Dial Preferences, page 4-11
- Specifying the Order of Dial Preferences, page 4-12

Viewing, Adding, Editing, or Deleting Notifications Preferences

You can view, add, edit, or delete notification 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.

The Notifications Preferences pane displays the following information:

- Type—Method by which you get notified:
  - Email—Cisco IPICS sends notification to an e-mail address that you specify.
  - Pager—Cisco IPICS sends notification to a pager through an e-mail gateway.
  - SMS—Cisco IPICS sends notification to an SMS through an e-mail gateway.
- Number/Address—This field specifies the e-mail address for the corresponding notification type.

Step 3 Take the desired action:

- To add a notification preference:
  a. Click **Add**.
  b. From the drop-down list, choose a method by which to receive notifications (Email, 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, 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, choose a method by which you want to receive notifications.
  d. 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, specify the e-mail address of the gateway through which the message is sent to the device.
  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 Click **Save** to save your changes.

Viewing, Adding, Editing, or Deleting Radio Preferences

You can view, add, edit, or delete radio 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.

The Radio Preferences pane displays the following information:

- Type—Radio descriptor for a serial radio that supports the IPICS Connect feature
- Value—IPICS Connect number of the associated radio

Step 3 Take the desired action:

- To add a radio preference, follow these steps:
  a. Click **Add**.
  b. From the drop-down list, choose the type of radio for which you are configuring the IPICS Connect number.
  c. In the field next to the drop-down list, enter the IPICS Connect number for the radio.
  d. Click **Done**.
  e. Repeat these steps as needed to add more dial preferences.
- To edit a radio preference, follow these steps:
  a. Check the check box next to the radio 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, choose the type of radio for which you are configuring the IPICS Connect number.
  d. In the field next to the drop-down list, enter the IPICS connect number for the radio.
  e. Click **Update**.
- To delete a radio preference, follow these steps:
  a. Check the check box next to the radio 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 4 Click **Save** to save your changes.

Specifying the Order of Radio Preferences

You can specify the order of the radios in your radio preferences. This feature is reserved for future use.

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.

Viewing or Updating IDC Dialer Preference

You must configure the IDC dialer preference items if you will use the IDC dialer feature. In addition, you must configure the CUCM or CME to which the IDC registers with the same information. (For more information about the IDC dialer feature, see *IPICS Dispatch Console User Guide* for this release.

You can view, or update IDC dialer 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.

The IDC Dialer Preferences pane includes these fields:

- IDC Dialer Phone Number—Unique number that the IDC requires to register with Cisco Unified Communications Manager (CUCM) or Cisco Unified Communications Manager Express (CME) when the user logs in. Displays on an end device when the IDC places a call to a device that is configured to display caller ID.
- End User Name—CUCM or CME end user name that is configured for the user.
- End User Password—CUCM or CME end user password that is configured for the user.
- Confirm End User Password—Confirmation of the password in the End User Password field

Step 3 Take these actions:

a. In the IDC Dialer Phone Number field, enter a unique number that the IDC requires to register with CUCM or CME when the user logs in. Displays on an end device when the IDC places a call to a device that is configured to display caller ID. This parameter must also be configured in CUCM or CME.

b. In the End User Name field, enter the CUCM or CME end user name that is configured for the user.

c. In the End User Password field, enter the CUCM or CME end user password that is configured for the user

d. In the Confirm End User Password field, re-enter the password that you entered in the End User Password field.

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

Viewing, Adding, Editing, or Deleting Dial Preferences

You can view, add, edit, or delete 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.

The Dial Preferences pane displays the following information:

- Type—This field specifies the description of the location to be dialed, such as business, car, or home.
- Dial Number—This field specifies the telephone number of the corresponding location type.

Step 3 Take the desired action:

- To add a dial preference, follow these steps:
  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.

     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, choose a description for the dial preference.
  d. In the field next to the drop-down list, 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.

   You can use the up arrow and down arrow buttons to move a check to an adjacent check box.

b. Click **Delete**.

Step 4 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; then, attempt to place a call to the participants by using the dial preferences that were set in the user profile.

Step 5 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, radios, users, phones, virtual talk groups, and policies, to which you are associated in Cisco IPICS. See Table 4-6 through Table 4-11 for information about the resources within each of these tabs.

Table 4-6 Channels Tab Fields

Field	Description
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 an IDC or a properly-configured Cisco Unified IP Phone. To view the channels to which you are associated, choose **Channels** from the View drop-down list. 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.

Table 4-7 describes the fields in the Radios tab.

Table 4-7 Radios Tab Fields

Field	Description
Associated Radios	This tab specifies the radios to which you are associated. The following information displays about the radios to which you are associated: • Radio Name—This field specifies the name of the radio. • Location—This field specifies the location of the radio. The location determines whether the radio is reachable. • Multicast Address—This field specifies the multicast address of the radio. • Type—This field specifies the type of radio. • Status—This field specifies the status of the radio. Radios can have one of the following statuses: • Enabled—This status specifies that the radio is enabled • Disabled—This status specifies that the radio is disabled • Descriptor Corrupted/Missing—This status specifies that the radio/tone descriptor file is either corrupted or is missing from Cisco IPICS • Active—This status specifies that the radio is in an active state • Pending—This status specifies that the radio is not currently in an active state

Table 4-8 describes the fields in the Incidents tab.

Table 4-8 Incidents Tab Fields

Field	Description
Associated Incidents	This tab specifies information about your incidents: • ID—This field specifies the incident identifier. • Name—This field specifies the incident name. • Started—This field indicates when the incident started. • State—This field indicates whether the incident is active or inactive.

Table 4-9 describes the fields in the Phones tab.

Table 4-9 Phones Tab Fields

Field	Description
Associated Phones	This tab specifies the phones with which you are associated. When you are associated with phones, you can use your IDC to communicate with other users who are connected via a telephone. 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 IDC.

Table 4-10 describes the fields in the Virtual Talk Groups tab.

Table 4-10 Virtual Talk Groups Tab Fields

Field	Description
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. To view the VTGs to which you are associated, choose **Virtual Talk Groups** from the View drop-down list. 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 4-11 describes the fields in the Policies tab.

Table 4-11 Policies Tab Fields

Field	Description
Associated Policies	This tab specifies the policies to which you are associated that you can activate by calling the policy engine. 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 4-15.

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**—This tab displays the channels to which you are associated.
- **Radios**—This tab displays the radios to which you are associated.
- **Incidents**—This tab displays the incidents to which you are associated.
- **Phones**—This tab displays the phones to which you are associated.
- **Virtual Talk Groups**—This tab displays the VTGs to which you are associated.
- **Policies**—This tab displays the policies to which you are associated.

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 4-6 for a description of each of the association tabs.

Downloading the IDC

As a Cisco IPICS user, you can download the current version of the IDC to your PC. To do so, perform the following steps from the PC to which you want to download the IDC.

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

Procedure

Step 1 Access the Home drawer in the Cisco IPICS Administration Console and click **Download IDC**.

Cisco IPICS initiates the IDC download utility, which installs the IDC on your PC and creates a shortcut on your desktop.

Step 2 Follow the on-screen prompts to download and install the IDC.

CHAPTER 5

Performing Cisco IPICS Dispatcher Tasks

A Cisco IPICS dispatcher is responsible for setting up virtual talk groups (VTGs), activating VTGs to begin conferences, and adding or removing members or participants in inactive and active VTGs. A dispatcher also monitors active VTGs, notifies participants about active VTGs, and can mute and unmute IDC users, as necessary.

In addition, a dispatcher manages policies, each of which activates a VTG at a particular time and 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 6, "Using the Cisco IPICS Policy Engine."

Note Only a dispatcher or an operator who belongs to a specific ops view should create, edit, or delete policies that are associated with that ops view. A dispatcher or operator who modifies a policy that belongs to another ops view could cause inconsistencies when users view policies. For more information, see Chapter 6, "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 Virtual Talk Groups 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 Virtual Talk Groups 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 7, "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 an inactive VTG. You use this VTG to arrange participants who can communicate when you activate it. You can create as many inactive VTGs as necessary and activate any of them when needed.

After you activate the VTG, you can easily manage it by adding and removing users, channels, and other VTGs, notifying and dialing out to VTG participants, and by muting and unmuting IDC users.

This chapter describes information about how to manage VTGs and includes the following sections:

- Managing Inactive VTGs, page 5-4
- Managing Active VTGs, page 5-11
- Using the Search Utility, page 5-23
- Best Practices for Managing VTGs, page 5-25

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 5-2.

For related information, see the "Best Practices for Managing VTGs" section on page 5-25.

Note You can perform some VTG management tasks in the IDC. For more information, see *IPICS Dispatch Console User Guide* for this release.

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 VTGs 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 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 5-1 describes the fields in the Virtual Talk Groups window.

Table 5-1 Fields in the Virtual Talk Groups Window

Field	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; 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.	See the "Managing Inactive VTGs" section on page 5-4
Status field	This field indicates whether a VTG is active or inactive.	See the "Managing Active VTGs" section on page 5-11
Prompt field	This field indicates whether a spoken name is recorded for the VTG. 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 8-7
Add button	Click this button to add a new Cisco IPICS VTG.	See the "Adding a New VTG" section on page 5-6 and the "Modifying a VTG" section on page 5-9
Delete button	Click this button to delete a VTG.	See the "Deleting a VTG" section on page 5-11
Change Status drop-down list	Choose from this drop-down list to activate or deactivate a VTG.	See the "Changing the Status of a VTG" section on page 5-12
Display Controls		
Rows per page drop-down list	Specifies how many rows of VTGs are included in a VTGs list page.	See the "Navigating Item Lists" section on page 1-13
Page field	Displays VTGs on a specific page.	
|< (First page) button	Displays the first page of the VTG list.	
< (Previous page) button	Displays the previous page of the VTG list.	
> (Next page) button	Displays the next page of the VTG list.	
>| (Last page) button	Displays the last page of the VTG list.	

The individual VTG windows contain the following information tabs:

- **General** tab—This tab allows you to manage information about the VTG, such as VTG name, description, and VTG status.
- **IDC** tab—This tab allows you to set attributes for the IDC.
- **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, activate and deactivate the VTG, and execute various activities within the active VTG. Activities that you can execute include notifying users, dialing out to specific VTG participants, and enabling/disabling IDC attributes.

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.

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 inactive VTG and active VTGs, see the "Managing Inactive VTGs" section on page 5-4, and the "Managing Active VTGs" section on page 5-11.

Managing Inactive VTGs

An inactive VTG 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 at any time, which brings the VTG participants together into a live conference.

You can view information about any VTG by clicking the VTG name that displays in the Virtual Talk Groups window. Information about the VTG displays in a separate window.

When you modify an inactive VTG, no changes occur in system resources or in the communication between participants until you activate the VTG. When you make changes to an active VTG, the original attributes of the VTG remains unchanged.

The following sections describe information about managing inactive VTGs:

- Guidelines for Managing Inactive VTGs, page 5-5
- Adding a New VTG, page 5-6
- Modifying a VTG, page 5-9
- Deleting a VTG, page 5-11

You perform the VTG 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 5-2.

Guidelines for Managing Inactive VTGs

When you are managing VTGs, 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 channel into a VTG from the Users, Channels, or Radios lists and that user or channel already exists in a group within the VTG, the channel or user does not appear another time as an individual user or channel. If you drag a user or channel into a VTG individually; then, add a group that contains the user or channel, Cisco IPICS does display the user or 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; 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 its own VTG 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. These channels or VTGs display crossed out in the VTG list.
- Mixing secure and non-secure channels in the same VTG is not recommended because users on non-secure channels will be able to hear users on 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" section on page 5-6.
- 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 radio channel, drag the radio that you want to add from the Radios Resources area to the Participants area.

Note To avoid audio loops, Cisco IPICS supports an active radio channel in only one VTG at a given time.

- 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 inactive VTG 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 you deactivate a VTG 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 an IDC user from a VTG and that user monitors a channel that remains in the VTG, that user can continue to participate in the VTG through the channel that is associated to the user.
- 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 channel 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.
- To add a channel or user, or VTG for which you searched, drag the resource from the Resources area to the Participants area.

Note Mixing secure and non-secure channels in the same VTG is not recommended because users on non-secure channels are able to hear users on secure channels.

Adding a New VTG

When you add a VTG, you specify the name of the VTG and, typically, designate the members who are participants in the VTG. You can activate the VTG 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 you deactivate a VTG 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, 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 unique name for the VTG.

The name can contain alphanumeric characters, special characters, and spaces.

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 IDC attributes, click the **IDC** tab.

For information about how some attributes behave with associations, see the "Understanding Association Attribute Behaviors" section on page 2-14.

Step 7 From the RX Mute During PTT drop-down list, 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 IDC, check the **Enable VAD** check box.

When VAD is enabled, the IDC 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 IDC 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 false (attribute check box is unchecked).

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 IDC, IP phones, dialed-in, and mobile client users.

Note If a VTG contains only channels and no users, enabling Listen Only on the IDC has no effect. However if the VTG contains users, enabling Listen Only dims the PTT button on the IDC but the channels in the IDC are not set to Listen Only.

Step 11 To uniquely identify VTGs by a specific color that displays on the IDC, choose a color from the VTG color drop-down list.

Step 12 To assign an IDC region to the VTG, choose a region from the VTG IDC Region drop-down list.

Step 13 To add participants to the VTG, click the **Participants** tab.

Step 14 To view the available resources that are configured in Cisco IPICS and that can be added as participants in this VTG, choose one of the following options from the View drop-down list 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. 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 5-23.

- **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, the Search button displays as dimmed and the search functionality becomes unavailable.

- **Radios**—Choose this option to view the available radios that are configured in Cisco IPICS.
- **Users**—Choose this option to view the available users who 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, 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 15 Add any number and any combination of these resources to the VTG as described in the "Guidelines for Managing Inactive VTGs" section on page 5-5.

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 16 Click **Save** to add the VTG without exiting the current window.

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

Step 17 To activate the VTG from this window, click **Activate VTG**.

Modifying a VTG

When you modify a VTG, you can change its name and add or remove participants.

Because an inactive VTG is not an active event, you can make any changes to it without affecting any current communication between users.

To modify 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 name of the VTG that you want to modify.

Step 3 If you want to change the name of the VTG, 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 IDC attributes, click the **IDC** tab.

For information about how some attributes behave with associations, see the “Understanding Association Attribute Behaviors” section on page 2-14.

Step 5 From the RX Mute During PTT drop-down list, 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 IDC, check the **Enable VAD** check box.

When VAD is enabled, the IDC 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 IDC 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 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 false (attribute check box is unchecked).

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 IDC, IP phones, dialed-in, and mobile client users.

Note When you enable a VTG that contains only channels and no users, enabling Listen Only on the IDC has no effect. If the VTG contains users and you enable Listen Only, the PTT button dims on the IDC but the channels in the IDC are not set to Listen Only.

Step 9 To uniquely identify VTGs by a specific color that displays on the IDC, choose a color from the VTG color drop-down list.

Step 10 To assign an IDC region to the VTG, choose a region from the VTG IDC Region drop-down list.

Step 11 To view the available resources that are configured in Cisco IPICS and that can be added as participants in the VTG, click the **Participants** tab.

Step 12 From the View drop-down list 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. 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 5-23 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.
- **Radios**—Choose this option to view the available radios that are configured in Cisco IPICS.
- **Users**—Choose this option to view the available users who 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 13 To add participants to the VTG after choosing the view in Step 12, see the "Guidelines for Managing Inactive VTGs" section on page 5-5.

Tip To expand a collapsed Channels, Channel Groups, Users, User Groups, or VTGs list, click the arrow to the left of the list.

Step 14 Click **Save** to modify the VTG 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 15 To activate a VTG in this window, click **Activate VTG**.

Deleting a VTG

If a VTG is no longer needed, you can delete it from Cisco IPICS. Deleting an inactive VTG has no effect on the participants within it.

You cannot delete a VTG that is associated with an active VTG. To delete such a VTG, you must first deactivate the active VTG. See the "Reactivating a VTG" section on page 5-22 or the "Using the Search Utility" section on page 5-23 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 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 VTGs 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 5-11
- Changing the Status of a VTG, page 5-12
- Adding Participants to and Removing Participants from an Active VTG, page 5-13
- Muting or Unmuting an IDC User in an Active VTG, page 5-15
- Notifying and Dialing Out to Participants, and Setting IDC Attributes in an Active VTG, page 5-19
- Reactivating a VTG, page 5-22

Guidelines for Managing Active VTGs

When you are managing active VTGs, 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. A notification message displays on that particular VTG to reactivate the VTG if the channel gets enabled again. 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 channel can be a participant in one active VTG at a time. If you try to add a channel that is in an active VTG to a another active VTG, or try to activate another VTG that has the channel in it, Cisco IPICS shows the 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

A VTG can have either of the following statuses:

- Activated—Participants in a VTG can communicate with each other.
- Deactivated—Channels in a VTG are no longer connected and participants in a VTG can no longer communicate with each other.

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

Activating a VTG causes Cisco IPICS to commit the network resources that are required to enable VTG participants to communicate with each other.

Note Activating or deactivating a VTG requires that the Cisco IPICS server communicate with the RMS. When you deactivate a VTG 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 can also be activated by a policy. For more information, see the Chapter 6, "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 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 can also be activated by a policy. For more information, see the Chapter 6, "Using the Cisco IPICS Policy Engine."

To determine the current status of VTGs, access the VTG Management drawer, click **Virtual Talk Groups**, and look at the information in the Status column for the VTG.

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.
- Check the check box next to each VTG that you want to change; then choose the desired action (**Activate** or **Deactivate**) from the Change Status drop-down list.

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 and are not saved to it 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:

- An IDC 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, 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 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. 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 5-23.

- **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, the Search button displays as dimmed and the search functionality becomes unavailable.

- **Radios**—Choose this option to view the available radios that are configured in Cisco IPICS.

Note To avoid audio loops, a radio can be active in only one VTG at a given time.

- **Users**—Choose this option to view the available users who 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, 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, after choosing the view in Step 4, see the "Guidelines for Managing Inactive VTGs" section on page 5-5.

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**.

Step 8 To notify or dial out to VTG participants, or to modify their IDC attributes, perform the steps in the "Notifying and Dialing Out to Participants, and Setting IDC Attributes in an Active VTG" section on page 5-19.

Muting or Unmuting an IDC User in an Active VTG

Cisco IPICS allows you to mute an IDC 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 an IDC 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 IDC, IP phone, dialed-in, and mobile client 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 2-14 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, IDC 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 2-14 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; 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 IDC microphone has been muted. This attribute applies to the IDC, IP phones, and dialed-in users.

- Check the **Disable Audio** check box to disallow the user from listening or speaking in the active VTG; then, click **Save**.

  This setting disables the user 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 IDC speaker has been muted. This attribute applies to the IDC, IP phones, dialed-in, and mobile client 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 (IDC, IP phones, dialed-in, and mobile client 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; then, take any of the following actions:

- From the drop-down list 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 IDC microphone has been muted. This attribute applies to the IDC, IP phones, and dialed-in users.

- From the drop-down list 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 (IDC, IP phones, dialed-in, and mobile client 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 IDC 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 IDC, IP phones, dialed-in, and mobile client 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 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 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 5-17.

Enabling or Disabling the Latch Feature in the User Details Window

Cisco IPICS lets you enable or disable the latch feature for an IDC 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 IDC 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 2-14 for more information about modifying attributes that are part of an association.

To enable or disable the latch feature for an IDC 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, IDC 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 2-14 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 an IDC 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 2-14 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 IDC Attributes in an Active VTG" section on page 5-19.

Notifying and Dialing Out to Participants, and Setting IDC 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, displaying a designated message on supported Cisco Unified IP Phone models, and enabling and disabling IDC attributes for selected 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, a designated message on supported Cisco Unified IP Phone models, or a pre-recorded prompt that plays to all participants in the selected VTG. You also can configure the system to send an audio message that plays on a Cisco Unified IP Phone when the phone receives a text notification to join a VTG. The policy engine obtains the contact information of the participants from the notification preferences that were configured in their user profiles. See the Chapter 6, "Using the Cisco IPICS Policy Engine," for more information about the policy engine and configuring notification actions.

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; then, attempt to place a call to the participants by using the dial preferences that were set in the user profile.

You can create notifications for users who are not configured in Cisco IPICS. For more information, see Appendix B, "Using Cisco IPICS for External Notifications."

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, "Listening on Call" is displayed for each dialed-in user. If an error occurs, nothing is displayed on the Participants page. To view the status of the dial-out operation, open the Execution Status page in the Policy Management area of the Policy Engine.

Cisco IPICS displays the method by which the participants are connected, (for example, by PSTN or IDC) 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 IDC 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 the **VTG Management > Virtual Talk Groups** window.

Step 2 Click the link of the active VTG for which you want to initiate actions.

Note To activate a VTG in Cisco IPICS, see the "Changing the Status of a VTG" section on page 5-12.

Step 3 From the View drop-down list in the Participants pane, 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 that are participating in this VTG.
- **Radios**—Choose this option to view the radios that participate in this VTG.
- **Users**—Choose this option to view the users who participate in this VTG. The window displays an icon next to each participant to indicate how the user is connected (via an IDC, phone, or channel) to the VTG.
- **Virtual Talk Groups**—Choose this option to view the other VTGs that participate in the VTG.

Step 4 To choose the participants who 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, 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 or designated message, to join an active VTG and take either of the following actions:
  - To modify the subject of the message, in the Subject field, enter the text that you want to display in the subject line of the notification message.
  - To modify the body of the message, in the Body field, enter the message text that you want to display in the body of the notification message.

    Notification is sent via e-mail message, SMS text message, page, or designated message on supported Cisco Unified IP Phone models. Cisco IPICS obtains the e-mail addresses, telephone numbers, and delivery options from the communication preferences information that the users and/or Cisco IPICS operators entered in the user profiles.

Note A Cisco Unified IP Phone Text Notification action requires that you configure parameters in the Cisco Unified Communications Manager for IP Phone Notifications area in the SIP Configuration menu. For instructions, see the "Configuring SIP" section on page 8-24.

- **Dial Participants**—Choose this option to dial out to selected participants to invite them to join an active VTG. When you choose participants for 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 IDC, 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 (IDC, IP phones, dialed-in users), except for radios, is disabled.

Step 6 If you choose **Notify Participants** in Step 5 take either of the following actions to attach or record audio that plays on a Cisco Unified IP Phone when the IP phone receives the text message.

Note This field is required. You must attach prerecorded audio or record new audio when you choose the Notify Participants option. If you do not specify an audio message by performing one of the following required actions, Cisco IPICS displays an error and does not allow you to proceed.

- To attach an audio file that plays with the text notification, perform the following steps:
  a. Click **Attach Audio**.
  b. When the Select Prompt window displays, click the radio button that displays next to the name of the .wav file that you want to attach.
  c. Click **Select**.

Note Before you attach an audio file, you must upload the .wav file, or a .zip file that includes the .wav file, to the Cisco IPICS server. For information about uploading a .wav or .zip file, see the "Uploading Customized Script Prompts" section on page 8-12.

- To record audio that plays with the text notification, perform the following steps:
  a. Click Record Audio.

     The Prompt Record window displays.
  b. From the Language drop-down list box, 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.
  c. In the Phone Number field, enter a telephone number where the system should call you. Enter only numbers in this field. This field is required.
  d. Make sure that you enter only numbers in this field. The SIP provider must be able to route the call to the number that you enter.
  e. In the Name field, enter a name for the .wav file of this prompt, including the extension .wav. This field is required.
  f. (Optional) In the Destination Folder field, enter the name of the logical folder in which the prompt will be stored.
  g. Click **Call**. The dial engine calls the telephone number that you specified.
  h. Answer the telephone and follow the verbal prompts to log in to the telephony user interface (TUI) and record the prompt.
  i. In the Call Completed dialog box, click **OK**.

Step 7 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.

A 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 allows 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 the VTG.

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 2-46.

Step 5 If the channel is unavailable because it is in use by another VTG, take the following actions:

a. In the Configuration drawer, click **Channels**.

b. In the Channels list, click the channel name link or check the check box next to the channel name.

c. Click the **Associations** button.

d. Click the **Virtual Talk Groups** tab.

e. Locate the active VTG that is listed in the Virtual Talk Groups list; then, navigate to **VTG Management > Virtual Talk Groups**.

f. Choose the active VTG that was listed in the Virtual Talk Groups tab of the Channels window.

g. In the VTG Management drawer, click **Virtual Talk Groups** again.

h. Click the link of another active VTG in the Virtual Talk Groups list and see if the channel is a participant in that VTG.

i. 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, radio channel, user, or VTG by using the search utility. The search utility is located in the Virtual Talk Groups window of each individual VTG.

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, radio 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; then, click the **Search** link that appears above the Resources area.

A separate search window displays.

Step 4 From the View drop-down list, in the top left corner of this window, choose one of the following options:

- **Channel**—Choose this option to search for channels.
- **Radio**—Choose this option to search for radio channels.
- **User**—Choose this option to search for users.
- **Virtual Talk Group**—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 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.

  Proceed to Step 6.

- If you are searching for a radio channel, take any or all of the following actions:
  - Choose a location from the Location drop-down list.
  - Enter a text string for the radio for which you are searching.

    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—Location of the user
- Role drop-down list—Cisco IPICS role of the user
- Ops View drop-down list—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; then, choose Dispatcher and West Side from the Role and Location drop-down lists.

  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 PTT channels, radio channels, users, or VTGs that display per results page by choosing from the Rows per page drop-down list 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.

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 conference participants, especially those who are 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 IDC 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 IDC 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 and monitor the receive indicator so that you do not talk over other users
  - If extensive conversation is required, consider an alternate method of communication

CHAPTER 6

Using the Cisco IPICS Policy Engine

The Cisco IPICS 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 2-63.

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 6-2.

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 6-2
- Policy Activities Available for Cisco IPICS Roles, page 6-2
- Understanding the Policies Window, page 6-3
- Adding a Policy, page 6-4
- Managing Actions for a Policy, page 6-5
- Managing Triggers for a Policy, page 6-12
- Associating Users with a Policy, page 6-15
- Activating a Policy Manually, page 6-16
- Deleting a Policy, page 6-16
- Viewing Information about Executing or Executed Policies, page 6-17
- Viewing Information about Scheduled Policies, page 6-18
- Re-Activating a Policy or an Action, page 6-19
- Using the Policy Engine Telephony User Interface, page 6-20

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, and contacts designated recipients according to notification instructions that you specify.

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 one time 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.

Calls arrive at the Cisco IPICS dial engine as SIP calls from the configured SIP provider and establish a unicast media connection to the Cisco IPICS server. When a caller joins a channel or VTG, the Cisco IPICS server configures a T1 resource on the RMS to allow for a multicast connection from the server to a dynamically allocated loopback. The loopback facilitates a multicast connection between the Cisco IPICS server and the selected channel or VTG on the RMS. This connection is made one time per channel or VTG, regardless of how many dial in users select the channel or VTG. When the last dial in user that is connected to that channel or VTG drops, the resource is released in the RMS.

The dynamically allocated loopback uses a multicast address from the multicast address pool. The Cisco IPICS server sends the audio that it receives from the connected call to this address. In addition, the Cisco IPICS server listens for multicast media on the multicast address for the selected channel and sends that media to the connected call.

Policy Activities Available for Cisco IPICS Roles

Table 6-1 lists the Cisco IPICS roles that are required to perform various policy engine activities.

Table 6-1 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

Table 6-1 Roles Required for Policy Activities (continued)

Role	Activate Policy	Add Policy	Modify Policy	Delete Policy	View Policies	View Users	View VTGs and Channels
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
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 6-2 describes the items in the Policies window.

Table 6-2 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 6-4
Type field	Type of the policy	See the "Adding a Policy" section on page 6-4
Action Names field	Actions that are associated with the policy	See the "Managing Actions for a Policy" section on page 6-5
Trigger Names field	Triggers that are associated with the policy	See the "Managing Triggers for a Policy" section on page 6-12
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 7, "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 3-25
Add button	Provides the ability to add a new policy	See the "Adding a Policy" section on page 6-4
Delete button	Provides the ability to delete a policy	See the "Deleting a Policy" section on page 6-16

Table 6-2 Items in the Policies Window (continued)

Item	Description	Reference
Activate button	Provides the ability to activate a policy	See the "Activating a Policy Manually" section on page 6-16
Associations button	Provides the ability to associate users with a policy	See the "Associating Users with a Policy" section on page 6-15

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
  - Executes a notification action. For more information, see the "Understanding Notification Actions" section on page 6-6.
  - 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 3-13

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.

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, executes a notification action, 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 6-3, as needed.

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

Table 6-3 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 6-5.
Designate the users who can activate or deactivate this policy.	See the Associating Users with a Policy, page 6-15.

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 6-4.

Table 6-4 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	Contacts designated recipients according to notification instructions that you specify. For more detailed information, see the "Understanding Notification Actions" section on page 6-6.

Table 6-4 Policy Actions (continued)

Action	Associated Policy Type	Description
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 to join 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:

- Understanding Notification Actions, page 6-6
- Adding or Updating an Action for a Multi-Purpose Type Policy, page 6-8
- Adding or Updating an Action for an Invitation Type Policy, page 6-11
- Deleting an Action, page 6-12

Understanding Notification Actions

Notification actions cause Cisco IPICS to contact designated recipients and provide them with information that you specify. The policy engine notification actions that are described in this chapter can notify only recipients that are configured in Cisco IPICS. To create notifications for users who are not registered to Cisco IPICS, see Appendix B, "Using Cisco IPICS for External Notifications."

This section describes the Email, IP Phone Text, Dial, Talk Group, Dial Engine Script, and Alert notification actions. For information about configuring these action types, see the "Adding or Updating an Action for a Multi-Purpose Type Policy" section on page 6-8.

A policy can notify any Cisco IPICS user. For information about the number of recipients that are supported for various notification actions, see *Cisco IPICS Compatibility Matrix*.

Email Notification Action

An Email notification action sends a message to the e-mail, SMS, and pager addresses that are configured as notification preferences for each user that you designate as a recipient. The policy engine can send a message that contains up to 1,000 characters. It truncates longer messages to 1,000 characters.

IP Phone Text Notification Action

An IP Phone Text notification action displays a designated message on supported Cisco Unified IP Phone models. The telephone numbers of each phone must be configured as a dial preference for the associated user.

This type of notification action requires that you configure parameters in the Cisco Unified Communications Manager Configuration for IP Phone Notifications area in the SIP Configuration menu. For instructions, see the "Configuring SIP" section on page 8-24.

Dial Notification Action

The policy engine executes a Dial notification action as follows:

- If the IP Phone Notifications parameters are configured in the IP Phone Notification Configuration window, the system checks whether each designated user has an associated Cisco Unified IP Phone configured in Cisco Unified Communications Manager. If a user does have an associated phone, the system plays the designated message on the speaker of the phone.
- If IP Phone Notifications parameters are configured but a user does not have an associated Cisco Unified IP Phone, or if the phone of a user is busy, the system calls the user as specified in the dial preferences and plays the designated message.
- If IP Phone Notifications parameters are not configured, the system calls the user as specified in the dial preferences and plays the designated message.

For information about configuring IP Phone Notifications parameters, see the "Managing Cisco Unified Communications Manager for IP Phone Notifications" section on page 8-25.

When you create a Dial notification action, you can specify a pre-recorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

If you use this action to contact Cisco Unified IP Phones, make sure that at least one multicast address is available in the multicast pool. For more detailed information, see the "Managing the Multicast Pool" section on page 2-33.

Talk Group Notification Action

A Talk Group notification action plays the selected prompt to all participants in the selected VTG.

When you create a Talk Group notification action, you can specify a pre-recorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

Note

- When a Talk Group notification executes, the designated message is added to the multicast stream of the VTG. To inform users that a system message is being played, consider starting the message with a statement such as, "This is the Cisco IPICS administrator with an important recorded message."
- A VTG participant who is dialed in through the TUI and who has the floor does not hear the talk group notification message.

Dial Engine Script Notification

A Dial Engine Script notification action executes the designated dial engine script once for each designated recipient.

Alert Notification Action

An alert notification action sends an alert message to the IDC of each user who is associated with the policy and show has executed the policy from the IDC. The alert message appears in a pop-up window on the IDC.

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

A Multi-Purpose type policy can activate a VTG, send notification messages to recipients, 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 after the policy execution completes.

Note After you save a notification action, you cannot change the type of that action. Instead, you must delete the action and then add a new one.

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 recipients
  - 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.

If a policy includes more than one action, each action name must be unique.

Step 6 Follow the steps in Table 6-5 to enter additional information for the action type that you chose.

Table 6-5 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.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
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 1-12. 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.	Notification types are Email, IP Phone Text, Dial, Talk Group, Dial Engine Script, and Alert. For detailed information about these notification types, see the "Understanding Notification Actions" section on page 6-6.
2. Take one of these actions: • If you chose **Email** 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 **IP Phone Text** from the Type drop-down list, in the Message area, enter the text to display on the phone. • If you chose **Dial** from the Type drop-down list, from the Prompt drop-down list, choose the prompt to play. You can also choose to record a prompt by clicking **Record New Message Notification**. • If you chose **Talk Group** from the type Type drop-down list, from the Prompt drop-down list, choose the prompt to play. You can also choose to record a prompt by clicking **Record New Message Notification**. • If you chose **Dial Engine Script** from the Type drop-down list, from the Dial Engine Script drop-down list, choose the desired script. • If you chose **Alert** from the Type drop-down list, enter text for the alert message in the Message field.	When you click **Record New Message Notification** for a Dial or Talk Group action, you can record a prompt that you can then choose from the Prompt drop-down list. After clicking **Record a New Prompt**, follow these steps: **1.** 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. **2.** In the Phone Number field, enter a telephone number where the system should call you. Enter only numbers in this field. The SIP provider must be able to route the call to the number that you enter. **3.** In the Name field, enter a name for the .wav file of this prompt, including the extension .wav. **4.** (Optional) In the Destination Folder field, enter the name of the logical folder in which the prompt will be stored. **5.** Click **Call**. The dial engine calls the telephone number that you specified. **6.** Answer the telephone and follow the verbal prompts to log in to the TUI and record the prompt. **7.** In the Call Completed dialog box, click **OK**.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
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.
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 1-12. If you want to remove any recipient from the list, click the check box next to the recipient in the Recipients area, click **Delete;** 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 7, "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.
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 1-12. If you want to remove any participant from the list, check the check box next to the participant in the Participants area, click **Delete**; 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**.

Table 6-5 Creating or Updating an Action for a Multi-Purpose Type Policy (continued)

Step	Notes
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 those 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 1-12. If you want to remove any recipient from the list, check the check box next to the recipient in the Recipients area, click **Delete**; 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 after 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.

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 1-12.

If you want to remove any recipient from the list, check 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 one time 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 6-13
- Deleting a Trigger, page 6-14

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 6-8.

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.

If a policy includes more than one trigger, each trigger name must be unique.

Step 7 Designate the date and time at which 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 for a single occurrence. 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 6-6 to designate how often the policy executes.

Table 6-6 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 after 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 3-20.

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 1-12.

The users that you choose appear in the list of associated users. If you want to remove any user from the list, check 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.

In addition, you can export to an .xml file information about policies to which you are associated or that are created by users who belong to or are accessible to your ops view.

To view information about policies that have not executed, see the "Viewing Information about Scheduled Policies" section on page 6-18.

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 6-7.

Table 6-7 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 6-7 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.
Export to an .xml file information about policies that are executing or that have executed to which you are associated or that are created by users who belong to or are accessible to your ops view.	Click **Download Execution Status**, which appears at the bottom of the window, and enter the file name and storage location in the pop-up window.
Export to an .xml file information about all policies that are executing or that have executed.	Click **Download All Execution Status**, which appears at the bottom of the window, and enter the file name and storage location in the pop-up window.
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.
Reactivate 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 6-19.

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 6-17.

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 reactivate feature to perform any of these activities:

- Reactivate 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 6-16. You can reactivate a single policy, or you can re-execute several policies at one time. You cannot reactivate an invitation type policy.
- Reactivate an action—Activates one or more specific actions in a designated policy.
- Reactivate an action for a specific participant—Activates a dial out or a notification action for one or more specific participants in that action.

To reactivate 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 6-8.

Table 6-8 Re-activation Activities

Activity	Procedure
Reactivate a policy	1. Check the check box next to each policy or policies that you want to reactivate. 2. Click **Reactivate** at the bottom of the list of policies.
Reactivate 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 reactivate. 3. Click **Reactivate** at the bottom of the list of policies.
Reactivate 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 reactivate. 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 group 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 D, "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 group
- 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 7, "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 group, 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 6-21
- Menu Guidelines, page 6-22

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 group, 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 group. (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 groups 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 group, press 1. Then, you can press 1 to select an assigned group to join by spelling out the group name, or press 2 to listen to the list of assigned groups and then selecting from that list. (If you know the name of the group that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available groups.) 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 group. 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 group, 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 7

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 7-1
- Understanding Ops Views Caveats, page 7-7
- Performing Ops Views Tasks, page 7-11

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 do not affect the way in which channels and VTGs display on the IDC 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 7-2 for more information.

For more information about Cisco IPICS license information, see the "Understanding the License Management Window" section on page 2-64.

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 2-63. For detailed information about how to obtain licenses in this release of Cisco IPICS, see *Cisco IPICS Server Installation and Upgrade Guide*.

This section describes the Cisco IPICS ops view management functions and includes the following topics:

- Understanding the Ops Views Window, page 7-2
- Creating New Ops Views, page 7-3
- Assigning Ops Views Resources, page 7-4
- The Benefits of Using Ops Views, page 7-4
- Understanding Ops Views Attributes, page 7-4
- Understanding Ops Views User Roles, page 7-6

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 7-1 describes the items in the Ops Views window.

Table 7-1 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 7-11.
LDAP Enabled field	Indicates whether LDAP is enabled for this ops view. When LDAP is enabled, LDAP is used for authenticating Cisco IPICS users.	
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.	
IDC Users Limit field	Maximum number of IDC users license ports that are allocated to this ops view.	

Table 7-1 Items in the Ops Views Window (continued)

Item	Description	Reference
Cisco Unified IP Phones Limit field	Maximum number of Cisco Unified IP Phone license ports that are allocated to this ops view.	See the "Performing Ops Views Tasks" section on page 7-11.
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 7-11.
Delete button	Click this button to delete an ops view.	See the "Deleting Ops Views" section on page 7-21.
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 7-15.

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 Administration > 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 2-64 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. For more information, see Table 7-3 on page 7-6.

When a resource contains or is associated to another resource that belongs to the ops view of a user, the user has the ability to remove the associated 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 7-11.

Assigning Ops Views Resources

Table 7-2 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 7-2 Cisco IPICS Ops View Resources

Resource	Where to Find More Information
Users	Managing Ops Views for a User, page 3-24
User groups	Managing Ops Views for a User Group, page 3-32
Channels	Associating Users to PTT Channels, page 2-17
Channel groups	Associating Ops Views to Channel Groups, page 2-26
VTGs	Managing VTGs, page 5-2 and Understanding VTG and Sub-VTG Caveats, page 7-8
Policies	Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine," and Chapter 6, "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 7-6 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 6, "Using the Cisco IPICS Policy Engine," and Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

- When a user logs in to an IDC or a Cisco Unified IP Phone, that user uses an IDC or Cisco Unified IP Phone 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 7-16.

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 that 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 the previously-configured ops view from the list of accessible ops views. The resource is accessible to the previous ops view, as well as the newly-configured ops view.

Understanding Ops Views User Roles

Some Cisco IPICS user roles expand to assume additional responsibilities. Table 7-3 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.

An operator or a dispatcher who belongs to the SYSTEM ops view can view all resources in all ops views.

Table 7-3 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 7-3 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 7-8.

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 6, "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 7-4 shows an example of VTG ops view accessibility.

Table 7-4 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 7-5 shows an example of sub-VTG ops view accessibility.

Table 7-5 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 7-6 shows an example of active/inactive state dependency on sub-VTG ops view accessibility.

Table 7-6 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 7-7 shows an example of how resources in sub-VTGs can affect ops view accessibility.

Table 7-7 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
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 VTGs that are accessible to the ops view.
- The Virtual Talk Groups window 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 window, but the Channels, Users, and VTGs windows 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 7-8.

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. For more information, see the "Managing Ops Views License Usage and Limits" section on page 7-16.

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 7-11
- Viewing Resources That Belong To and are Accessible To Ops Views, page 7-15
- Viewing Ops Views License Details, page 7-16
- Deleting Ops Views, page 7-21

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.

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.

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 In the **License Allocation** pane, enter applicable license information in the fields, as described in the Table 7-8.

Note The Current Usage values in the License Allocation pane indicate the number of license ports for the feature that are currently in use.

Table 7-8 License Allocation Fields in the Ops View Window

Feature	Limit
LMR Ports	Number of LMR license ports that you allocate for this ops view. Enter the number of LMR ports in the Limit field.
Multicast Ports	Number of multicast license ports that you allocate for this ops view. Enter the number of multicast ports in the Limit field.
IDC Silver Users	Number of IDC silver users ports that you allocate for this ops view. Enter the number of IDC silver users ports in the Limit field.
IDC Platinum Users	Number of IDC platinum users ports that you allocate for this ops view. Enter the number of IDC platinum users ports in the Limit field.
IDC Mobile Users	Number of IDC mobile users ports that you allocate for this ops view. Enter the number of IDC mobile users ports in the Limit field.
Cisco Unified IP Phones	Number of Cisco Unified IP Phone ports that you allocate for this ops view. Enter the number of Cisco Unified 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 7-16.

Step 6 In the **Dial Information and Dial Port Resource Allocation** pane, enter applicable dial information in the fields, as described in the Table 7-9.

For information about how to allocate dial ports, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 7-18. 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 6, "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 Communications Manager) 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 8-32.

Table 7-9 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. **Note** When the policy engine is installed and you want to assign a DN to allow for dial-in access, you must assign the DN to an ops view.
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.
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 7-9 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. Blast notifications are sessions that are typically short in duration and play out short messages; 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. If you do not allocate all of the licensed dial ports specifically for dial-in/dial-out or notifications, Cisco IPICS allocates the remainder of the licensed dial ports to this field. 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 7-18.

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 7-18.

For more information about the Cisco dial engine, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

Step 7 In the LDAP Authentication pane, check the Use LDAP Authentication check box if you want to enable LDAP authentication for users who are associated with this ops view.

For more information about LDAP authentication, see the "Configuring LDAP" section on page 2-98.

Step 8 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 7-15.

For information about assigning resources to ops views, see the "Assigning Ops Views Resources" section on page 7-4.

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 7-4 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; 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; 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.
  - 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.
  - 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 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 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 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 7-16
- Configuring Licenses for Ops Views Usage, page 7-18

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, IDC 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 7-11.

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, IDC 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 IDC User Usage—An IDC silver, platinum, or mobile user uses a license each time that the user logs in to an IDC. This license is used against the ops view to which the user belongs.

Note If all Cisco IPICS licenses have been used, IDC user access to the system will be interrupted. Make sure that you are aware of the current status of IDC 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 7-18 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 6, "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, IDC 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 7-18
- Determining How Many Dial Ports to Allocate, page 7-19

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 that they 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 7-11.

For license allocation and dial information field descriptions, see the "Adding Ops Views" section on page 7-11.

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 6, "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 3-24, and the "Managing Ops Views for a User Group" section on page 3-32.

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 To associate a channel or channel group to an ops view, you must be assigned the system administrator role 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 2-17 and the "Associating a Channel or Channel Group to an Ops View" section on page 7-20.

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**.

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 Communications Manager 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 6, "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 7-18.
- 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 2-33.

This chapter includes these topics:

- Obtaining Information about Dial Engine Services, page 8-2
- Managing Tracing for the Policy Engine, page 8-3
- Managing Prompts, page 8-7

- Managing Dial Engine Scripts, page 8-21
- Configuring SIP, page 8-24
- Managing Cisco Unified Communications Manager for IP Phone Notifications, page 8-25
- Configuring Text to Speech, page 8-28
- Configuring Dial Engine Parameters, page 8-28
- Managing Direct Dial Numbers, page 8-29
- Configuring the SIP Provider, page 8-32

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.

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:
  - IN_SERVICE—The SIP subsystem and SIP provider are configured in Cisco IPICS. When the service is in this state, the dial engine can receive calls. However, if the configuration is not correct, for example, if the SIP Provider user name or password is not correct, the dial engine cannot place calls to a SIP provider that requires authentication.
  - OUT_OF_SERVICE—The SIP subsystem is in the process of shutting down.
  - PARTIAL_SERVICE—The SIP subsystem is in the process of shutting down.
  - SHUTDOWN—The SIP subsystem and SIP provider are not configured in Cisco IPICS.
- 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. *n* is a number that the system assigns to the file. It increments by 1 when a new file is created.
- 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.
- XDebug *n* (extended debug)—Generates more verbose detailed information. *n* is a number 1 through 5 that indicates the level of xDebug logging that is enabled.

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 8-4
- Configuring Trace Levels for Dial Engine Trace Files, page 8-4
- Performing Advanced Tracing Activities, page 8-6
- Obtaining Trace Files, page 8-7
- Interpreting Trace Files, page 8-7

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 **Reset**.

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 can change tracing levels, 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 Communications Manager 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 **Reset**.

Performing Advanced Tracing Activities

You can perform the following advanced tracing activities for dial engine trace files.

Note Cisco recommends that you do not perform advanced tracing activities unless you are instructed to do so 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 8-4.
- 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 8-7.

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 8-8—Describes how to add, rename, and delete logical language folders under which prompts are stored
- Managing Standard Script Prompts, page 8-10—Describes how to upload standard script prompts to the repository
- Managing Customized Script Prompts, page 8-11—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 8-14—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 8-8
- Adding a Language, page 8-9
- Renaming a Language, page 8-9
- Deleting a Language, page 8-9

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.

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.

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 8-10—Displays a list of prompts and related information
- Uploading Standard Script Prompts, page 8-11—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. Cisco IPICS supports unencrypted .zip files that use the DEFLATE compression algorithm. For example, .zip files created with WinZip, if they use legacy compression, and .zip files created with Info-Zip are compatible with Cisco IPICS.

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.

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 8-12—Displays a list of prompts and related information
- Uploading Customized Script Prompts, page 8-12—Copies prompt .wav files to the repository

- Downloading a Customized Script Prompt, page 8-13—Provides the capability for you to listen to a prompt
- Renaming a Customized Script Prompt, page 8-14—Changes the name of a customized script prompt
- Deleting a Customized Script Prompt, page 8-14—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 of only 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 push-to-talk (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. Cisco IPICS supports unencrypted .zip files that use the DEFLATE compression algorithm. For example, .zip files created with WinZip, if they use legacy compression, and .zip files created with Info-Zip are compatible with Cisco IPICS.

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.

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.

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 being 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 8-15—Displays a list of prompts and related information
- Uploading Spoken Names Prompts, page 8-16—Copies prompt .wav files to the repository
- Downloading a Spoken Names Prompt, page 8-17—Provides you with the capability to listen to a prompt
- Recording a Spoken Name Prompt, page 8-18—Lets you record a prompt
- Changing Information about a Spoken Names Prompt, page 8-20—Lets you change the name, language, resource type, and associated resource of a prompt
- Deleting a Spoken Names Prompt, page 8-20—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. Cisco IPICS supports unencrypted .zip files that use the DEFLATE compression algorithm. For example, .zip files created with WinZip, if they use legacy compression, and .zip files created with Info-Zip are compatible with Cisco IPICS.

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 1-12.

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.

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 1-12.

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 by Using the Dial Engine, page 8-18
- Recording a Spoken Names Prompt by Using the Windows Sound Recorder, page 8-19

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 6-20.

Recording a Spoken Names Prompt by Using the Dial Engine

When you record a spoken names prompt by 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; 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 populates the Resource Type, Associated Resource, and Language fields with the information that is 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 1-12.

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 by 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 8-16.

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 8-15.

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.

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 additional scripts.

- BulkNotifyDialer—Used to notify recipients when Cisco IPICS receives an external notification request
- 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 8-21
- Adding a Dial Engine Script, page 8-22
- Viewing or Changing Information about a Custom Dial Engine Script, page 8-22
- Deleting a Custom Dial Engine Script, page 8-23

Viewing a List of Dial Engine Scripts

The Dial Engine Script Management window displays a list of dial engine scripts. For each script, this window shows the following information:

- Name—Name of the script
- Script—File name 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.

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.

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 8-21.

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 used 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 8-21.

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 following parameters:

- Parameters required to work with the SIP provider.
- Parameters required to use the IP Phone Text Notification action in a policy
- Parameters required to use the Dial notification action in a policy to send a message to a Cisco Unified IP Phone

For related information, see the "Configuring the SIP Provider" section on page 8-32.

To configure SIP for the policy engine, perform the following steps.

Note After you configure SIP, verify that the Dial Engine and SIP subsystem are IN_SERVICE. For more information, see the "Obtaining Information about Dial Engine Services" section on page 8-2.

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-IPICS.
- 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.
- In the Port field, enter the port number that the SIP provider uses for SIP.
- 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.

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

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

Step 5 Your changes take effect only after you restart the dial engine. To restart the dial engine, follow these steps:

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
```

Managing Cisco Unified Communications Manager for IP Phone Notifications

If you configure policies to use the IP Phone Text Notification action or to use the Dial Notification action to send a message to a Cisco Unified IP Phone, you must configure at least one Cisco Unified Communications Manager under IP Phone Notification Configuration for these policies to execute.

When you configure a Cisco Unified Communications Manager for IP phone notification, you provide information about a Cisco Unified Communications Manager in which end users contain information about IP phones that Cisco IPICS should contact. You can provide information for up to three Cisco Unified Communications Managers. Then, when a policy that includes a IP Phone Text Notification action or to use the Dial Notification executes, Cisco IPICS contacts each of the configured Cisco Unified Communications Managers and provides all configured IP phone numbers to each one. When a provided phone number matches a phone number on a Cisco Unified Communications Manager, it returns the MAC address of the corresponding IP phone to Cisco IPICS, and Cisco IPICS contacts the phone at that MAC address.

Managing IP phone notification involves these activities:

- Viewing a List of Cisco Unified Communications Managers for IP Phone Notifications, page 8-25
- Adding a Cisco Unified Communications Manager for IP Phone Notification, page 8-26
- Viewing or Changing Information about a Cisco Unified Communications Manager Configured for IP Phone Notification, page 8-26
- Deleting a Cisco Unified Communications Manager for IP Phone Notification, page 8-27

Viewing a List of Cisco Unified Communications Managers for IP Phone Notifications

The IP Phone Notification Configuration window displays a list of Cisco Unified Communications Managers configured for IP phone notifications. For each notification, this window shows the following information:

- Name—A system-provided identifier for the notification. The name includes the designation CUCM (for Cisco Unified Communications Manager) and the IP address of the Cisco Unified Communications Manager server that the IP phone notification is configured for.
- Version—Cisco Unified Communications Manager version that is running on the configured server.
- Host Name or IP Address—Host name or IP address of the Cisco Unified Communications Manager.

To display the IP Phone Notification Configuration window, choose **Dial Engine > IP Phone Notification Configuration** from the **Policy Engine** tab.

Adding a Cisco Unified Communications Manager for IP Phone Notification

When you add a Cisco Unified Communications Manager for IP phone notification, you make it available for use by policies that include the IP Phone Text Notification action or the Dial notification action to send a message to a Cisco Unified IP Phone.

To add a Cisco Unified Communications Manager for IP phone notification, perform the following procedure.

Note For information about Cisco Unified Communications Manager Application Users and end users, see your Cisco Unified Communications Manager documentation.

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > IP Phone Notification Configuration**.

The IP Phone Notification Configuration window displays.

Step 2 Click **Add** at the bottom of the list of notifications.

Step 3 From the Version drop-down list, choose the version of Cisco Unified Communications Manager that is running on the server that Cisco IPICS should contact for this notification.

Step 4 In the Host Name or IP Address field, enter the host name or the IP address of the Cisco Unified Communications Manager server.

Step 5 In the Administrator User Name field, enter the name of the Application User in Cisco Unified Communications Manager who has administrator privileges.

Step 6 In the Administrator Password field, enter the password of the Application User in Cisco Unified Communications Manager who has administrator privileges

Step 7 In the End User Name field, enter the name of the end user in Cisco Unified Communications Manager to which IP Phones are associated.

Step 8 In the End User Password field, enter the password of the end user in Cisco Unified Communications Manager to which IP Phones are associated.

Step 9 To add the notification, click **Save**.

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

Viewing or Changing Information about a Cisco Unified Communications Manager Configured for IP Phone Notification

You can view or modify information about any Cisco Unified Communications Manager configured for IP phone notification. To do so, perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > IP Phone Notification Configuration**.

The IP Phone Notification Configuration window displays.

Step 2 Click the link in the Name column of the Cisco Unified Communications Manager for IP phone notification.

Step 3 View or update the following information as needed:

- Version—Version of Cisco Unified Communications Manager that is running on the server that Cisco IPICS should contact for this notification
- Host Name or IP Address field—Host name or the IP address of the Cisco Unified Communications Manager server
- Administrator User Name—Name of the Application User in Cisco Unified Communications Manager who has administrator privileges.
- Administrator Password—Password of the Application User in Cisco Unified Communications Manager who has administrator privileges
- End User Name—Name of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated.
- End User Password—Password of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated.

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

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

Deleting a Cisco Unified Communications Manager for IP Phone Notification

To delete a Cisco Unified Communications Manager configured for IP phone notification perform the following procedure:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > IP Phone Notification Configuration**.

The IP Phone Notification Configuration window displays.

Step 2 Check the check box next to the Cisco Unified Communications Manager name 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 Cisco Unified Communications Manager configured for IP phone notification, click **Cancel**.

Configuring Text to Speech

Text to Speech (TTS) allows Cisco IPICS to speak the following items when it plays a message through the dial engine:

- Channel names
- Policy names
- VTG names
- Bulk notification messages

Before you can configure TTS, you must setup up appropriate hardware and third-party software. For detailed information, see *Solution Reference Network Design (SRND)* (latest version).

To configure TTS, perform the following steps:

Procedure

Step 1 In the **Policy Engine** tab, choose **Dial Engine > TTS Management**.

The TTS Management window displays.

Step 2 In the Text-To-Speech Provider Configuration pane, take these actions:

- In the Provider Name field, enter the name of your TTS software vendor.
- In the Number of Licenses field, enter the number of TTS licenses that you have.

Step 3 In the Text-To-Speech Server Configuration pane, take these actions:

- In the Server Name field, enter the IP address of the TTS server.
- In the Port field, enter the port number on the TTS server that your TTS software uses.
- From the Language drop-down list, choose the language that you want TTS to use for its pronunciation rules.
- From the Gender drop-down list, choose the type of voice that you want TTS to use.

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

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

Step 5 In the **Policy Engine** tab, choose **Dial Engine > Dial Engine Parameters**.

The Dial Engine Parameters window displays.

Step 6 Check the TTS Enabled check box.

Step 7 Click **Save** to save your changes.

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

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 procedure:

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.

The 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.

Note You should change the Default Session Timeout value only if you are instructed to do so by the Cisco TAC.

The Dial Engine Parameters window displays the codec that the policy engine uses. This codec is G.711 u-law and cannot be changed.

Step 7 If you will use TTS, check the TTS Enabled check box.

Step 8 Click **Save** to save your changes.

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

Managing Direct Dial Numbers

Direct dial numbers allow you to use the IDC push-to-talk (PTT) features to speak directly with a phone user. A direct dial call is a SIP call that originates from an IDC and flows through the RMS to the SIP provider. The telephone can be any one that can be reached by the SIP provider.

Note Before you can manage direct dial numbers, you must first configure an RMS router for use with the Cisco IPICS server. For more information, see Appendix A, "Configuring the Cisco IPICS RMS Component."

After a direct dial number (to a phone) has been configured, you must associate it with a user before the user can use the direct dial number from an IDC to access a phone. To associate direct dial numbers with users, see the "Associating Phones with a User" section on page 3-19. For information about using direct dial numbers on an IDC, see *Cisco IPICS Dispatch Console User Guide*.

Managing direct dial numbers involves these activities:

- Viewing a List of Direct Dial Numbers, page 8-30
- Designating a Dial Prefix for Direct Dial Numbers, page 8-30
- Adding a Direct Dial Number, page 8-31
- Viewing or Changing Information about a Direct Dial Number, page 8-31
- Deleting a Direct Dial Number, page 8-32

Viewing a List of Direct Dial Numbers

The Direct Dial Management window provides you with the ability to designate global dial settings. Global dial settings include a dial prefix 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 an IDC
- 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 to avoid dial plan conflicts. This digit string should match the value that you 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 8-32.)

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 Dial 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 an IDC as a label for this number.

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.

Step 5 Click **Save** to add the direct dial number.

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

What to Do Next

Associate the direct dial number with a user. For more informations, see the "Associating Phones with a User" section on page 3-19.

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 an IDC
- 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 IDC 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 or dial-out features. A SIP provider handles calls to and from the policy engine.

You must use Cisco Unified Communications Manager or a Cisco Unified Communications Manager Express 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 Communications Manager or a supported router with Cisco IOS software is installed and running in your network.

- Configuring Cisco Unified Communications Manager as the SIP Provider, page 8-32
- Configuring a Cisco Unified Communications Manager Express as the SIP Provider, page 8-35

Configuring Cisco Unified Communications Manager as the SIP Provider

Assuming that Cisco Unified Communications Manager is configured and running in your network, this section describes additional configuration that is required for Cisco Unified Communications Manager to function as the SIP provider for the policy engine.

Before you configure Cisco Unified Communications Manager for the policy engine, you must provide SIP configuration information as described in the "Configuring SIP" section on page 8-24.

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 Communications Manager Configuration

Information	Your Value
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	
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 Communications Manager for the policy engine, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Manager 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 Communications Manager.

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 in to Cisco Unified Communications Manager.
- 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 Communications Manager 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 Communications Manager.

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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager Administration, take the following actions to configure an 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 Communications Manager 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 Communications Manager 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 Unified Communications Manager Express as the SIP Provider

Assuming that Cisco Unified Communications Manager Express 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 an IDC.

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 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 8-24)

```
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 Cisco 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 To exit, enter this command:

```
Router(config)# end
```

CHAPTER 9

Managing Radios and Radio Descriptors

The Cisco IPICS administrator is responsible for configuring the radios and radio descriptors that are used with Cisco IPICS. This chapter provides detailed information about managing these items. In includes these topics:

- "Managing Radios" section on page 9-1
- "Managing Radio Descriptors" section on page 9-21

Managing Radios

Cisco IPICS provides support for tone-controlled radios by enabling the definition of radio channels in the Cisco IPICS server configuration. The IDC sends RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis. Cisco IPICS supports up to 50 configured channels, with up to 36 channels active at any one time.

At the LMR gateway, these packets get converted into audible tones via the configured ear and mouth (E&M) interface to the physical radio to provide tone control for radios.

Cisco IPICS also provides support for serial-controlled radios through an integrated radio control service that translates control commands from Cisco IPICS to proprietary serial protocols. Cisco IPICS access serial controlled radios via asynchronous serial ports on the LMR gateway.

Using radio control to manage radios involves the following general steps:

1. Configure hardware as described in *Solution Reference Network Design (SRND)* (latest version).
2. Create a location that the radio uses for multicast. (See the "Managing Locations" section on page 2-27.)
3. Create and provision a radio descriptor. (See the "Adding Descriptors" section on page 9-36.)
4. Add the radio and assign the desired descriptor to it. (See the "Adding a Radio" section on page 9-8.)

This section contains the following radio management topics:

- Tone Control Radio Overview, page 9-2
- Serial Control Radio Overview, page 9-3
- ISSI Gateway Overview, page 9-3
- Understanding How Buttons Display on the IDC, page 9-4
- Radio Frequency Channels, page 9-4
- Configuring Channel Selectors and Control Sequences, page 9-4

- Understanding the Radios Window, page 9-7
- Adding a Radio, page 9-8
- Viewing and Editing Radio Details, page 9-14
- Associating a User to a Radio From the Radios Window, page 9-15
- Enabling or Disabling a Radio, page 9-17
- Deleting a Radio, page 9-18
- Accessing and Using the Serial Radio Control Interface, page 9-18

You perform the radio management tasks in the **Configuration > Radios** window in the Administration Console. For more information about these windows, including how to access them, see the "Understanding the Radios Window" section on page 9-7.

Tone Control Radio Overview

Each radio channel that you configure in the Cisco IPICS Administration Console represents a physical radio that you can configure with one or more tone sequences. Tone sequences control various tones and functionality. Each tone sequence includes the frequency or frequencies, volume (power), duration, and other parameters that are necessary to generate a specific tone and invoke a specific action.

Tone control, also referred to as *Tone Remote Control* (TRC), refers to the use of inband tone sequences to control a radio that is connected to an LMR gateway (typically a base station). In Cisco IPICS, you can use tone control to modify or tune to a different radio frequency (RF) channel, change the transmit power level, enable or disable radio built-in encryption, and control other operations. TRC uses well-defined audio sounds (also referred to as *tones*) to change the behavior of a device. A tone-keyed radio system requires that a specific tone be present on the incoming analog (e-lead) port. If this tone is not present, the radio does not transmit audio.

The Radio Details page shows available controls and channels. The IDC generates the necessary radio control tone sequences when users press the associated button. For more information about channel selectors, see the "Configuring Channel Selectors and Control Sequences" section on page 9-4.

Note

- For information about various Requests for Comment (RFCs), access the RFC repository that is maintained by the Internet Engineering Task Force (IETF).
- For more detailed information about how to use the tone-controlled radio functionality on the IDC, see *IPICS Dispatch Console User Guide* for this release.

Channel selector buttons, signals, and commands are defined in descriptor files. The following list describes these descriptor files:

- Radio Descriptor Files—Channel selector buttons that provide the functionality for specific radio types are defined in the radio descriptor files. The radio descriptor file defines the tones or events that must be sent to the radio to enable or disable specific capabilities. For more information, see the "Tone Radio Descriptors" section on page 9-22.
- Tone Descriptor Files—Contain signals and commands. You can associate signals, that are defined in a tone descriptor file, to channels. Commands in a tone descriptor can be referenced by any radio descriptor file. See the "Tone Descriptors" section on page 9-21 for more information.

Serial Control Radio Overview

Serial controlled radios can be configured to have channel selectors and control functions. Channel selectors represent controls that allow an IDC or Administration Console user to select a radio channel or talkgroup and to set up a private or group call. Control functions are controls that allow an IDC or Administration Console user to invoke functions or modes of operation.

For serial control, Cisco IPICS defines generic control commands that are configured in a radio descriptor. A radio control service that is integrated with Cisco IPICS translates these commands to proprietary commands.

The Serial Radio Control Interface (SRCI) and the IDC provide access to the channel selectors and control functions that are defined in the radio descriptor, if a radio is in a location other than the location that you logged in to. The SRCI and IDC also provide feedback from the controlled radio when a channel selector is changed or a control function is invoked. For radios that support these features, the SRCI and IDC provide the talker ID for incoming calls and emergency detection.

ISSI Gateway Overview

A Project 25 (P25) Inter-RF Subsystem Interface Gateway (ISSIG) allows multiple RF subsystems (RFSSs) to be connected together into wide area networks that extends area coverage for P25 compliant digital radios. With the ISSIG, a radio from IPICS can roam to another RFSS. The ISSIG is composed of two parts:

- The P25G (or IPICSG) serves as a proxy for all non-P25 clients within IPICS and is responsible for transcoding between multicast RTP streams (using G.711 codec) and SIP based P25 CAI frames (using IMBE codec). It is also responsible for encryption and decryption when necessary.
- The (or RNC) serves as a local RFSS for IPICS and is responsible for interfacing with other RFSSs via ISSI. It can be a home RFSS to subscribers and groups or serving RFSS for subscribers and groups homed elsewhere. It performs all SIP based call processing between IPICS and remote RFSSs.

Before an ISSIG is provisioned within the IPICS Server, a descriptor must be created that describes groups that a given ISSIG may need to affiliate and supplementary services that are available via the ISSIG. An example ISSIG descriptor is available from the **Configuration > Descriptors** page on the IPICS Administration console. For more information about adding an ISSIG descriptor, see the "Adding Descriptors" section on page 9-36.

An ISSIG is provisioned much like a serial radio within IPICS and is accessible from the **Configuration > Radios** page on the IPICS Administration console. The main difference is that the ISSIG Connection block has information unique to ISSIGs. For more information about provisioning an ISSIG, see the "Adding a Radio" section on page 9-8.

Channels representing P25 groups are provisioned similar to other channels from the **Configuration > Channels** page on the IPICS Administration console. The difference in this case is that the Media Connection Assignment is set to ISSIG. For more information about provisioning channels representing P25 groups, see the "Viewing and Editing Channel Details" section on page 2-5.

An existing IPICS user can be assigned a P25 subscriber unit ID from the Communications tab of the User Details page accessible via User Management on the IPICS Administration Console. For more information about assigning P25 Subscriber Unit IDs to IPICS users, see the "Managing Communications Preferences for a User" section on page 3-13.

Understanding How Buttons Display on the IDC

When you use tone control, the buttons that display on the IDC get populated from information that the IDC receives from the Cisco IPICS server. The Cisco IPICS server performs a one-to-one mapping of the available IDC buttons and sends it to the IDC.

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

Radio Frequency Channels

In Cisco IPICS, a channel can refer to the RF channel (the frequency) to which the radio is tuned and on which content is streaming. Be aware of the following RF caveats when you use the IDC:

- A radio frequency does not define a channel and the audio content may differ depending on the location of the frequency. For example, a channel that is tuned to one frequency in one location may receive different content from the same type of radio that is tuned to the same radio frequency in another location.
- A channel may appear on more than one frequency, so the same content may be audible on several different frequencies.
- Any radio frequency in a specific location may carry several different content streams simultaneously.

You can associate radios and IDC users to enable user access to specified radios. You also can specify channel selector and control permissions to users by choosing the level of permission that pertains to each individual channel selector or radio control button. These permissions determine which channel selector buttons and radio controls the users can access. For example, if you do not configure any channel selector buttons for a user, the user can listen to the channel but cannot change the channels or control the radio.

Examples of radio control functions include MON (monitor), POW (power level) and Enc (encryption).

See the "Configuring Channel Selectors and Control Sequences" section on page 9-4 for more information about channel selectors and tone control sequences for radios.

Configuring Channel Selectors and Control Sequences

This section describes how to configure channel selectors and tone control sequences.It includes the following topics:

- Channel Selector Configuration, page 9-4
- Tone Sequence Configuration (Tone Control Radios), page 9-5
- Caveats for Configuring Default Tone Sequences (Tone Control Radios), page 9-6

Channel Selector Configuration

You select channel descriptors and controls that are available to radio users in the Configuration > Descriptors window. When you configure or update descriptors and controls, the IDC of the any user who is associated to a radio gets updated.

Note When you configure channel selectors, consider the different actions that users may want to perform on the channel and which commands need to be sent to the radio when those actions are performed.

The channel selector attributes include the following elements:

- Label—This field specifies the name of the radio channel selector, as defined in the radio descriptor file. See the "Managing Radio Descriptors" section on page 9-21 for more information about descriptors.

Note When you configure channel selector attributes, be aware that mixing left-to-right (LTR) and right-to-left (RTL) character sets for different languages may cause undesirable behaviors in the server or IDC.

- Enabled—If checked, this box indicates whether a PTT channel is allowed to associate to this channel. That is, this channel selector displays in the drop-down list for the radio connection for the channel.
- Associated Channel—This field displays the name of the currently associated channel and its short name (a condensed name of the channel).

Tone Sequence Configuration (Tone Control Radios)

The tone control sequences, which are defined in a radio descriptor file, contain information about how to tune the radio to another channel within that radio. See the "Managing Radio Descriptors" section on page 9-21 for more information.

You can also configure default tone sequences. However, be aware of the caveats that the "Caveats for Configuring Default Tone Sequences (Tone Control Radios)" section on page 9-6 describes before you configure these sequences.

The control attributes for tone sequences include the following elements:

- Label—This field indicates the name of the tone sequence, as defined in the tone descriptor file. These sequences may include names such as Monitor On/Off or Hi/Medium/Low Power and are used to identify a tone sequence.
- Enabled—If checked, this check box indicates that this control can be made available to the IDC.
- Description—This field indicates a description of the tone control sequence. A tone control can be either a stateful or momentary operation.

  If a control is stateful, the IDC displays the button.

  For example, Encryption is a stateful operation and the IDC monitors its setting. Another example is a Transmit Power setting that can be toggled between High, Medium, and Low.

  A momentary control is one in which the functional state is not monitored or remembered. Most signals are momentary, meaning that they are sent without being monitored by the system.

Note Because of the limitations of tone-controlled radios, you may be able to toggle a feature on, but you may not have any way to know when the feature has been toggled back. For example, even though you can enable monitor mode, this mode can be turned off for a variety of reasons, including pressing the PTT button or changing the radio channel.

For more information about tone and radio descriptors, see the "Tone Descriptors" section on page 9-21 and the "Understanding the Descriptors Window" section on page 9-35.

Caveats for Configuring Default Tone Sequences (Tone Control Radios)

Cisco IPICS allows you to configure a default tone sequence that transmits on the last used channel whenever the currently-tuned channel is unknown.

Note Be aware that the channel on which the tone sequence transmits is determined by the capabilities of the specific radio equipment systems that are being used and you should configure the channel based on that information.

You can configure the following options for a default channel:

- Associate to no tones
- A tone sequence that instructs that the radio transmits on a default channel, such as F1
- A tone sequence that instructs that the radio transmits on the currently-tuned channel, if that capability is available

Note When some users do not have access to channel selectors and cannot select a channel on which to transmit, the IDC does not know which channel the radio has been tuned to. Therefore, the IDC does not provide the user with a visual indicator and does not allow the user to transmit under those conditions. The channel that gets used depends on the configuration and on the radio capabilities as described earlier in this chapter.

Be aware that when you configure a default tone sequence, it may transmit over an unintended channel under the following conditions:

- If you configure the system so that a default tone sequence transmits on the currently-tuned channel, Cisco IPICS uses the last used channel to transmit if the transmission occurs before a specific channel has been selected.
- If an IDC user pushes a PTT button to talk, the tone control sequence may transmit over that specific channel, even if it was not the intended channel to use for transmission.
- If an IDC user begins to transmit while another user attempts to change channels in the same radio, transmission may occur in the channel that was selected by the second user. Or, the channel may not actually be changed but the tone control sequence sent by the attempted channel change may transmit over an unintended frequency.

Note The behavior of the IDC depends on the capabilities of the radio system that is being used.

Understanding the Radios Window

The Configuration > Radios window, in the Administration Console, lists information about each of the radios that you have added in Cisco IPICS.

Table 9-1 describes the items in the Radios window.

Table 9-1 Items in the Radios Window

Item	Description	Reference
Table Columns		
Name	Indicates the names of radios that are configured in Cisco IPICS.	See the "Adding a Radio" section on page 9-8 and the "Viewing and Editing Radio Details" section on page 9-14.
Radio Type	Indicates the name of the radio descriptor that is associated with the radio. The radio descriptor describes the radio type and associated channel selectors and control functions.	
Control Type	Indicates whether the radio is tone controlled or serial controlled.	
Pooled (Serial controlled radios only)	Indicates whether the radio is enabled as a pooled resource and whether it is currently allocated. Pooled radios cannot be controlled manually. They are automatically allocated and configured by Cisco IPICS on demand when a channel is activated via a VTG or a user on an IDC. The value does not apply if the radio is tone controlled.	See the "Adding a Radio" section on page 9-8 and the "Viewing and Editing Radio Details" section on page 9-14.
Status	Indicates whether the radio is enabled or disabled. Disabled radios cannot be controlled and are not available on the pool.	
Control Status (Serial controlled radios only)	Indicates the control status of the radio. The value does not apply if the radio is tone controlled.	
Reserved By (Serial controlled radios only)	Indicates whether a radio that is not a pooled resource is reserved by a user or VTG. The value does not apply if the radio is tone controlled or if the radio is a pooled resource.	
VTG	Indicates whether the radio can be assigned to a VTG.	
User	Indicates whether the radio can be assigned to a user.	
Buttons		
Add	Click this button to configure new radios.	See the "Adding a Radio" section on page 9-8.
Delete	Click this button to delete radios from Cisco IPICS.	See the "Deleting a Radio" section on page 9-18.
Associations	Click this button to associate radios to users.	See the "Associating a User to a Radio From the Radios Window" section on page 9-15.
Radio Control (Non-pooled serial controlled radios only)	Opens a browser-based control user interface. This button is active only if you check the check box for a single non-pooled serial controlled radio. It is dimmed if the radio is tone controlled or pooled, or if multiple check boxes are checked.	See the "Accessing and Using the Serial Radio Control Interface" section on page 9-18.

Table 9-1 Items in the Radios Window (continued)

Item	Description	Reference
Display Controls		
Rows per page drop-down list	Specifies the number of rows of radios that are included in a radios list page.	See the "Navigating Item Lists" section on page 1-13.
Page field	Displays radios on a specific page.	
|< (First page) button	Displays the first page of the radio list.	
< (Previous page) button	Displays the previous page of the radio list.	
> (Next page) button	Displays the next page of the radio list.	
>| (Last page) button	Displays the last page of the radio list.	

Adding a Radio

When you add a radio it becomes available for use by Cisco IPICS.

Before you add a radio, make sure that you configure locations, as described in the "Managing Locations" section on page 2-27.

To add a new radio, perform the following procedure:

Procedure

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

Step 2 In the Radios window, click **Add** and designate the type of radio that you want to add by choosing one of these options from the drop-down list that displays:

- **Add Tone Controlled Radio**
- **Add Serial Controlled Radio**
- **Add ISSI Gateway**

The General tab for a new radio displays. Table 9-2 describes the fields in this tab.

Note Depending on the type of radio being added, the fields available in the General tab for a new radio differ. When a filed does not apply to all three radio types, Table 9-2 indicates to which radio types the field does apply.

Table 9-2 General Tab Fields in Radios Window

Field	Description
General Information Area	
Name	Enter the name of the radio.
Radio Type	Choose the type of radio from the drop-down list. The choices that display for radio type are based on the radio types that are in the radio descriptor files. For more information about radio descriptor files, see the "Managing Radio Descriptors" section on page 9-21.

Table 9-2 General Tab Fields in Radios Window (continued)

Field	Description
Description	Enter a description of the radio.
Pooled Resource	**Note** This field is available only when adding a serial controlled radio. Check this check box to designate that the radio is a pooled resource. Pooled radios are not controlled manually. They are automatically allocated and configured by Cisco IPICS on demand when a channel is activated via a VTG or a user on an IDC.
Content Source Information Area	
Location	Choose a location for the radio from the drop-down list. Location is used to determine how the IDC client can reach the radio (via multicast or unicast). **Note** IDC users must log in from the same location as the radio to access it. Cisco IPICS supports remote log in only if the Cisco IPICS server is configured with an RMS in the same location as the radio. See the "Managing Locations" section on page 2-27for information about configuring locations.
Multicast Address	Depending on the radio type, do one of the following: • For a tone controlled radio, enter the multicast address that is used to transmit audio and tones. • For a serial controlled radio or an ISSI gateway, enter the multicast address that is defined in the dial peer configuration of the LMR gateway.
Multicast Port	Depending on the radio type, do one of the following: • For a tone controlled radio, enter the multicast port for the radio. • For a serial controlled radio or an ISSI gateway, enter the port number that is defined in the dial peer configuration of the LMR gateway.
Codec	**Note** This option is available only when adding a serial controlled radio or tone controlled radio. Enter the codec that is defined in the dial peer configuration of the LMR gateway.
Secure Radio	**Note** This option is available only when adding a serial controlled radio or tone controlled radio. Choose **Yes** or **No** from the drop-down list. **Note** This field defines the security label of the radio only, and not the security of the individual channels that can be carried over the radio.

Table 9-2 General Tab Fields in Radios Window (continued)

Field	Description
Voice Delay (msec)	**Note** This field is available only when adding a tone controlled radio. This field specifies a value, in milliseconds, that is set on the LMR gateway that you must replicate on the server for radio instances that are associated to the router. The value of this parameter on the router determines how long the LMR gateway delays the audio before sending it to the radio. The delay is necessary to ensure that tones do not overlap with audio when the static tone configuration is used in the dial peers. **Note** Make sure that the value that you enter for this parameter is the same that is configured on the LMR gateway. This field must map to the value that is entered in the timing delay-voice tdm CLI command. see *Solution Reference Network Design (SRND)* (latest version) for more information.
Hangover Time (msec)	**Note** This field is available only when adding a tone controlled radio. This field specifies a value, in milliseconds, that is set on the LMR gateway that you must replicate on the server for radio instances that are associated to the router. The value of this parameter on the router determines how long the LMR gateway keeps the radio keyed after the last audio packet is received on a talk spurt. This setting is used to protect the system against packet loss and to accommodate for the configured delay time. Hangover time is usually larger than the delay time to ensure that all the buffered audio is played before unkeying the radio. **Note** Make sure that the value that you enter for this parameter is the same that is configured on the LMR gateway. See *Solution Reference Network Design (SRND)* (latest version) for more information. Valid values: 0 through 10000 **Note** This option is available only when adding a tone controlled radio.
Ops Views Area	
Ops Views— *Display only*	Indicates that the radio is associated to the System ops view. For general information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."
Restrictions Area	
Allow association to users	Check this check box if you want the radio to be available for association with on ore more users.

Table 9-2 General Tab Fields in Radios Window (continued)

Field	Description
Allow use in VTGs	**Note** This option is available only when adding a serial controlled radio or tone controlled radio. ISSI Gateways do not support this option. Check this check box if you want the radio to be available for use in one or more VTGs. If you do not check this check box, the radio can be used only for the following: • For a tone controlled radio, as a channel media connection. • For a serial controlled radio, only to place private calls to another serial radio.
Radio Controlled Service Area	
RCS Name	**Note** This field is available only when adding a serial controlled radio or ISSI Gateway. Valid values: **local-rcs** or **Auto Select**
Radio Connection Area **Note** The Radio Connection area is available only when adding a serial controlled radio.	
IP Address	Enter the IP address of the LMR gateway to which the radio connects.
Port	Enter the port number of the auxiliary or asynchronous line of the LMR gateway to which the radio is physically connected. Determine this port number by adding 4,000 to the line number to which the radio is serially connected. To find the line number, use the **show line** command on the LMR gateway.
User Name	*Optional*. Enter the user name of the LMR gateway.
Password	*Optional*. Enter the password of the LMR gateway.
ISSIG Connection Area **Note** The ISSIG Connection area is available only when adding an ISSI Gateway.	
P25G Unit ID	Enter the unit ID number for the P25 gateway (P25G). When a multicast client streams media, the P25G converts the G.711 stream to an IMBE stream over the ISSI. This requires the use of a unit ID. The P25G unit ID serves as proxy unit ID for multicast communications. The P25G Unit ID must be entered as a 6-digit hexadecimal value. Valid values: 000001 through FFFFFC
P25G IP Address	Enter the IP address of the P25G.

Table 9-2 General Tab Fields in Radios Window (continued)

Field	Description
RFSSG ID	Enter the ID number for the radio frequency sub-system gateway (RFSSG). The RFSSG serves as a gateway to other radio frequency sub-systems (RFSSs). The RFSSG ID is comprised of the following three IDs, from left to right: • Site ID; valid values: 01 through FF • System ID; valid values: 001 through FFF • Wide Area Connection Number (WACN) ID; valid values: 00001 through FFFFF
RFSSG IP Address	Enter the IP address for the RFSSG, which is the same IP address as the deployed ISSIG.

Step 3 Click **Save**.

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

Note If you are adding a serial radio and the IP address/port provided in the radio connection section is unreachable, the radio could take as long as 30 seconds to save. This applies only to serial radios.

Step 4 To configure channel selectors for this radio, take these actions:

a. Click the **Selectors** tab.

b. In the Channel Selectors pane, check the check boxes next to the channel selectors that you want to enable.

If you want to check all check boxes at once, check the **Enabled** check box.

Note Channel selectors and radio controls are defined in the radio type descriptors.

c. In the Channel Selectors pane, choose a priority for each channel selector from the Priority drop-down lists.

Cisco IPICS uses this information to select a pooled radio when a channel selector for multiple pooled radios that belong to the same radio descriptor is used.

Priority levels are 1 (highest priority) through 5 (lowest priority). The default value is 3.

d. Click **Save**.

If you do not want to save these configurations, click **Cancel**.

Step 5 To configure Control Functions for this radio, take these action:

a. Click the **Controls** tab.

b. In the Controls pane, check the check boxes next to the controls that you want to enable.

If you want to check all check boxes at once, check the **Enabled** check box.

Note Radio controls are defined in the radio type descriptors.

c. Click **Save**.

If you do not want to save these configurations, click **Cancel**.

For detailed information about tone control sequences, see the "Configuring Channel Selectors and Control Sequences" section on page 9-4.

Step 6 To disable or enable the radio, click the **Disable** or **Enable** button.

If the radio is enabled, the **Disable** button displays. If the radio is disabled, the **Enable** button displays. For more information about enabling or disabling radios, see the "Enabling or Disabling a Radio" section on page 9-17.

Note If a pooled radio is allocated to a channel, the name of the channel and a link to the channel display for Pooled Usage in the General area. You cannot disable a pooled radio that is allocated to a channel until it is released by all IDC users and VTGs that activated the channel that uses the pooled radio. You also can force a radio to be deallocated by clicking the **Deallocate** button in the radio details page.

Step 7 To configure the IDC details for this radio, take these actions:

a. Click the **IDC** tab.

The IDC tab for the selected channel displays. This window contains IDC information for this radio. Table 9-3 describes the fields in the IDC tab.

Table 9-3 IDC Tab Fields in Radios Window

Field	Description
IDC Tab	
RX Mute During PTT	This attribute specifies the transmission settings for all radios or only one radio. It controls the audio for the active radios while you are transmitting. The following values affect how the mute functionality is configured on the IDC: • None—When PTT is engaged, the radio is muted • All—When PTT is engaged, RX (receive transmission) is muted on all channels • Radio—When radio is engaged, RX is muted for this radio only **Note** When you initially assign a radio to the IDC, the RX mute settings that you have configured apply. The IDC user can modify this setting. However, if you change the setting after the radio has been assigned to the user, the changes do not become effective.
Allow Latch	When set to true (attribute check box is checked) on a radio or VTG, the user can use latch (lock in radios) on any radio that you specify. **Caution** Use the latch functionality with caution. Be aware that when you latch the PTT button, this action blocks transmissions from half-duplex radios when these devices are attached to the channel or VTG via an LMR gateway. By default, this attribute is set to false (attribute check box is unchecked).

Table 9-3 IDC Tab Fields in Radios Window (continued)

Field	Description
Listen Only	When set to true (attribute check box is checked), the user can hear but cannot talk, on the radio.
Radio Color	Color tag that you can choose from a drop-down list. With this setting, you can uniquely identify specific radios by using predefined colors for the background text that appears on the radio. You configure the color by choosing from the options in the drop-down list. **Note** If you do not want the radio to be tagged with a color, you can choose **Not colored** from the drop-down list.
Region	Choose an IDC region from the drop-down list. When configured, the regions appear as tabs in the IDC display for IDC users who are associated with this radio. To create IDC regions, see the "Adding IDC Regions" section on page 2-96.

b. Click **Save**.

If you do not want to save these configurations, click **Cancel**.

To associate users to a radio, see the "Associating a User to a Radio From the Radios Window" section on page 9-15.

Viewing and Editing Radio Details

You can view and edit information for any radio. Information that you can modify for a radio includes changing the name of a radio, enabling or disabling the channel selectors and tone control sequences, enabling or disabling the radio, and associating the radio to users.

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

Procedure

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

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

The General tab for the selected radio displays.

Step 3 Take any of the following actions:

- To view or edit general information, update information in the General tab, then click **Save**.

  For descriptions of the fields in the General tab, see Table 9-2 on page 9-8.
- To view or edit IDC information, update information in the IDC tab, then click **Save**.

  For descriptions of the fields in the IDC tab, see Table 9-3 on page 9-13.
- To enable or disable channel selectors for the radio, check or uncheck the check boxes next to the channel selectors that you want to modify in the Selectors tab, then click **Save**.
- To enable or disable tone control sequences for the radio, check or uncheck the check boxes next to the tone control sequences that you want to modify in the Controls tab, then click **Save**.

Note

- If you are saving a serial radio and the IP address/port provided in the radio connection section is unreachable, the radio could take as much as 30 seconds to save.
- If radio descriptor files are renamed, deleted, or corrupted, an error message displays in the Radio Management window. This message includes the affected radio descriptor files and a recommendation about how to proceed.

Step 4 To view or edit the IDC attributes for the radio, make the desired changes in the **IDC** tab, then click **Save**.

For descriptions of the fields in the IDC tab, see Table 9-3 on page 9-13.

Step 5 To view or edit radio associations, see the "Associating a User to a Radio From the Radios Window" section on page 9-15.

Associating a User to a Radio From the Radios Window

You can associate specific users to a radio in the Radios window. When you do so, the radios that you choose become available on an IDC.

When you associate a user with a radio, the user has the permission to change to any enabled channel on that radio. However, you can restrict the channels to which the user can tune by setting radio permissions for that user.

Because the radio permissions are separate from channel permissions, a user could have permission to tune a channel on a radio but not have access to the association Cisco IPICS channel.

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

You can also associate a user with a radio in the Users window. For information, see the "Associating Radios with a User" section on page 3-22.

To associate a user with a radio, perform the following procedure:

Procedure

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

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

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

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

The Users tab displays for the radio. This tab displays a list of the users that are associated with the radio and the status of each user.

Step 3 To add a user to be associated with the radio, click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the radio by choosing criteria that is 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—Choose from a list of locations

  See the "Managing Locations" section on page 2-27 for detailed information about how to configure locations.
- Role drop-down list—Choose from a list of Cisco IPICS roles
- Ops View drop-down list—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria; 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 radio, 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.

Note You can add multiple users simultaneously by clicking the check boxes next to each user and clicking **OK**.

Step 6 To view or edit radio permissions for a user, select the user by checking the check box next to the user name and choose one of the following options from the Radio Permissions drop-down list:

- **Channel Selector Permissions**—When you choose this option, a separate window displays for channel selector permissions. In this window, you can configure specific channels that the user can communicate on.
- **Control Function Permissions**—When you choose this option, a separate window displays for radio control function permissions. In this window, you can configure specific radio controls that the user can access to control the radio.

Note The Radio Permissions drop-down list appears dimmed if you do not have any users checked or if you have more than one user checked.

Step 7 To select the radio permissions on this radio for the user, take any of the following actions in the applicable radio permissions window:

- To move a channel selector or control function from one list to the other, click the item to highlight it; then, click **>** or **<**. Or, double-click the item.
- To move several channel selectors or control functions from one list to the other at one time, **Shift-click** or **Ctrl-click** to select the items, then, click **>** or **<**.
- To move all channel selectors/control functions from one list to the other at one time, click **>>** or **<<**.

Step 8 Click **Save**.

Note If you are saving a serial radio and the IP address/port provided in the radio connection section is unreachable, then the radio could take as much as 30 seconds to save.

Step 9 To remove a user from the association to the radio, check the check box to the left of the user name; then, click the **Delete** button.

You can remove multiple users from the association at the same time by checking the check boxes that display by the user names of the users that you want to remove and clicking **Delete**.

Enabling or Disabling a Radio

You can enable or disable a radio in Cisco IPICS. If the radio is disabled, you can can still modify the multicast address, location, LLGT, and all of the other attributes of the radio. However, if the radio is enabled, you cannot modify these attributes.

If the radio is part of an active VTG and you disable the radio, it disconnects from the VTG.

Note After you define a radio, the radio type cannot be changed even if you disable the radio. If you want to change the radio type after you define the radio, you must delete the radio and create a new radio instance. If you only want to modify the types of tones on a radio type, you can upload a new descriptor file for the same radio type and the changes get applied to that radio instance. For more information about descriptors, see the "Managing Radio Descriptors" section on page 9-21.

To enable or disable a radio, perform the following procedure:

Procedure

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

Step 2 Under the Name column, click the link of the radio that you want to enable or disable.

The General tab displays for the radio.

Step 3 To enable or disable the radio, click the **Enable/Disable** button at the bottom of the window.

Note If the radio is currently enabled, only the **Disable** button displays. If the radio is currently disabled, only the **Enable** button displays.

If you do not want to enable or disable the radio, click **Cancel**.

Deleting a Radio

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

Before you delete a radio, you must remove any associated media connections in all of the channels for that radio.

Note You cannot delete a pooled radio that is allocated to a channel. Before deleting the radio, deactivate the VTG that caused the channel activation or have all users that activated the channel deactivate it. You can also can force a radio to be deallocated by clicking the **Deallocate** button in the radio details page. After the radio is forcibly deallocated, you can delete it.

To delete a radio, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each radio 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 radio, click **Cancel**.

Accessing and Using the Serial Radio Control Interface

After you configure a serial controlled radio, you can access and use the SRCI from an IDC, as described in *IPICS Dispatch Console User Guide* for this release, or from the Cisco IPICS Administration Console.

To access the SRCI from the Administration Console, perform any of the following actions:

- Navigate to the **Configuration > Radios** window, click the link for the desired radio in the Name column, then click **Controls**, which displays at the bottom of each tab.
- Navigate to the **Configuration > Radios** window, check the check box next to the radio for which you want to access the SRCI, then click **Radio Control**.
- Navigate to the **VTG Management > Virtual Talk Groups** window, and click a VTG name. In the **Participants** tab, double-click a radio in the Participants or Resources box.
- If the radio is associated with a user, navigate to **User Management > Users**, choose a user, click **Associations**, choose the Radio tab, choose the desired radio, then click **Radio Control**.

The SRCI displays in its own page and is organized as follows:

Radio Information

The top area of the SRCI provides the following information and functions:

- Name of the radio, as configured in the Name field in the General tab for the radio.
- Type of the radio, as defined in the radio descriptor.

- Connection status of the radio, which can be any of the following:
  - CONNECTED_ONLINE—Radio is ready for control.
  - CONNECTED_OFFLINE—Radio connection to the LMR gateway is active, but Cisco IPICS cannot communicate with the radio. This situation can occur if the radio is turned off or is not connected to the correct asynchronous line on the correct LMR gateway, or if the connected radio is of the wrong type.
  - AUTHENTICATION_FAILURE—The login credentials provided in the radio details are not correct and IPICS cannot connect to the specified port on the LMR Gateway.
  - SOCKET_FAILURE—Cisco IPICS cannot connect to the LMR gateway IP address and port that are as configured in the General tab for the radio. This situation can occur if the IP address or port number are incorrect, the LMR gateway is turned off, the LMR gateway is disconnected from the network or in an unreachable network, or the LMR gateway is in use and needs to be cleared.
  - DISCONNECTED—Cisco IPICS has not initialized the connection or is in the process of re-initializing the connection because of a SOCKET_FAILURE or AUTHENTICATION_FAILURE situation.
  - RADIO CONTROL SERVICE UNAVAILABLE: The Cisco IPICS Radio Control Service is down and needs to be restarted.
- **Reserve/Release** toggle button—The **Reserve** button allows you to indicate to other users that you would like to use this radio. When you click this button, your Cisco IPICS user name and full name appear in the Reserved By field and the date and time that you clicked it appear in the Reserved On field. In addition, the name of the button changes to **Release**. In this case, other SRCI and IDC users see the **Release** button and they see your information in the Reserved By and Reserved On fields.

  This function is provided as a courtesy only and does not block any user from controlling the radio. Any SRCI or IDC user can click the **Release** button, which clears the Reserved By and Reserved On information and changes the button name to **Reserve**.

  If the radio is in an active VTG, Cisco IPICS disables the **Reserve/Release** button. In addition, the VTG name and the date and time that this radio was added to the VTG appear in the Reserved by field, with the date and time this radio was added to the active VTG. (Any user can control a radio that is reserved by a VTG.)

Radio Display and Controls

The second-from-the-top area of the SRCI provides the following information:

- The type of call that is active on the controlled radio, followed by the channel selector name, the private call alias/ID, or the group call name. Call types are indicated as follows:
  - [Channel/TG]—Conventional channel and trunked talkgroup operation
  - [Private Call]—Unit to unit calls (iDEN and Sprint Nextel only)
  - [Group Call]—Dynamic group operation (iDEN and Sprint Nextel only)
- A green icon that appears when there is inbound voice traffic on the channel.
- When there is inbound voice to the radio and the radio detects the talker ID, this ID displays below the channel selector for the duration of the inbound voice.
- Configured control functions. Each function appears as a button, and the current state of each function displays above the corresponding button.

Channel Selectors

The third-from-the-top area of the SRCI includes channel selectors. Each configured channel selector displays as a button. Depending on the radio control configuration, a user may be able to press a channel selector button to change the channel/talkgroup on the radio or place a private or group call.

IPICS Connect

Applies to Nextel radios only.

The bottom area of the SRCI allows you to make private calls, group calls, and call alerts (pages). This area applies to Nextel radios only.

Making private and group calls from the channel selector area is a one touch operation. From the IPICS Connect box, you can make ad-hoc private and group calls, including combining users from different predefined groups. You can also send a call alert (page) to a predefined participant or ad-hoc participant.

The names that display in the Select From Groups/Users list come from channel selectors for private and group calls that are defined in the serial radio descriptor, and from Cisco IPICS users that are associated with a Nextel radio.

To make a private call, follow these steps:

Step 1 Take either of these actions:

- Enter a direct connect number to call in the Direct Connector Number field and then click **<<** to move the number to the Participants list. The number must be in a Nextel-supported format.
- Click a name of a user to call in the Groups/Users list and then click **<<** to move the name to the Participants list.

Step 2 Click **Call** to initiate the private call to the selected number or user.

To make a group call, follow these steps:

Step 1 Enter a group name (from 1 to 20 characters) in the Group/User Alias field.

Step 2 Take either or both of these actions:

- Enter a direct connect number in the Direct Connector Number field and then click **<<** to move the number to the Participants list.
- Click a name in the Groups/Users list and then click **<<** to move the item to the Participants list.

Repeat this step as needed to specify up to 20 items in the Participants list.

Step 3 Click **Call** to initiate the group call.

To send a call alert, also known as a page, follow these steps:

Step 1 Take either of these actions:

- Enter a direct connect number to page in the Direct Connector Number field and then click **<<** to move the number to the Participants list.
- Click a name of the user to page in the Groups/Users list and then click **<<** to move the name to the Participants list.

Step 2 Click **Alert** to initiate the alert to the selected direct connect number or user.

You can send a call alert only to one participant at a time.

Managing Radio Descriptors

This section describes radio and tone descriptor management tasks and includes the following topics:

- Tone Descriptors, page 9-21
- Tone Radio Descriptors, page 9-22
- Serial Radio Descriptors, page 9-25
- ISSIG Descriptors, page 9-31
- Caveats for IDC Operation, page 9-34
- Understanding the Descriptors Window, page 9-35
- Adding Descriptors, page 9-36
- Updating Radio and Tone Descriptors, page 9-37
- Deleting Radio and Tone Descriptors, page 9-38

Tone Descriptors

A tone descriptor file is an .xml file that defines commands and over-the-air signals that can be associated to one or more Cisco IPICS channels. Commands can be referenced by any radio descriptor and signals can be associated to any channel.

A tone sequence is a list of tones and events that are used to either control a radio or to signal a channel. For more information about tone sequences, see the "Configuring Channel Selectors and Control Sequences" section on page 9-4.

Most tone control radios support a standard set of tone sequences. Some sequences are used to change the RF channel, while other sequences are used to enable the scan functionality on a radio. There are many more tone sequences that are used for tone signaling.

For tone sequences, Cisco IPICS supports both RFC 2833 tone and RFC 2833 event (DTMF) commands. For more information, see the "Caveats for IDC Operation" section on page 9-34.

For some examples of valid and invalid descriptor file entries, see the "Examples of descriptor .xml files" section on page 9-24.

Unlike momentary controls, signals do not cause the radio to change configuration; rather, signals are treated like voice and are transmitted over the currently-tuned radio channel frequency.

Each tone in a sequence is specified by the frequency (from 0 to 3999 Hz), a decibel (db) level (0 to –63), and a duration in milliseconds. This sequence of tones can be used by different radios. For tone signaling purposes, each telephony event in a sequence is specified by the event type (from 0 to 255), a db level (0 to –63), and a duration in milliseconds.

Note Any RFC 2833 tone or event has a maximum duration of eight seconds. See the "Caveats for IDC Operation" section on page 9-34 for more information.

The Cisco IPICS server provides signaling sequences in an example tone descriptor file called ExampleToneSet.xml; however, you may need to modify this example file or create additional tone descriptors that properly model your specific radio hardware. To add or update descriptors, see the "Managing Radio Descriptors" section on page 9-21.

Note

- If you must modify or create tone descriptors, see the documentation that you received with your radio or other device that you need to control for the specific signaling sequences that it supports.
- When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file. See the "Adding Descriptors" section on page 9-36 and "Updating Radio and Tone Descriptors" section on page 9-37 for more information.

Caution Improperly constructing an .xml file, removing a tone descriptor file, or removing elements from a tone descriptor file that is referenced by a radio descriptor file may have unpredictable results. Cisco recommends that you only modify the tone descriptor file when absolutely necessary.

For information about the descriptor management functions in the Descriptors window, see the "Understanding the Descriptors Window" section on page 9-35.

Tone Radio Descriptors

Radio descriptors define the controls that a particular type of tone control or serial control radio supports.

Note A radio type may refer to a specific make and model of radio or special tone-controlled hardware, such as a CPI box, which interprets the inband tones and causes the configuration of an attached radio to be changed.

Radio descriptors are .xml files that contain commands that are used to control functions on a radio. These files contain the following elements:

- Channel selectors—Used to change the frequency on a radio
- Control functions—Stateful controls, such as power settings and encryption on/off, and simple (momentary) controls, such as monitor and scan

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file. See the "Adding Descriptors" section on page 9-36 and "Updating Radio and Tone Descriptors" section on page 9-37 for more information.

For each radio capability, the radio descriptor defines the tones (events) that need to be sent to the radio to enable or disable that capability.

Note For tone control channel selectors and control functions (both stateful and simple), Cisco IPICS supports only RFC 2833 tones. See the "Caveats for IDC Operation" section on page 9-34 for more information.

The tone control sequences that define the control functions can be included directly in the radio descriptor, or can be referenced by name in a tone descriptor file. For more information about tone descriptors, see the "Tone Descriptors" section on page 9-21.

The Cisco IPICS server provides an example radio descriptor file; however, you may need to modify this example and/or create additional radio descriptors that properly model your specific radio hardware. The example file is in the list of descriptors.

If you must modify or create radio descriptors, see the documentation that came with your radio, or other device that is being controlled, for the specific tone sequences that it supports.

Caution Because improperly constructing an .xml file, removing a radio descriptor file, or removing elements from a radio descriptor file may have unpredictable results, Cisco recommends that you only modify the radio descriptor file when absolutely necessary.

For more information about adding or modifying descriptor files, see the "Managing Radio Descriptors" section on page 9-21. To see examples of valid and invalid descriptor file .xml entries, see the "Examples of descriptor .xml files" section on page 9-24.

See the "Radio Descriptor Format" section on page 9-23 for an example of the format of a radio descriptor.

Radio Descriptor Format

The following example shows the format of a radio descriptor .xml file:

Radio Descriptor File Format

```
<?xml version="1.0" encoding="UTF-8"?>
<ipics:RadioTypeDescriptor... name="CPITestBox">
```

where:

name= represents the name of the radio type that displays in the UI; this name should be unique.

```
<Commands>... </Commands>
```

Commands define "macro-like" tone/event sequences that can be used elsewhere within the radio descriptor.

```
<ChannelSelectors>... </ChannelSelectors>
```

Channel selectors define the available tone sequences needed to use each channel on the radio.

```
<ControlFunctions>... </ControlFunctions>
```

Control functions define the available stateful control sequences and the tones that need to be sent to enable each stateful state.

Examples of descriptor .xml files

The following example shows valid radio signaling .xml entries. Even though this example shows more than six consecutive RFC 2833 tone sequences, it is still valid because the tones are separated by a pause entry of at least 1 ms (frequency = 0 tone).

```
<Signal shortName="TV" longName="Start TV" description="Start the Television">
    <Action type="pressed">
        <Command>
            <Rfc2833Tone db="0" duration="40" frequency="100" />
            <Rfc2833Tone db="0" duration="40" frequency="200" />
.
.
.
duration="40" frequency="600" />
            <Rfc2833Tone db="0" duration="1" frequency="0" />
            <Rfc2833Tone db="0" duration="40" frequency="700" />
            <Rfc2833Tone db="0" duration="40" frequency="800" />
        </Command>
    </Action>
</Signal>
```

The remaining examples involve invalid entries.

The following example shows more than six RFC 2833 tone entries as part of a radio signaling tone sequence and does not include any pause entries.

```
<Signal shortName="TV" longName="Start TV" description="Start the Television">
    <Action type="pressed">
        <Command>
            <Rfc2833Tone db="0" duration="40" frequency="100" />
            <Rfc2833Tone db="0" duration="40" frequency="200" />
            <Rfc2833Tone db="0" duration="40" frequency="300" />
            <Rfc2833Tone db="0" duration="40" frequency="400" />
            <Rfc2833Tone db="0" duration="40" frequency="500" />
            <Rfc2833Tone db="0" duration="40" frequency="600" />
            <Rfc2833Tone db="0" duration="40" frequency="700" />
        </Command>
    </Action>
</Signal>
```

The following example shows DTMF events as part of a radio control tone sequence.

```
<ChannelSelector label="F2">
    <Action type="tune">
        <CommandRef href="hlgt" />
        <Command>
            <Rfc2833Tone db="-10" duration="40" frequency="1850" />
            <Rfc2833Event db="-30" duration="200" event="5" />
        </Command>
    </Action>
    <Action type="begintransmit">
        <CommandRef href="hlgt" />
        <Command>
           <Rfc2833Tone db="-10" duration="40" frequency="1850" />
           <Rfc2833Event db="-30" duration="200" event="5" />
        </Command>
        <CommandRef href="llgt" />
    </Action>
</ChannelSelector>
```

The following example shows more than six consecutive RFC 2833 radio control tone sequences.

```
<State shortName="On">
    <Action type="pressed">
        <Command>
            <Rfc2833Tone db="-10" duration="200" frequency="1105" />
.
.
.
          <Rfc2833Tone db="-10" duration="200" frequency="1605" />
            <Rfc2833Tone db="-10" duration="200" frequency="1705" />
        </Command>
    </Action>
</State>
```

Serial Radio Descriptors

The following sections describe the general steps for creating a serial descriptor for serial radio control:

- Step 1: Create the Header, page 9-25
- Step 2: Create the Body, page 9-25

Step 1: Create the Header

A radio descriptor begins with the element <SerialRadioTypeDescriptor>. This element includes the following attributes:

- name—Contains 1 through 64 characters and specifies the name of the radio descriptor.
- controlType—Always set to SERIAL.
- controlModule—Specifies the type of radio that is controlled. Use “Nextel” for iDEN radios in a Sprint Nextel or private iDEN network. Use “EFJohnson” for EF Johnson model 5300 mobile radios.

The following is an example of a serial descriptor header:

```
<ipics:SerialRadioTypeDescriptor xmlns:ipics=        "urn:com.cisco.ipics.RadioDescriptor"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:schemaLocation="urn:com.cisco.ipics.RadioDescriptor
../../SerialRadioTypeDescriptor.xsd "
               name="Nextel"
               controlType="SERIAL"
               controlModule="Nextel">
```

Step 2: Create the Body

The body of the radio descriptor has two main sections, <ChannelSelectors> and <ControlFunctions>, each of which define buttons that the SRCI renders.

Channel Selectors

<ChannelSelector> elements are controls that set up the radio for a specific mode of communication. The controls include selecting a channel/talkgroup on the radio or placing a private or dynamic group all.

Each <ChannelSelector> has a required “label” attribute that is 1 through 12 characters in length and that defines the name of a button that the SRCI renders.

The <Action> element within each <ChannelSelector> includes the “type” attribute. This attribute must be set to “tune” and indicates that this control is communications related.

The <Action> element includes the <Command> element. This attribute specifies the tuning action and can be either <Channel> or <GroupCall>.

Selecting a Channel or Talkgroup

For channel or talkgroup controls, the element within <Command> must be <Channel>. The <Channel> element must include these attributes:

- zone—Must be set to a valid zone in the radio that represents this channel selector.
- channel—Must be set to a valid channel in the radio that represents this channel selector.

iDEN radios do not have the concept of zones and channels. For these radios, always set the zone attribute 1. The channel attribute represents the talkgroup ID and can range from 1 to 200.

The following example shows the use of the <ChannelSelector> element:

```
<ChannelSelector label="CHAN 5">
          <Action type="tune">
                    <Command>
                              <Channel zone="1" channel="5" />
                    </Command>
          </Action>
</ChannelSelector>
```

Setting up a Private Call

This feature applies only to iDEN radios.

To define a channel selector that can set up a private call, the <Command> element must contain a child element called <GroupCall>. The <GroupCall> element includes the “name” attribute, which defines the name of the button that represents this private call. The “name” attribute can contain 1 through 12 characters.

The <GroupCall> element contains the ID of the remote radio that will participate in this call. The radio is represented by the <Call> element and contains an attribute called “number.”

The following example represents an iDEN private call with the direct connect number of the participant in the <Call> element:

```
<ChannelSelector label="W Plinge">
          <Action type="tune">
                    <Command>
                              <GroupCall groupName="W Plinge">
                                        <Call number="123*45678*9" />
                              </GroupCall>
                    </Command>
          /Action>
</ChannelSelector>
```

Setting up a Group Call

This feature applies only to iDEN radios that are in iDEN networks that are capable of dynamic group calls.

To define a channel selector that can set up a group call, the <Command> element contains one or more child elements called <GroupCall>. Each <GroupCall> element includes the “name” attribute, which defines the name of the button that represents this private call. The “name” attribute can contain 1 through 12 characters.

The following example represents an iDEN group call with the direct connect numbers of the participants in <Call> elements:

```
<ChannelSelector label="My Team">
          <Action type="tune">
                    <Command>
                              <GroupCall groupName="My Team">
                                        <Call number="123*45678*9" />
                                        <Call number="123*45678*10" />
                                        <Call number="123*45678*11" />
                                        <Call number="123*45678*12" />
                              </GroupCall>
                    </Command>
          </Action>
</ChannelSelector>
```

Control Functions

Control functions define buttons on the SRCI that can control certain functions of the control radio. Control functions do not exist in iDEN radios. These control functions are listed as <Simple> elements, with the following attributes:

“shortName” is an attribute of a control function. It is 1 through 12 characters in length and defines the name of the control as rendered on the SRCI.

“description” is an attribute of a control function. It describes the nature of the control function.

Each <Simple> element contains an <Action> element, which defines the control functions with the “type” attribute. An <Action> element is always set to a value of “pressed” and contains a <Command> element, which determines the specific command for the control function.

Cisco IPICS provides the following control functions:

- Monitor—When representing a control function to enable or disable monitor mode in the controlled radio, use the following xml within <ControlFunctions>:

```
<Stateful shortName="MON" longName="Monitor" description="Set Monitor Mode"
presentation="multiple">
                    <State shortName="ON" longName="ON" description="Monitor mode is
on" user_selectable="true">
                              <Action type="pressed">
                                        <Command>
                                                  <SetMonitorMode value="ON" />
                                        </Command>
                              </Action>
                    </State>
                    <State shortName="OFF" longName="OFF" description="Monitor mode
is off" user_selectable="true">
                              <Action type="pressed">
                                        <Command>
                                                  <SetMonitorMode value="OFF" />
                                        </Command>
                              </Action>
                    </State>
                    <State shortName="UNKWN" longName="UNKNOWN" description="Monitor
mode is in an unknown state" user_selectable="false">
                              <Action type="pressed">
                                        <Command>
                                                  <SetMonitorMode value="UNKNOWN" />
                                        </Command>
                              </Action>
                    </State>
                    <State shortName="UNSPRT" longName="UNSUPPORTED"
description="Monitor mode is not supported" user_selectable="false">
                              <Action type="pressed">
                                        <Command>
```

```
                                        <SetMonitorMode value="UNSUPPORTED" />
                                    </Command>
                                </Action>
                            </State>
                        </Stateful>
```

- Secure Transmit Mode—When representing a control function to toggle between secure and clear transmit modes in the controlled radio, use the following xml within <ControlFunctions>:

```
<Stateful shortName="SEC" longName="Secure Tx Mode" description="Select Between Secure
and Clear Transmit Modes" presentation="multiple">
                        <State shortName="SEC" longName="SECURE" description="Secure
transmit mode is set to SECURE" user_selectable="true">
                                <Action type="pressed">
                                        <Command>
                                                <SetSecureTxMode value="SECURE" />
                                        </Command>
                                </Action>
                        </State>
                        <State shortName="CLR" longName="CLEAR" description="Secure
transmit mode is set to CLEAR" user_selectable="true">
                                <Action type="pressed">
                                        <Command>
                                                <SetSecureTxMode value="CLEAR" />
                                        </Command>
                                </Action>
                        </State>
                       <State shortName="KEYFL" longName="KEYFAIL" description="Keyfail.
Key required for encryption is not present" user_selectable="false">
                                <Action type="pressed">
                                        <Command>
                                                <SetSecureTxMode value="KEYFAIL" />
                                        </Command>
                                </Action>
                        </State>
                        <State shortName="NOENC" longName="NO_ENCRYPT" description="No
encryption module present" user_selectable="false">
                                <Action type="pressed">
                                        <Command>
                                                <SetSecureTxMode value="NO_ENCRYPT" />
                                        </Command>
                                </Action>
                        </State>
                        <State shortName="MSMTCH" longName="MISMATCH"
description="Mismatch between user selected secure transmit mode and actual
fixed/strapped tx mode" user_selectable="false">
                                <Action type="pressed">
                                        <Command>
                                                <SetSecureTxMode value="MISMATCH" />
                                        </Command>
                                </Action>
                        </State>
                        <State shortName="UNKWN" longName="UNKNOWN"
description="Secure/Clear Transmit mode is in an unknown state"
user_selectable="false">
                                <Action type="pressed">
                                        <Command>
                                                <SetSecureTxMode value="UNKNOWN" />
                                        </Command>
                                </Action>
                        </State>
                        <State shortName="UNSPRT" longName="UNSUPPORTED"
description="Encryption is not supported" user_selectable="false">
                                <Action type="pressed">
```

```
                                    <Command>
                                          <SetSecureTxMode value="UNSUPPORTED" />
                                    </Command>
                              </Action>
                        </State>
                  </Stateful>
```

- Repeater/Talkaround—When representing a control function to toggle between repeater and talkaround modes in the controlled radio, use the following xml within <ControlFunctions>:

```
<Stateful shortName="RTA" longName="Repeater/Talkaround" description="Select Between
Repeater and Talkaround Transmit Modes" presentation="multiple">
                        <State shortName="RPTR" longName="REPEATER" description="Transmit
mode is set to REPEATER" user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetRepeaterTaMode value="REPEATER" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="TA" longName="TALKAROUND" description="Transmit
mode is set to TALKAROUND" user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetRepeaterTaMode value="TALKAROUND" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNKWN" longName="UNKNOWN"
description="Repeater/Talkaround mode is in an unknown state" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetRepeaterTaMode value="UNKNOWN" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNSPRT" longName="UNSUPPORTED"
description="Repeater/TA mode selection is not supported" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetRepeaterTaMode value="UNSUPPORTED" />
                                    </Command>
                              </Action>
                        </State>
                  </Stateful>
```

- Transmit Power—When representing a control function to toggle transmit power in the controlled radio, use the following xml within <ControlFunctions>:

```
<Stateful shortName="PWR" longName="Transmit Power Mode" description="Change the
transmit power level" presentation="multiple">
                        <State shortName="HIGH" longName="HIGH" description="Transmit
power mode is set to HIGH" user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetTxPowerMode value="HIGH" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="LOW" longName="LOW" description="Transmit power
mode is set to LOW" user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetTxPowerMode value="LOW" />
```

```
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNKWN" longName="UNKNOWN" description="Transmit
power mode is in an unknown state" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetTxPowerMode value="UNKNOWN" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNSPRT" longName="UNSUPPORTED"
description="Transmit power mode selection is not supported" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetTxPowerMode value="UNSUPPORTED" />
                                    </Command>
                               </Action>
                        </State>
                  </Stateful>
```

- Scan—When representing a control function to toggle scan mode in the controlled radio, use the following xml within <ControlFunctions>:

```
<Stateful shortName="SCN" longName="Scan" description="Set Scan Mode"
presentation="multiple">
                        <State shortName="ON" longName="ON" description="Scan is on"
user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetScanMode value="ON" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="OFF" longName="OFF" description="Scan is off"
user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetScanMode value="OFF" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNKWN" longName="UNKNOWN" description="Scan is
in an unknown state" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetScanMode value="UNKNOWN" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNSPRT" longName="UNSUPPORTED"
description="Scan is not supported" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetScanMode value="UNSUPPORTED" />
                                    </Command>
                              </Action>
                        </State>
                  </Stateful>
```

- Emergency Mode—When representing a control function to toggle emergency mode in the controlled radio, use the following xml within <ControlFunctions>:

```
<Stateful shortName="EMG" longName="Emergency" description="Enable/Disable Emergency
Mode" presentation="multiple">
                        <State shortName="ON" longName="ON" description="Emergency mode
is on" user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetEmergencyMode value="ON" />
                                    </Command>
                              </Action>
                        </State>
                       <State shortName="OFF" longName="OFF" description="Emergency mode
is off" user_selectable="true">
                              <Action type="pressed">
                                    <Command>
                                          <SetEmergencyMode value="OFF" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNKWN" longName="UNKNOWN"
description="Emergency mode is in an unknown state" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetEmergencyMode value="UNKNOWN" />
                                    </Command>
                              </Action>
                        </State>
                        <State shortName="UNSPRT" longName="UNSUPPORTED"
description="Emergency mode is not supported" user_selectable="false">
                              <Action type="pressed">
                                    <Command>
                                          <SetEmergencyMode value="UNSUPPORTED" />
                                    </Command>
                              </Action>
                        </State>
                  </Stateful>
```

ISSIG Descriptors

An ISSI Gateway (ISSIG) descriptor is identified by the following XML block:

```
<ipics:SerialRadioTypeDescriptor
xmlns:ipics="urn:com.cisco.ipics.RadioDescriptor"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:com.cisco.ipics.RadioDescriptor
../../SerialRadioTypeDescriptor.xsd "
name="ISSIG-Example" controlType="P25G"
controlModule="P25Gateway">
```

The controlType and controlModule attributes determine that it is an ISSIG descriptor.

Each group accessible by the ISSIG is defined as channel selectors in the following format:

```
<ChannelSelector label="TG 1R DES">
        <Action type="tune">
            <Command>
      <P25GroupCall groupId="0001" systemId="001" wacnId="00001" alias="TG 1R DES" type="S
tandard" sln="1" strapping="Selectable" />
            </Command>
        </Action>
</ChannelSelector>
```

The <P25GroupCall> element describes the subscriber group. The groupId attribute describes the subscriber group ID and is always a 4-digit hexadecimal value. The systemId attribute is always 3-digit hexadecimal value and is equal to that of the RFSS where the group is “homed” (provisioned). The wacnId attribute is always a 5-digit hexadecimal value and is that of the RFSS where the group is “homed” (provisioned). The alias attribute is similar to other channel selectors. The type attribute indicates whether the talkgroup is a “standard” talkgroup; currently “standard” is the only valid option. The encryption key is indicated by the sln attribute, and it refers to the Storage Location Number in the encryption module. The encryption strapping attribute indicates whether the transmit mode secure/clear selection is “selectable” (the IDC user can select secure or clear mode for transmissions), “secure” (a channel associated with this talkgroup shall always transmit in secure mode), and “clear” (a channel associated with this talkgroup shall always transmit in clear mode).

Control functions represent functions that can be toggled between their respective states. IPICS supports two control functions for ISSI interoperability: emergency and secure transmit mode.

Each control function element is call Simple and requires two attributes. The shortName attribute is the label that will appear on the radio control user interface within IPICS, and the description attribute appears as a description for the respective control function in the radio details screen in IPICS. The actual control function is represented within the Command element. The following examples show how the control functions should appear in a descriptor.

```
<ControlFunctions>
  <Stateful shortName="SEC" longName="Secure Tx Mode" description="Select Between Secure a
nd Clear Transmit Modes" presentation="multiple">
    <State shortName="SEC" longName="SECURE" description="Secure transmit mode is set to S
ECURE" user_selectable="true">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="SECURE" />
        </Command>
      </Action>
    </State>
    <State shortName="CLR" longName="CLEAR" description="Secure transmit mode is set to CL
EAR" user_selectable="true">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="CLEAR" />
        </Command>
      </Action>
    </State>
    <State shortName="KEYFL" longName="KEYFAIL" description="Keyfail. Key required for enc
ryption is not present" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="KEYFAIL" />
        </Command>
      </Action>
    </State>
    <State shortName="NOENC" longName="NO_ENCRYPT" description="No encryption module prese
nt" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="NO_ENCRYPT" />
        </Command>
      </Action>
    </State>
    <State shortName="MSMTCH" longName="MISMATCH" description="Mismatch between user selec
ted secure transmit mode and actual fixed/strapped tx mode" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="MISMATCH" />
        </Command>
```

```
      </Action>
    </State>
    <State shortName="UNKWN" longName="UNKNOWN" description="Secure/Clear Transmit mode is
 in an unknown state" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="UNKNOWN" />
        </Command>
      </Action>
    </State>
    <State shortName="UNSPRT" longName="UNSUPPORTED" description="Encryption is not suppor
ted" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetSecureTxMode value="UNSUPPORTED" />
        </Command>
      </Action>
    </State>
</Stateful>
    <Stateful shortName="EMG" longName="Emergency" description="Enable/Disable Emergency M
ode" presentation="multiple">
    <State shortName="ON" longName="ON" description="Emergency mode is on" user_selectable
="true">
      <Action type="pressed">
        <Command>
          <SetEmergencyMode value="ON" />
        </Command>
      </Action>
    </State>
    <State shortName="OFF" longName="OFF" description="Emergency mode is off" user_selecta
ble="true">
      <Action type="pressed">
        <Command>
          <SetEmergencyMode value="OFF" />
        </Command>
      </Action>
    </State>
    <State shortName="UNKWN" longName="UNKNOWN" description="Emergency mode is in an unkno
wn state" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetEmergencyMode value="UNKNOWN" />
        </Command>
      </Action>
    </State>
    <State shortName="UNSPRT" longName="UNSUPPORTED" description="Emergency mode is not su
pported" user_selectable="false">
      <Action type="pressed">
        <Command>
          <SetEmergencyMode value="UNSUPPORTED" />
        </Command>
      </Action>
    </State>
</Stateful>
</ControlFunctions>
```

The <SupplementaryServices> element represent features that require user interaction and are directed to one or more remote units. They have their own user interface on the dispatch console for processing the service, where the dispatcher selects from a list of units or enters a unit ID.

```
<SupplementaryServices>
  <SupplementaryService shortName="ALRT" longName="Call Alert" />
  <SupplementaryService shortName="CALL" longName="Individual Call" />
  <SupplementaryService shortName="MSSG" longName="Status Message" />
```

```
  <SupplementaryService shortName="QERY" longName="Status Query" />
  <SupplementaryService shortName="RMON" longName="Radio Unit Monitor" />
  <SupplementaryService shortName="CHEK" longName="Radio Check" />
  <SupplementaryService shortName="DTCH" longName="Radio Detach" />
  <SupplementaryService shortName="INHB" longName="Radio Inhibit" />
  <SupplementaryService shortName="UNHB" longName="Radio Uninhibit" />
</SupplementaryServices>
```

The <StatusMessages> element is a list of pre-defined short messages intended to be used on a system capable of sending such messages. These are not considered Short Message Service (SMS) where a text message is sent. In this case, the system sends a numeric value that represents a text message. All radios in the system must be provisioned with the same set of IDs for the respective messages. The example below uses 16-bit hexadecimal values for the id attributes, and "longName" values (per the P25 short message specification) for the alias attributes.

```
<StatusMessages>
<StatusMessage id="01" alias="Request To Talk" />
<StatusMessage id="02" alias="Request To Patch" />
<StatusMessage id="03" alias="NCIC Check" />
<StatusMessage id="04" alias="License Check" />
</StatusMessages>
```

The <StatusUpdates> element is a list of pre-defined update messages intended to be used on a system capable of sending such messages. It is intended to represent the status of a radio or radio user. In this case, the system sends a numeric value that represents a specific status. The example below uses two 8-bit hexadecimal values for the id attributes, and "longName" values (per the P25 short message specification) for the alias attributes.

```
<StatusUpdates>
<StatusUpdate id="10" alias="On Duty" />
<StatusUpdate id="20" alias="Off Duty" />
<StatusUpdate id="30" alias="Lunch Break" />
<StatusUpdate id="40" alias="Do No Disturb" />
</StatusUpdates>
```

Caveats for IDC Operation

For Serial Control the CTRL button opens a browser-based UI to control radios.

If you are using a tone controlled radio, be aware of the following IDC operation caveats when configuring tone sequences in radio and tone descriptor files:

- For tone control sequences (channel selectors and radio control functions), Cisco IPICS supports only RFC 2833 tones (DTMF entries are not supported).
- You cannot enter more than six consecutive RFC 2833 tones in a tone control sequence.

  The following example shows the format of an RFC 2833 tone:

  ```
  <Rfc2833Tone db="0" duration="40" frequency="100" />
  A tone sequence is a sequence of tones, as shown in the following example:
  <Rfc2833Tone db="0" duration="40" frequency="100" />
  <Rfc2833Tone db="0" duration="40" frequency="200" />
  <Rfc2833Tone db="0" duration="40" frequency="300" />
  <Rfc2833Tone db="0" duration="40" frequency="400" />
  <Rfc2833Tone db="0" duration="40" frequency="500" />
  <Rfc2833Tone db="0" duration="40" frequency="600" />
  ```

Note The tone sequence in the previous example does not display more than six consecutive RFC 2833 tones (“100” through “600”).

- For tone signaling, Cisco IPICS supports both RFC 2833 tone and RFC 2833 event (DTMF) commands.

  You can enter more than six consecutive RFC 2833 tones only if the sixth tone event is separated by a pause entry (such as one ms) or a DTMF digit entry (such as digit one for 200 ms).

Note When you enter DTMF digits, be sure to configure a delay between the digits so that DTMF gets detected, as required by the local specifications. U.S. specifications require a delay of 40 ms.

There is no limit to the number of DTMF entries that are allowed in a signaling tone sequence.

Note You can define a pause by a tone with a frequency of zero, as in the following example:

<Rfc2833Tone db=”0” frequency=”0” duration=“40” />

where:

db=“0” frequency=“0” represents the pause entry.

- Because tone sequences, whether in signaling or control sequences, are grouped into RFC 2198 packets, a maximum duration gets imposed for some of the tones. For example, if ‘n’ is the total number of tones in the tone sequence, where max(n) = 6, the maximum duration for the first (n–1) tones cannot be more than two seconds.
- The maximum duration for any RFC 2833 tone or event is 8 seconds.
- Because preamble tones that are longer than one second compromise the beginning of talk spurts, there is a maximum possible voice delay of one second.

For some examples of valid and invalid descriptor file entries, see the “Examples of descriptor .xml files” section on page 9-24.

Understanding the Descriptors Window

The Descriptors window lists information about each of the radio and tone and serial descriptor files that you have added in Cisco IPICS.

This window also enables you to perform several radio and tone descriptor management functions. To display the Descriptors window, navigate to **Configuration > Descriptors** in the Administration Console.

Table 9-4 describes the items in the Descriptors window.

Table 9-4 Fields in the Descriptors Window

Field	Description	Reference
Name field	This field indicates the name of the radio type that Cisco IPICS supports.	See the "Tone Radio Descriptors" section on page 9-22, the "Tone Descriptors" section on page 9-21, and the "Adding Descriptors" section on page 9-36.
File Name field	This field indicates the name of the radio/tone descriptor .xml file.	
Type field	This field indicates the type of descriptor. **Note** When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file.	
File Size (KB) field	This field indicates the size of the descriptor file.	
Last Update field	This field indicates the date and time of the last modified descriptor file.	
Add button	Click this button to add new descriptor files.	See the "Adding Descriptors" section on page 9-36.
Update button	Click this button to update existing descriptor files.	See the "Updating Radio and Tone Descriptors" section on page 9-37.
Delete button	Click this button to delete descriptor files from Cisco IPICS.	See the "Deleting Radio and Tone Descriptors" section on page 9-38.
Display Controls		
Rows per page drop-down list	Specifies the number of rows of descriptors that are included in a descriptors list page.	See the "Navigating Item Lists" section on page 1-13.
Page field	Displays descriptors on a specific page.	
|< (First page) button	Displays the first page of the descriptors list.	
< (Previous page) button	Displays the previous page of the descriptors list.	
> (Next page) button	Displays the next page of the descriptors list.	
>| (Last page) button	Displays the last page of the descriptors list.	

Adding Descriptors

You can add descriptors to Cisco IPICS in the Configuration > Descriptors window in the Administration Console.

For detailed information about descriptors, see the "Tone Radio Descriptors" section on page 9-22 and "Tone Descriptors" section on page 9-21.

For examples of valid and invalid descriptor file .xml entries, see the "Examples of descriptor .xml files" section on page 9-24.

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file.

To add a new descriptor file, perform the following procedure:

Procedure

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

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

The New Descriptor window displays.

Step 3 From the Descriptor Type drop-down list, choose one of the following options:

- **Tone Radio**—Choose this option to add a descriptor file for a tone control radio.
- **Serial Radio**—Choose this option to add a descriptor file for a serial control radio.
- **Tones**—Choose this option to add a tone descriptor file.
- **ISSI Gateway**—Choose this option to add an ISSI Gateway descriptor file.

Step 4 To locate the descriptor file that you want to add, click **Browse**.

Step 5 In the Choose File window, navigate to the location of the descriptor file that you want to add and highlight the file.

Step 6 Click **Open**.

The File to Upload field gets populated with the descriptor file that you selected.

Step 7 Click **Save**.

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

Note If you need to modify an existing descriptor file, follow the steps in the "Updating Radio and Tone Descriptors" section on page 9-37.

Updating Radio and Tone Descriptors

You can update an existing descriptor file in Cisco IPICS in the Descriptors window.

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file.

When you update a radio descriptor to add new channel selectors or control functions, all of the radio instances that are currently using this descriptor get updated accordingly. If there are any IDC users using these radio instances, their IDC clients get updated also.

If you update a tone descriptor, the system checks the newly uploaded file for missing commands that may be in use by the radio descriptor file.

Note If you upload a new file that is missing a command, which is in use by the radio descriptor, the system does not allow the update.

For more detailed information about radio and tone descriptors, see the "Tone Radio Descriptors" section on page 9-22 and the "Tone Descriptors" section on page 9-21.

To update radio and tone descriptors, perform the following procedure:

Procedure

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

Step 2 Click the radio button next to the descriptor that you want to update.

Step 3 Click **Update**.

Step 4 Click the **Browse** button, that is next to the File to Upload field.

Step 5 In the Choose File window, navigate to the location of the descriptor file that you want to use to update and highlight the file.

Step 6 Click **Open**.

The File to Upload field gets populated with the descriptor file that you selected.

Step 7 Click **Save**.

If you do not want to update the descriptor, click **Cancel**.

Note If there are multiple radio descriptor files for the same type of radio, the Cisco IPICS server uses the latest uploaded file. This feature allows you to update the radio descriptor file for a given radio type by uploading a new descriptor file.

Deleting Radio and Tone Descriptors

You can delete radio and tone descriptor files from Cisco IPICS.

You cannot delete radio descriptor files that are being used by radios.

For more detailed information about radio and tone descriptors, see the "Tone Radio Descriptors" section on page 9-22 and the "Tone Descriptors" section on page 9-21.

To delete a radio, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each radio 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 radio(s), click **Cancel**.

CHAPTER 10

Configuring and Managing Cisco IPICS High Availability

Cisco IPICS provides the option of configuring a secondary hot standby server to provide high availability with no single point of failure. If a primary server fails, the secondary server automatically takes over service without communication interruption. This chapter describes the high availability function in detail It includes these topics:

- Overview, page 10-1
- Configuring Cisco IPICS Servers for HA, page 10-3
- Unconfiguring HA, page 10-6
- HA Affect on the IDC Connections, page 10-6
- HA Affect On Connected Devices, page 10-8
- Synchronizing the Server Time on HA Servers, page 10-8
- Performing a Manual Failover, page 10-9
- Resolving a Split Brain Scenario, page 10-10
- Reestablishing HA Configuration After Prolonged Server Downtime, page 10-14

Overview

The Cisco IPICS high availability (HA) feature allows two Cisco IPICS servers to be configured as a redundant pair: one *active server* to control the system users and connected devices, and a second *standby server* ready to assume control if the active server encounters a problem or goes off-line.

Defining the Active and Standby Servers

During initial configuration, the primary and standby server role is determined by the type of license file installed on the server.

- Install the *IPICS Base server* and *Policy Engine Base* license on the server designated as the primary server. This server will assume the active role.
- Install only the *High Availability* license on the server designated as the secondary server. This server will assume the standby role.

Once the server pair is operating in HA mode, the *active* and *standby* roles can switch between the servers. When a user logs into the Cisco IPICS Administration Console, they are automatically logged in to whichever server is the current active server.

Tip See the "Managing Your Licenses" section in *Cisco IP Interoperability and Collaboration System Server Installation Guide* for more information.

Remote Server Locations Using Secure Communication

The redundant Cisco IPICS servers can be located at remote locations, so that a catastrophic event in one location does not affect the other server. Secure communication is established during initial configuration, when the severs perform a one-time exchange of SSH/TLS certificates and public keys. See the "Configuring Cisco IPICS Servers for HA" section on page 10-3 for more information.

Server Failover Due to Local Critical Process Failure

If a local critical process (such as tomcat) fails, the active server instructs the standby server to assume the active role. This process can take several minutes and assumes that the standby server is ready and reachable.

Server Failover Due to Lost Heartbeat Message

The redundant servers also maintain communication by exchanging regular *heartbeat* messages. If the active server does not respond to the messages after a configured time, the standby server assumes the active role. This loss of heartbeat communication can be caused by a loss of network connectivity or a hardware failure.

By default, if the primary and standby servers exchange heartbeat messages every 15 seconds. If 5 heartbeat messages fail (for a total of 75 seconds), the standby server assumes the active role.

See the "Configuring Cisco IPICS Servers for HA" section on page 10-3 for information about modifying the default heartbeat time, if necessary.

Affect of Failover on IDCs and Connected Devices

If a failover occurs, IDC connections may be temporarily lost while the transfer is completed. The consoles continue to operate in off-line mode, however, and are automatically reconnected to the new server with no user interaction. The console remains connected even if the original server comes back online and assumes the standby role. See the "HA Affect on the IDC Connections" section on page 10-6 for more information.

Some connected devices such as iPhones also remain connected during a failover. Other devices, such as Cisco Unified IP Phones or standard telephones, must manually reconnect. See the "HA Affect On Connected Devices" section on page 10-8 for more information.

Manually Failover and Recovering from a Split Brain Scenario

You can manually force the active server to failover to the standby server. See the "Performing a Manual Failover" section on page 10-9 for more information.

If communication is lost between the primary and secondary servers, both servers may temporarily assume the active role. This situation is known as a *split brain scenario*. After communication is reestablished, you must manually transition the secondary server to the standby role. For more instructions, see the "Resolving a Split Brain Scenario" section on page 10-10.

Configuring Cisco IPICS Servers for HA

To configure Cisco IPICS HA, you must install and configure a primary server and a secondary server. These servers can be at different locations because they communicate using a secure, encrypted connection.

Before configuring HA, you must configure both servers with an IP address, an NTP server, and the correct license for each server, as described below.

Before You Begin

Before configuring redundant Cisco IPICS servers, do the following:

- Obtain the Network Time Protocol (NTP) server addresses that will be used to synchronize the Cisco IPICS servers. See the "Synchronizing the Server Time on HA Servers" section on page 10-8 for more information.
- Obtain the IP addresses for the primary and the secondary servers
- Obtain the **ipicsadmin** user passwords for the secondary server
- Obtain the *IPICS Base server* and *Policy Engine Base* licenses for the Primary server, and the *High Availability* license for the Secondary server. See the "Managing Your Licenses" section in *Cisco IP Interoperability and Collaboration System Server Installation Guide*.
- Verify that the installed HA server pair matches one of the supported configurations that is defined in *Cisco IPICS Compatibility Matrix*.
- Verify that any existing data on either HA server should be merged, or perform a clean install of the IPICS software
- Perform a clean install of the IPICS server software, if necessary. Any data on either server will be merged when the servers are configured for HA.
  - Data from a server that was previously configured as either primary or secondary in a different HA pair will be merged to the new HA configuration.
  - Existing data will be merged even if the server was not previously configured for HA.
  - If you do not want the existing data from a server to be merged when creating an HA pair, you must perform a clean install of the IPICS server software to remove that data. See the *Cisco IPICS Server Installation and Upgrade Guide* for more information.

To configure redundant Cisco IPICS servers for HA, perform the following procedure:

Procedure

Step 1 Physically install the primary and secondary servers.

See *Cisco IP Interoperability and Collaboration System Server Installation Guide* for instructions.

Step 2 (Optional) Perform a clean install of the IPICS server software, if necessary, to remove any existing data from the primary or secondary server.

Note Any data on either server will be merged when the servers are configured for HA. Perform a clean install of the server software to delete any existing data. See the *Cisco IPICS Server Installation and Upgrade Guide* for instructions.

Step 3 Configure an IP address on each server.

See *Cisco IP Interoperability and Collaboration System Server Installation Guide* for instructions.

Step 4 Configure both the primary and secondary servers with an NTP server to synchronize the system time.

Note HA servers use the internal time setting to exchange HA heartbeats and data. HA configuration fails if NTP is not configured on both servers.

a. Enter the following command on both servers to enable NTP:

```
ntpsetup -s enable <ntp-server> <backup-ntp-server>
```

For example:

```
ntpsetup -s enable ntp-sj1.cisco.com ntp-sj2.cisco.com
```

b. Enter the following command on both servers to verify the system settings:

```
ntpsetup -c
```

c. Enter the following command on both servers to restart the node manager:

```
service ipics_nm restart
```

Step 5 Install the following software licenses on the primary and secondary servers.

a. On the primary server, install the *IPICS Base server* and *Policy Engine Base* licenses. The primary server does not require the HA license (the HA license should never be installed on the primary server).

b. On the secondary server, install the *High Availability* license only. The secondary server does not require any other licenses.

See the "Managing Your Licenses" section in *Cisco IP Interoperability and Collaboration System Server Installation Guide*.

Step 6 Log in to the Cisco IPICS Administration Console for the primary server.

See the "Accessing the Administration Console" section on page 1-11 for instructions.

Step 7 From the Cisco IPICS Administration Console, navigate to the **Configuration > High Availability > Security** tab.

If HA partner trust has not yet been configured, the window shows that the **Server Status** is `Not Trusted`.

a. In the IP Address, field, enter the **IP address** of the HA Partner server.

   The HA Partner is the secondary Cisco IPICS server. The User Name field displays the user name of the Partner Server linux administrator (ipicsadmin).

b. In the User Password field, enter the password of the ipicsadmin user.

c. Click **Save** to save the HA Partner IP address and establish trust between the redundant servers.

   To establish trust, the servers exchange public keys and SSL certificates.

   If successful, the Server Status changes to Trusted and the HA Configuration tab appears.

Step 8 Click the HA Configuration tab:

Note

- The HA Configuration window appears only after high availability mode is enabled, as described in Step 7.
- The IP addresses for the primary and secondary server are read-only. The primary server IP address is the Cisco IPICS server to which you are currently logged in. The secondary server IP address is the address you entered to enable high availability mode in Step 7.
- If high availability mode is enabled, but the HA is not yet configured, the Standby Server Status is Not Ready.

a. In the Heartbeat Port field, enter the IP port number for HA heartbeat traffic. The default value is 3444.

b. In the Heartbeat Interval (seconds) field, enter a number between 5 and 600 to define the number of seconds between heartbeats.

   Each heartbeat checks to confirm the status and availability of the partner server. The default value is 15 seconds.

c. In the Missed Heartbeat Count field, enter number from 5 to 30 to define the number of missed heartbeats before the active role is transitioned to the secondary server.

   The default is five missed heartbeats (75 seconds if the Heartbeat interval is 15 seconds). The transition process takes approximately 150 to 180 seconds.

d. Click **Update** to save the changes.

Step 9 Click **Configure** to save the changes and activate high availability (server redundancy).

After a brief delay, you are automatically logged out of the IPICS system until HA configuration operations are complete.

Step 10 Verify that the **Standby Server Status** changes to `Ready`.

a. Log in to the Cisco IPICS Administration Console.

b. Navigate to the **Configuration > High Availability** window.

c. Click the **HA Configuration** tab.

d. Verify that the **Standby Server Status** is `Ready`.

Unconfiguring HA

Certain situations require you to temporarily unconfigure HA. These situations include restoring data from a Cisco IPICS database backup or generating SSL certificates for an IPICS server.

To unconfigure Cisco IPICS servers for HA, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console on the active server, navigate to the **Configuration > High Availability** window.

Step 2 Click the **HA Configuration** tab.

Step 3 Click the **Unconfigure** button**.**

Step 4 Click **Logout** to log out from the active server.

Step 5 Wait a few minutes for the active server to reconfigure.

Step 6 (Optional) Delete the security trust certificates used with the partner server:

Note Delete the HA security certificates only if you need to regenerate or replace the SSL certificates. The default IPICS server SSL certificates expire after three years and must be replaced. See Appendix E, "Generating SSL Certificates" for more information.

a. Log in again to the primary server.

b. Navigate to the **HA Security** window (expand the Configuration drawer and choose **High Availability > HA Security**).

c. Enter the password for the partner server in the password field to enable the **Delete** button.

A valid password is required to guarantee that the trust certificates are removed from the partner server.

d. Click **Delete** to delete the trust certificates used with the partner server.

HA Affect on the IDC Connections

When a user logs in to an IDC, the Log in selector displays all active and standby servers. To connect, users must select the active server. If the standby server is selected, the connection is denied and automatically redirected to the active server.

Note The role of active and standby can switch between the available servers. Users must always log in to the active server. The same user name and password is used for either server.

A failover occurs when the active server goes down or loses connectivity with the standby server. In this case, IDCs are automatically transferred to a standby server and service continues as normal. During the short time that the IDC is establishing a connection with the a standby server, the console operates in offline mode, using the last configuration provided by the previously active server. The console also

displays a message informing the user of the offline status. No action is required by the console user during this offline period. A new message appears when the console automatically reconnects to the new server.

After a failover, consoles remain connected to the new active server even if the original server is brought back online. The restored server becomes the new standby, ready take to control if a failover occurs. If the console user logs out, the user can log back in to the active server (as displayed in the log in server selector).

If a user attempts to log in to the standby server, the console is automatically redirected to the active server.

Note

- Because there is a short pause in Cisco IPICS server operations during a failover, it is possible that not all data becomes synchronized from the active server to the standby. If this situation occurs, some configurations that were entered immediately before the failover could be lost. See the following example for more information.
- Photographs and videos that were uploaded to an incident shortly before a failover may need to be uploaded again because these files can be large and files are replicated at a lower priority than system data.

Example

In this example, a Cisco IPICS system is configured with redundant servers, as described in the "Configuring Cisco IPICS Servers for HA" section on page 10-3. The system has been running for 10 days with no problems. When dispatcher Dan starts his shift, he logs in to his console by selecting the active server from the login dialog. At lunch time, a localized earthquake occurs and the active server falls out of the rack. The console used by Dan detects the broken link to the server and automatically connects to the standby server, a process that takes about 10 seconds. Although Dan notices that the console is disconnected from all servers, the console remains connected to media resources and Dan is still able to notify Adam (the administrator) about the localized earthquake by using a console channel push-to-talk (PTT) feature. 10 seconds later, the console that is used by Dan automatically connects to the standby server. There is no visible change to the console.

45 minutes after the server failover, Adam the administrator remounts the original server involved in the earthquake and restores the server network connection. However, the console that is used by dispatcher Dan continues to connect to the new active server, and the restored server becomes the new standby.

The next day, when Dan returns to work, he logs in to the console and connects to the new active server, which is identified as the active server in the login server selector.

One issue did occur during this process. Before the earthquake, the channel Fire was assigned to user Ursula. Ursula saw the new channel because the console received an update from the active server. But before the channel assignment was propagated to the standby server, the active server was knocked off the network by the earthquake. Because the new Fire channel was not propagated to the standby before the failover occurred, the Fire channel does not appear on the new active server and must be reconfigured.

The next day, Amy attempts to log in to the console. Because she was not online at the time of the failover, her console still shows the original active server in the login server selector. When she attempts to connect to this server, which is now the standby, the application pauses for approximately 5 seconds. When the connection fails, the console is automatically redirected to the other server. The console connects to the new active server and the console is updated to reflect the new server status.

HA Affect On Connected Devices

If a Cisco IPICS server failover occurs, connected devices are affected in the following ways:

- Mobile client—Mobile clients automatically switch to the new active server.
- Cisco Unified IP Phone—The Cisco Unified IP Phone administrator must configure a Cisco Unified Phone Service for both the primary and secondary IPICS server. This configuration allows either the user or the administrator to subscribe to the services for both servers. (For more information, see the "Cisco Unified Phone Services" section in *Cisco Unified Communications Manager System Guide*.)

  If you are using a Cisco Unified IP Phone and the active server goes down, you must manually reconnect to the active IPICS server. Open the **Services** menu, select the new active Cisco IPICS server, and log in again.
- Standard telephone—Standard dial-in phone calls are dropped, but users can call back in to the system after a short delay.

Note

- Cisco IPICS does not automatically call back dial-out users participating in a VTG when a failover occurs.
- Any running external notifications or policies are restarted after a failover. Duplicate notifications may be sent to users.

Synchronizing the Server Time on HA Servers

Before servers are configured for HA, you must configure the internal time on each server using the Network Time Protocol (NTP). HA servers use the internal time setting to exchange HA heartbeats and data. HA configuration fails if NTP is not configured on both servers.

In addition, the time setting should not be manually changed on either HA server. If the time settings are more than 30 seconds apart, the servers can lose HA communication and enter a *split brain* scenario. See the "Resolving a Split Brain Scenario" section on page 10-10 for more information.

To synchronize the time settings on the primary or secondary servers, perform the following procedure:

Procedure

Step 1 Configure both the primary and secondary servers with an NTP server:

The NTP server sets the system time and ensures the active and standby server times are synchronized.

a. Enter the following command on both servers to enable NTP:

```
ntpsetup -s enable <ntp-server> <backup-ntp-server>
```

For example:

```
ntpsetup -s enable ntp-sj1.cisco.com ntp-sj2.cisco.com
```

b. Enter the following command on both servers to verify the system settings:

```
ntpsetup -c
```

Note If the same files or records exist on both servers but have different timestamps, only the file or record with the most recent timestamp is retained. The older data is overwritten.

Step 2 Enter the following command on both servers to restart the node manager:

```
service ipics_nm restart
```

Step 3 If both servers are in *active* state due to a time misconfiguration, you must force the secondary server back into standby mode. See the "Resolving a Split Brain Scenario" section on page 10-10 for more information.

Performing a Manual Failover

To manually cause the currently active server and standby servers to reverse roles, perform the following procedure. The active role will be transferred to the standby server. This procedure is necessary if you want to take the active server offline, and ensures a stable failover between servers.

Before You Begin

- Either the primary or secondary server can be in the Active state. Use the following procedure to transfer the active role to the server currently in the Standby state.
- To perform a manual failover, HA must be configured and the Standby Server Status must be Ready. See the "Configuring Cisco IPICS Servers for HA" section on page 10-3 for more information.
- Before you begin, review the affect of a failover on consoles and connected devices. See the "HA Affect on the IDC Connections" section on page 10-6 and the "HA Affect On Connected Devices" section on page 10-8.

Procedure

Step 1 Log in to the Cisco IPICS Administration Console.

See the "Accessing the Administration Console" section on page 1-11 for instructions.

Step 2 Navigate to the **Configuration > High Availability** window.

Step 3 Click the **HA Configuration** tab.

Note If the HA Configuration tab is not available, the high availability mode is not enabled. Complete the instructions in the "Configuring Cisco IPICS Servers for HA" section on page 10-3.

- The Standby Server Status is Ready.
- The server in standby mode should assume the active role.

If the Standby Server Status is `Not Ready`, the high availability mode is enabled, but not configured. Complete Step 8 in the "Configuring Cisco IPICS Servers for HA" section on page 10-3.

Step 4 Click the **Failover Now** button to transfer the active state to the standby server.

The standby server becomes the new active server and the active server becomes the standby server.

Resolving a Split Brain Scenario

A *split brain scenario* occurs when the communication between the primary and secondary servers is lost, causing both servers to independently assume the active server role. Although this situation allows consoles and devices to connect with each server for continued operation, the data stored on each server is not synchronized with the other server. Over time, the data differences between the servers becomes greater.

When the communication link between the servers is reestablished, both servers remain in active state. This situation is known as a split brain scenario. To resolve this misconfiguration, one server must be returned to the standby state, and the data on the two servers must be reconciled.

Note

- Although either server can be returned to standby state, Cisco recommends that you keep the primary server in active state and returning the secondary server to standby, as described in the following instructions.
- A *split brain* scenario can occur if the system time on the servers is more than 30 seconds apart. See the "Synchronizing the Server Time on HA Servers" section on page 10-8 for information about synchronizing the server time using NTP.

Overview of Reconciliation Methods

The following methods are used to reconcile server data and restore server redundancy. Review the following descriptions to decide which method to use:

- Method 1: Force the Secondary Server into Standby State, page 10-10—Use this method if the servers have been in split brain mode for a short time (less than 5 days). This process entails forcing the secondary server into standby state, and then using Linux commands to synchronize the databases and file systems of the two servers. This method automatically returns the servers to high availability operation, and users can continue to access the primary server.
- Method 2: Reconfigure High Availability, page 10-12—Use this method if the servers have been in a split brain mode for 5 or more days, or if you are concerned that forcing the secondary into standby state (Method 1) might cause data loss. This method entails bringing down the secondary server, unconfiguring high availability on the primary server, and then manually reconciling the files that exist on both servers. After complete, you must reconfigure HA on both servers to restore server redundancy.
- Method 3: Workaround, page 10-13—Use this method only if Method 1 and Method 2 do not work. This method forces the primary to be the only active server but does not reconcile the data.

Method 1: Force the Secondary Server into Standby State

Use Method 1 to manually force the secondary server into standby state. After the secondary server is in standby state, use an SSH client to resynchronize the server databases and file systems.

Resynchronizing the server databases causes the following to occur:

- Records that exist on the primary server but not the secondary server are replicated from the primary server to the secondary server
- Records that exist on the secondary server but not on the primary server are replicated from the secondary server to the primary server

- If a record exists on both servers, the record on the primary server is considered the *master*, and the corresponding record on the secondary server is replaced

Resynchronizing the file system files causes the following to occur:

- Files that exist on the primary server but not on the secondary server are copied from the primary server to the secondary server.
- Files that exist on the secondary server but not on the primary server are deleted.
- If the same file exists on both servers, the file with the more recent timestamp (per coordinated universal time, or UTC) is retained and copied to the other HA server. The old version of the file is overwritten. If you prefer to merge the files instead of deleting the older file, ask your Linux systems administrator for information about reconciling file differences using **scp** or **sftp**.

This process automatically returns the servers to high availability operation, and users can continue to access the primary server.

Procedure

Step 1 (Optional) View the files and folders that are replicated during synchronization.

View the file at the following location:

```
/opt/cisco/ipics/conf/fileDirectory
```

This file contains the local source directories and the remote destination directories:

```
/idspri/backup/                                                  /idspri/backup
/opt/cisco/ipics/tomcat/current/webapps/ipics_files/
/opt/cisco/ipics/tomcat/current/webapps/ipics_files
/opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs/
/opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs
/idspri/archive/                                                 /idspri/archive
/idspri/db_table_archive/
/idspri/db_table_archive
/opt/cisco/ipics/tomcat/current/webapps/documents/
/opt/cisco/ipics/tomcat/current/webapps/documents
```

Note This file is used to determine what will be replicated. Do not alter the file in any way.

Step 2 Force the secondary server into standby state:

a. Determine which server was configured as the secondary server.

   See the "Configuring Cisco IPICS Servers for HA" section on page 10-3.

b. Log in to the Cisco IPICS Administration Console for the secondary server.

   See the "Accessing the Administration Console" section on page 1-11 for instructions.

c. Navigate to the **Configuration > High Availabily** window.

d. Click the HA Configuration tab:

e. Verify that the Standby Server Status is Not Ready.

f. Click the **Go Standby** button at the bottom of the window.

   The **Go Standby** button is enabled only when both servers are in active mode, and communication between them has been reestablished.

g. Click **OK** when the confirmation message appears.

The secondary server logs out all current user sessions.

h. Wait for the split brain remediation process to complete.

The remediation process reestablishes the HA server pair with an active and standby server configuration.

When the process is complete, any login attempts to the secondary server are redirected to the primary server. See the "HA Affect on the IDC Connections" section on page 10-6 for more information.

Step 3 Resynchronize the database between the primary and secondary server:

a. Use an SSH client to log in to either the primary or secondary HA server with the user name **Informix**. The command will work the same on either server.

b. Start the database synchronization process by entering the following command:

```
server> /opt/cisco/ipics/database/bin/ipicsedr_control_repl REPAIR
```

c. Monitor the database synchronization process by entering the following command:

```
server> /sbin/service ipics ha-status
```

Note The database replication repair processes are concurrent and run in background. The status of the different processes are listed under "Pending Database Replication Synchronization Processes". The repair process is completed when the section has no outstanding entries.

Step 4 Resynchronize the file system files:

a. Use an SSH client to log in to the primary server with the user name **ipicsadmin**.

Note The following commands must be run on the primary server.

b. Start the file system synchronization process by entering the following command:

```
server> /opt/cisco/ipics/database/bin/ipicsrsync run ipicsadmin
```

c. Monitor the synchronization process by entering the following command:

```
server> /opt/cisco/ipics/database/logs/rsync.log
```

Step 5 Log in to the Cisco IPICS Administration Console for the primary server and verify that the primary server is in active state and the secondary server is in standby state.

Method 2: Reconfigure High Availability

Use Method 2 to manually inspect the data integrity between the two servers and reconcile the data, if necessary. For more information, see the "Overview of Reconciliation Methods" section on page 10-10.

Procedure

Step 1 Log in to the secondary server using SSH.

Step 2 Enter the following commands to stop access to the secondary server:

- `server> /sbin/service ipics stop`
- `server> /sbin/service ipics_nm stop`

Step 3 Take these actions to unconfigure HA on the primary server:

a. Log in to the Cisco IPICS Administration Console for the primary server.

See the "Accessing the Administration Console" section on page 1-11 for instructions.

b. Expand the Configuration drawer and click **High Availability**.

c. Click the **HA Configuration** tab.

d. Click the **Unconfigure** button**.**

e. Click **Logout** to logout from the active server.

f. Wait a few minutes for the primary server to reconfigure.

g. Log in again to the primary server.

h. Navigate again to the **HA Security** screen (expand the Configuration drawer, click **High Availability**, and then click the **HA Security** tab.

i. Click **Delete** in the **HA Security** screen to delete the HA security certificates and disable HA mode.

Step 4 Inspect the following directories in both servers to verify that files in both servers are the same:

- /idspri/backup
- /opt/cisco/ipics/tomcat/current/webapps/ipics_files
- /opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs
- /idspri/archive
- /idspri/db_table_archive
- /opt/cisco/ipics/tomcat/current/webapps/documents

Note The /documents directory contains all uploaded iPhone and IDC content, and is considered critical data.

Step 5 If the files are not the same, move the correct files to the primary server directories

Step 6 Reconfigure high availability on the primary and secondary servers.

See the "Configuring Cisco IPICS Servers for HA" section on page 10-3.

Note If the role of the original primary server is changed to the secondary role, new HA licenses are required.

Method 3: Workaround

If neither Method 1 nor Method 2 corrects the split brain scenario, use the following workaround to force the primary server to be the only server in active state.

Procedure

Step 1 Shut down the secondary server:

a. Log in to the secondary server using SSH.

b. Shut down the server using the following command:

```
shutdown -h now
```

c. Power off the machine

Step 2 Stop and restart all services on the primary server:

a. Log in to the primary server using SSH

b. Restart the IPICS services using the following commands:

```
service ipics stop-all
service ipics start-all
```

Step 3 (Optional) If the `stop-all` and `start-all` commands are not available on the primary server, enter the following alternative commands:

```
service ipics_nm stop
service ipics stop
service ipics start
```

(wait 10 seconds)

```
service ipics_nm start
```

Step 4 Power up the secondary server.

Reestablishing HA Configuration After Prolonged Server Downtime

When one of the servers in an HA server pair goes down for an extended length of time, the remaining active server saves database updates in a transaction log. Under normal operation, the database updates are restored to the down HA server when it comes back online.

If the second server remains offline for an extended time, however, and the system experiences heavy activity, the database log may run out of space. If the database log reaches 100 percent capacity, a database replication block state (DDRBLOCK state) can occur, blocking all database updates until cleared.

To prevent this situation, the Cisco IPICS system automatically unconfigures HA if usage exceeds 90 percent of capacity. An error message is also issued when capacity reaches 75 percent of capacity and again at 90 percent of capacity (when HA is also unconfigured.

If HA is unconfigured following extended downtime for one of the servers, you must reconfigure HA on the active server, as described in the "Configuring Cisco IPICS Servers for HA" section on page 10-3.

CHAPTER 11

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 11-1
- Backing up the Cisco IPICS Server Database, page 11-2
- Restoring Data from a Database Backup, page 11-9
- Downloading and Viewing the Backup and Restore Logs, page 11-14
- Troubleshooting Cisco IPICS Backup and Restore Procedures, page 11-15

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 11-6.

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 11-9.

A backup set contains all data in the Cisco IPICS server database, including radio descriptor files and IDC alert tones.

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 11-9.

Caution Database restores should only be done when there are no other users logging in to the system; otherwise, they may see errors or other strange behavior.

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.

Note For optimum performance, Cisco recommends that you back up your database during periods of low activity or other off-peak hours. If you perform a backup during periods of high activity, the length of time that it takes to complete this operation can be significantly increased.

This section includes information about backing up the database and includes the following topics:

- Managing Database Backups from the Database Management Window, page 11-2
- Performing a Manual Database Backup, page 11-3
- Understanding Naming Conventions for Backup Directories, page 11-6
- Changing the Default Settings for a Scheduled Database Backup, page 11-6
- Guidelines for Choosing a Destination for Database Backups, page 11-8
- Caveats for Remote Host Database Backups, page 11-9

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 11-3 for more information about backing up your database.
- Restore From Backup—From this tab, you can restore your database backup. See the "Restoring Data from a Database Backup" section on page 11-9 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 11-6 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 11-14 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 11-6 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/cron** directory. You can remove the **/cron** subdirectory in the field to place your files in the **/idspri/backup** directory. However, 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.

Tip 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 11-16 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:

- 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 11-9.

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 window 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 1-13.

If the backup operation was successful, you see a Status Text of **Available**.

Table 11-1 describes the fields in the Backup Log pane.

Table 11-1 Field Descriptions in the Backup Log Pane

Field	Description
ID	This field represents the internal ID of the database backup. Cisco IPICS assigns 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 "Understanding Naming Conventions for Backup Directories" section on page 11-6.
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**.
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 displays 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 > Log** 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 indicate that the script completed but they do not necessarily indicate that 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 11-15.

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 Cisco IPICS performed the database backup (for example, IDSB_2007-07-04_17-13-55).

Changing the Default Settings for a Scheduled Database Backup

Cisco IPICS is preconfigured with default settings for database backups. Table 11-2 shows the default settings for scheduled database backups:

Table 11-2 Default Settings for Scheduled Database Backups

Setting	Value
Frequency	Daily
Time of day	23:59 (11:59 p.m.)

Table 11-2 Default Settings for Scheduled Database Backups (continued)

Setting	Value
Destination directory	The Cisco IPICS server **/idspri/backup/cron** directory. Cisco IPICS displays the **/idspri/backup** directory as part of the Local Directory option, and prepopulates the **/cron** subdirectory in the Local Directory field. **Note** If you choose the **Default** option, Cisco IPICS changes the default settings and stores database backups in the **/idspri/backup** directory.
Backup retention	8 days

You can modify any of the default settings that are displayed in Table 11-2. 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 back up 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:
  - 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 backup files to be stored.

Note Cisco IPICS does not purge Remote Host backups.

See the "Guidelines for Choosing a Destination for Database Backups" section on page 11-8 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 to choose the number of days that you want the backup files 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.

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. To modify the time of day for the scheduled backup to begin, click the **Start Time** drop-down lists 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.

To discard your changes and return to the current default settings, click the **Cancel** button.

Caution If you do not click **Save**, your changes are not saved and the server reverts to the current settings.

Guidelines for Choosing a Destination for Database Backups

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

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

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.
  - 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 11-16 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.

Caution Database restores should only be done when there are no other users logging in to the system; otherwise, they may see errors or other strange behavior.

Note You cannot restore data from a database backup if high availability is running. In this case, you must temporarily unconfigure high availability before performing the restore. For instructions, see the "Unconfiguring HA" section on page 10-6.

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 VTGs, 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 running 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 could fail, or you could encounter unpredictable errors when you perform tasks in the Administration Console.

This section contains information about restoring your data and includes the following topics:

- Options for Using the Restore Procedure, page 11-10
- Performing the Restore Procedure, page 11-10
- Checking the Restore Status in the Database Log, page 11-12

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 make after Cisco IPICS performs the database backup will not be restored.

Performing the Restore Procedure

To restore your data, perform the following procedure:

Before you begin

Ensure that no other users are logged in to the system.

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, 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 and that you include the following directories in the directory path:

- The **/idspri/backup** directory—Cisco IPICS stores 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 11-17 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:

  - IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user name for access to the remote host.

    The user name to restore the database 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 database backup.
  - 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 When you perform a restore operation, 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 in the Administration Console until the restore operation completes. The Tomcat service restarts during the restore operation and automatically logs all users out of Cisco IPICS.

Tip You can check the status of the restore operation before it completes by viewing 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 11-12.

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 11-12.
- 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 a message that is similar to the following example:

     ```
     You entered an invalid user name or password, or your browser was unable to
     recognize your entries.
     Please enter your user name and password 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 11-12. If you still cannot log in to check this status, follow the troubleshooting procedures in the "Unable to Log In to the Administration Console After Restoring Data" section on page 11-18 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 that pertain to 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 that are listed in Step 3 in the "Downloading and Viewing the Backup and Restore Logs" section on page 11-14 to unzip the .zip file and view or download the db-maintenance.log file.

Checking the Restore Status in the Database Log

When the restore process begins, 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 11-14.

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 or root 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. The root user has access to all files in the Cisco IPICS server.

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**

Step 3 Check the last lines of this output 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 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 provide you with information that indicates why the restore process did not complete successfully; for example, a remote restore operation could not complete because you entered an incorrect password for the remote host.
  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 11-15 to attempt to fix the problem.
  e. Retry the restore operation by following the procedure in the "Performing the Restore Procedure" section on page 11-10.

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.

  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. After you download the files to your PC, you can view them as a text file.

Cisco recommends that you regularly check the database logs for status messages and/or error information that may be pertinent to recent backup and recovery activity.

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 the db-maintenance.log file to select it.

Step 8 Click **Extract**.

The Extract window opens.

Step 9 Navigate to the location of the directory where you want to save the db-maintenance.log file.

Step 10 Click **Extract**.

The extract program saves the db-maintenance.log file to the location that you specified on your PC.

Step 11 Double-click the dbm_log_archive.log.gz file to open it.

The .gz file opens and displays the dbm_log_archive.log file in a separate window.

Step 12 Click the dbm_log_archive.log file to select it.

Step 13 Click **Extract**.

The Extract window opens.

Step 14 Navigate to the location of the directory where you want to save the dbm_log_archive.log file.

Step 15 Click **Extract**.

The extract program saves the dbm_log_archive.log file to the location that you specified on your PC.

Step 16 To view the content of the log files, open the files with any software program, such as Notepad, that allows you to view text files.

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 11-16
- Restoring Data from a Remote Host Without scp Support, page 11-17
- Unable to Log In to the Administration Console After Restoring Data, page 11-18
- Unable to Retrieve a Database Backup from a Remote Host After Reinstalling Cisco IPICS, page 11-19
- Cannot Access the Administration Console to Back Up and Restore the Cisco IPICS Database, page 11-20

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, the remote host is a Windows PC or server).

Solution Choose the Local Directory option when you back up your files; then, use a Secure File Transfer Protocol (SFTP) client software program to copy your backup data to a remote host.

To back up your data to a remote host that does not support scp, perform the following procedure:

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 11-3.

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 use 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 **IDSB_2006-11-02_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 SSH Secure Shell program copies the backup folder and its contents to the folder that you specified on your PC. After the copy operation 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.

To restore your data from a remote host that does not support scp, perform the following procedure:

Procedure

Step 1 Access the remote host 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 use 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 Cisco IPICS server and displays the contents of the **/root** directory in the right pane of the window.

Step 8 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\IDSB_2006-11-02_14-04-52**.

Step 9 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 10 In the **Enter Folder Name** field, enter **/idspri/backup**.

The right pane of the window displays the contents of the **/idspri/backup** folder.

Step 11 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 SSH Secure Shell program copies the backup folder and its contents from your PC to the **/idspri/backup** directory. After the copy operation completes, the backup folder displays in the right pane.

Step 12 Click the **New Terminal Window** icon or choose **Window > New Terminal** from the menu bar to open a terminal window session.

Step 13 Enter the following command to change the ownership of the backup folder and files from the root user and group to the informix user and ipics group:

[root]# **chown -R informix:ipics /idspri/backup/IDSB***

Step 14 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 15 To close the SSH Secure Shell terminal window, click **Close**.

Step 16 To close the SSH Secure Shell File Transfer Client, click **Close**.

Step 17 Restore your files from the local directory by following the procedure in the "Performing the Restore Procedure" section on page 11-10. Be sure to specify the full directory path of the backed-up database when you perform 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 After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 11-12, you determine that the restore process has completed successfully. However, when you attempt to log in to the Cisco IPICS console, you receive a **Cannot find server or DNS Error** error message in your browser and you cannot access the Administration Console.

Solution The Tomcat service may not have 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 by using the root user ID.

Step 2 To restart the Cisco IPICS processes including the Tomcat service, enter the following command:

[root]# **service ipics restart**

Note Be aware that this command also restarts the policy engine, which cancels any active dial-in or dial-out calls.

Cisco IPICS displays the `[OK]` message after the Tomcat process and other Cisco IPICS processes have stopped, and again after they have successfully restarted.

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 11-12, you determine that the restore process has completed successfully. However, when you attempt to log in to the Cisco IPICS Administration Console, the system displays 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 In this case, the Cisco IPICS database might not have restarted after the restore operation. To restart the database, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the root user ID.

Step 2 To check the status of the database, enter the following command:

[root]# **onstat -**

Note This command displays the current status of the database.

If the database is online and running, the command displays the following response.

```
IBM Informix Dynamic Server Version 10.00.UC8W4   -- On-Line -- Up 15:54:28 -- 505836
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:

[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 After reinstalling the Cisco IPICS operating system, you attempt 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 the scp process uses 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*> | <*dnsname*>

where:

<*ip_address*> or <*dnsname*> 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 To accept the new public host key for the Cisco IPICS server, enter **Yes**.

Step 5 Enter **exit** to log out of the Cisco IPICS server.

Step 6 Enter **exit** 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 11-9.

Cannot Access the Administration Console to Back Up and Restore the Cisco IPICS Database

Problem You cannot access the Administration Console, so you are unable to perform backup and restore operations.

Solution For situations where you cannot access the Administration Console, you can use the command-line interface (CLI) to perform backup and restore procedures.

Note Cisco recommends that you use the Administration Console for normal backup and restore procedures. Use these CLI commands only in those situations where you cannot access the Administration Console.

To back up and restore your data by using CLI, perform the procedures that are documented in the following sections:

- Using CLI to Manually Back Up the Cisco IPICS Database, page 11-20
- Using CLI to Manually Restore the Cisco IPICS Database, page 11-22

Using CLI to Manually Back Up the Cisco IPICS Database

To manually back up your database by using CLI, use the **backup_ipics_ids** script. This script backs up your database, either to the default backup location or to a location that you specify. Use the arguments in the script to specify the location of the backup. You can back up your database files to the local server or to a remote server that supports the **scp** command.

To manually back up your database files, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the informix user ID.

If you cannot log in directly as the informix user (for example, if you do not know the password for the informix user ID), you can log in as the root user; then, access the informix user ID by using one of the following methods:

- Log in with the informix user ID by entering the following command:

  [root]# **su - informix**

- Reset the password for the informix user ID by entering the following command:

  [root]# **reset_pw -u informix**

  For more information about using the **reset_pw** command, see the "Troubleshooting the Cisco IPICS Server" chapter of the *Cisco IPICS Troubleshooting Guide*.

  A terminal window displays.

Step 2 To back up your database files, enter the following command:

[informix]$ **backup_ipics_ids** [**cp** <*localdirectory*>] [**scp** <*remotedirectory*> <*remoteip*> <*remoteuserid*> <*remotepassword*>]

where:

<*localdirectory*> specifies a subdirectory of the **/idspri/backup** directory where you want to store the database backup. If this directory does not exist, Cisco IPICS creates it for you as **/idspri/backup/***localdirectory*. For example, if you specify a directory of **mybackups** and that directory does not exist, Cisco IPICS creates a directory named **/idspri/backup/mybackups** and places the backup in that directory.

<*remotedirectory*> specifies the full directory path on the remote host where you want to store the database backup. This directory must exist; otherwise, the backup operation fails.

<*remoteip*> specifies the remote host IP address.

<*remoteuserid*> specifies the remote host user ID.

<*remotepassword*> specifies the password for the remote host user ID.

By default, if you do not specify any arguments with the **backup_ipics_ids** command, Cisco IPICS stores the database backup in the following directory:

/idspri/backup/IDSB_*yyyy-mm-dd_hh-mm-ss*

where:

yyyy-mm-dd_hh-mm-ss specifies the year, month, day, hour, minute, and second, respectively, that Cisco IPICS performed the backup procedure.

After you enter the **backup_ipics_ids** command, Cisco IPICS backs up the database files, creates the **IDSB**_*yyyy-mm-dd_hh-mm-ss* subdirectory, and stores the backup in the specified subdirectory.

Using CLI to Manually Restore the Cisco IPICS Database

You can use the **restore_ipics_ids** script to restore your database from a backup file that you obtained from a backup operation. You can restore your database from a backup file on the local Cisco IPICS server or from a file on a remote server.

When you restore your files, you specify the full directory path where the backup file resides. The backup file has a file extension of .ota. An example of a full directory path is as follows:

/idspri/backup/IDSB_2007-05-01_17-11-47

By default, Cisco IPICS stores scheduled backup files in the **/idspri/backup/cron** directory. To restore your database from a scheduled backup that uses the default values, specify an .ota file from the **/idspri/backup/cron/** directory.

To manually restore your database from an existing backup, perform the following procedure. If high availability is running, you must temporarily unconfigure high availability before performing this procedure. For instructions, see the "Unconfiguring HA" section on page 10-6.

Procedure

Step 1 Open a terminal window and log in to the server by using the informix user ID.

A terminal window displays.

Step 2 If you already know the name of the backup file to use for the restore procedure, continue to Step 3. Otherwise, find the .ota file to use for the restore procedure by performing the following tasks:

- To find an .ota file on the local server, perform the following steps:
  - **a.** To list all of the .ota files on your server, enter the following command:

    [root]# **find / -name *.ota | more**

    The name and full directory path of all .ota files that are on the server displays.

    Note If many .ota files exist on your server, the list of files displays in multiple screens. Press the **Spacebar** to continue to the next screen.

  - **b.** Make a note of the full directory path and name of the .ota file that you want to use for the restore procedure.
- To find an .ota file on a remote host, log in to the remote host and perform Steps a and b.

  Note When Cisco IPICS performs a remote backup, it creates a copy of each remote backup and stores it in the **/idspri/backup** directory on the local server; therefore, you can also find the list of remote backups in the **/idspri/backup** directory on the local server.

Step 3 To restore your database files, enter the following command:

[informix]$ **restore_ipics_ids** [**L**] [**L A** <*localdirectory*>] [**L A R** <*remoteuserid*> <*remotepassword*> <*remoteip*> <*remotedirectory*>]

where:

<*localdirectory*> specifies the full directory path on the local server where the .ota file is located.

<*localfilename*>**.ota** specifies the name of the backup file on the local server to use for the restore procedure.

<*remoteuserid*> specifies the remote host user ID.

<*remotepassword*> specifies the password of the remote host user ID. If backup files are not on the same server to which you are restoring, precede any special characters in the password with a backslash (\).

<*remoteip*> specifies the remote host IP address.

<*remotedirectory*> specifies the full directory path on the remote host where the .ota file is located.

Cisco IPICS restores the database from the .ota file that you specify.

CHAPTER 12

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:

- Understanding the Serviceability Drawer, page 12-1
- Viewing the Information in the Dashboard Window, page 12-1
- Viewing Cisco IPICS Server Diagnostic Information, page 12-6
- Viewing the Cisco IPICS System Logs, page 12-9

Understanding the Serviceability Drawer

The Serviceability drawer is located in the Server tab of the Administration Console and contains 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 12-1.
- 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 12-6
- 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 12-9.

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, incident, VTG, user, license, and RMS details.

The format of this window includes multiple panes, 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 12-2
- Understanding the Channel Dashboard, page 12-3
- Understanding the Incident Dashboard, page 12-3
- Understanding the Virtual Talk Group Dashboard, page 12-4
- Understanding the User Dashboard, page 12-4
- Understanding the License Dashboard, page 12-5
- Understanding the RMS/UMS Dashboard, page 12-6

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 12-1 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 8-3.

Table 12-1 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 6-4 and the "Managing Actions for a Policy" section on page 6-5.
Policy Engine status	The status of the policy engine. A status of Up indicates that the policy engine is active; a status of Down indicates that the policy engine is inactive.
Configured activity log size (in MB)	The maximum size of the activity log file. **Note** For more information about activity logs, see the "Managing Activity Logs" section on page 2-71.
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 currently uses.
CPU - percent idle	The percentage of CPU resources that are idle and available. The CPU resources are obtained from the CPU in the server.

Table 12-1 Elements in the System Dashboard (continued)

Element	Description
Disk usage (in GB) [used / free / total]	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, and the total amount of hard disk space that is available in your server.
Total/Available number of multicast addresses in pool	The total number of multicast addresses in the multicast address pool and the number of multicast addresses that are available. For more information about the multicast address pool, see the "Managing the Multicast Pool" section on page 2-33.

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 12-2 for all of the elements that are contained in this pane.

Table 12-2 Elements in the Channel Dashboard

Element	Description
Total number of channels	The total number of channels that you have configured in the Cisco IPICS server.
Number of enabled channels	The number of channels that are enabled.
Number of disabled channels	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	The number of enabled channels that are present in a virtual talk group (VTG).

Understanding the Incident Dashboard

The Incident Dashboard displays information about the total number of incidents and the number of active and inactive incidents in your system. For more information about channels and how they are used in Cisco IPICS, see the "Managing Incidents" section on page 2-58.

See Table 12-3 for all of the elements that are contained in this pane.

Table 12-3 Elements in the Incident Dashboard

Element	Description
Total number of incidents	The total number of incidents that you have configured in the Cisco IPICS server.
Number of active incidents	The number of incidents that are active.
Number of inactive incidents	The number of incidents that are inactive.

Understanding the Virtual Talk Group Dashboard

The Virtual Talk Group Dashboard displays information about the number of VTGs and inactive VTGs in your system. For more information about VTGs, see the "Managing VTGs" section on page 5-2.

See Table 12-4 for all of the elements that are contained in this pane.

Table 12-4 Elements in the VIrtual Talk Group Dashboard

Element	Description
Number of VTG templates	The number of VTG templates, or inactive VTGs, that exist in the server.
Number of active VTGs	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 a Cisco Unified IP Phone, and the number of users who are logged in to Cisco IPICS by using the IDC. For more information about users, see the "Managing Users" section on page 3-1.

See Table 12-5 for all elements in the user dashboard.

Table 12-5 Elements in the User Dashboard

Element	Description
Number of users logged in to the administration console	The total number of users who are logged in to the Administration Console.
Number of Cisco Unified IP phone users logged in to Cisco IPICS	The total number of Cisco Unified IP Phone users who are logged in to the Cisco IPICS system.
Number of IDC users logged in to Cisco IPICS	The total number of IDC 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 total number licenses for various items and the current status of those items. For more information about licenses, see the "Managing Licenses" section on page 2-63.

Table 12-6 describes the elements that are contained in this pane.

Table 12-6 Elements in the License Dashboard

Element	Description
Concurrent UMS Servers	The number of concurrent UMS servers that your Cisco IPICS system is licensed to use and the number of UMS servers that are available for use.
Concurrent LMR Ports	The number of concurrent LMR ports that your Cisco IPICS system is licensed to use and the number of LMR ports that are available for use.
Concurrent Dispatch Console Silver Users	The total number of concurrent IDC Silver users that your system is licensed for and the number of IDC Silver users that the system can currently accept.
Concurrent Dial Users	The total number of concurrent dial users that your system is licensed for and the number of dial users that the system can currently accept.
Concurrent Multicast Ports	The number of concurrent multicast ports that your Cisco IPICS system is licensed to use and the number of multicast ports that are available for use.
Concurrent Gateway P25 Vocoders	The number of concurrent P25 channels that your Cisco IPICS system is licensed to use and the number of P25 channels that are available for use.
Concurrent Dispatch Platinum Users	The total number of concurrent IDC Platinum users that your system is licensed for and the number of IDC Platinum users that the system can currently accept.
Concurrent Cisco Unified IP Phone Users	The total number of concurrent Concurrent Cisco Unified IP Phone users that your system is licensed for and the number of Cisco Unified IP Phone that the system can currently accept.
Concurrent ISSI Gateway Servers	The number of concurrent ISSI Gateway servers that your Cisco IPICS system is licensed to use and the number of ISSI Gateway servers that are available for use.
Concurrent EndToEnd P25 Vocoders	The number of concurrent connections to end-to-end P25 channels that your Cisco IPICS system is licensed to use and the number of concurrent connections to end-to-end P25 channels that are available for use.
Concurrent Mobile Endpoint Users	The total number of concurrent mobile client (endpoint) users that your system is licensed for and the number of mobile endpoint users that the system can currently accept.

Understanding the RMS/UMS Dashboard

The RMS/UMS Dashboard displays information about the 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 2-39. For more information about the UMS, see the "Managing the UMS" section on page 2-50.

See Table 12-7 for all of the elements that are available in this pane.

Table 12-7 Elements in The RMS Dashboard

Element	Description
RMS *rms-hostname*	The status for the RMS with the specified *rms-hostname*. For more information, see the Status field in Table 2-14 on page 2-42.
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; this 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.

To download all diagnostic information that is included in this window, along with the ipics.log file, click the **Download Diagnostic Results** button. For more information about how to download the diagnostic results, see the "Downloading the Server Diagnostic Information" section on page 12-8.

For more information about the log severity information that is included in each message, see the "Understanding the System Log Severities" section on page 12-10.

See Table 12-8 for all of the elements that are contained in the Diagnostic Summary pane.

Table 12-8 Elements in the Diagnostic Summary Pane

Element	Description
Cisco IPICS Server Hostname:	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**
Cisco IPICS Server Current Date and Time:	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**

Table 12-8 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Cisco IPICS Server OS Version:	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]# **versions**
Cisco IPICS Server Software Version:	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]# **versions**
Cisco IPICS Server Software Version upgrade history:	The date and time that the current version of Cisco IPICS was installed and provides a history, with release versions, of the times that the software has been uninstalled or upgraded. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/ipics-release.history**
Hardware Platform Details:	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:	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:	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**
Uploaded License File Name(s):	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:	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/***

Table 12-8 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Cisco IPICS Database Status:	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:	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]# **top-ipics**
Cisco IPICS Radio Control Service Status:	The current status of the Cisco IPICS Radio Control service. This service controls serial radios. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **service ipics_rcs status**
Cisco IPICS Server Hard Disk Utilization Information:	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**
Cisco IPICS IDC Configuration File Contents:	The contents of the idc.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/idc.ini** **Note** Cisco IPICS uses the idc.ini file to determine how to communicate with the Cisco IPICS server. The idc.ini file is present only if you have generated an IDC installer. If you have not yet generated the IDC installer file, Cisco IPICS displays the following message: `Cannot find any idc.ini files under the /opt/cisco/ipics/tomcat/current/webapps/ipics_files/store/installer folder.` For more information about the idc.ini file, and how to generate an IDC installer, see the "Managing IDC Versions" section on page 2-86.

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 Severities" section on page 12-10.

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.

Tip 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.

This section includes the following topics:

- Understanding the System Log Severities, page 12-10
- Searching the System Logs By ERROR or WARNING Messages, page 12-11
- Downloading System Logs, page 12-12

Understanding the System Log Severities

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 12-9 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 12-9 System Log Entry Types

Log Entry Type	Purpose
TRACE	Detailed debug information about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational messages about noteworthy events, such as the start of a scheduled policy.
WARN	Warning messages about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.
ERROR	Messages that are 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	An unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires you to take immediate action to fix the specified error. 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. 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. Cisco recommends that you do not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Searching 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 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 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 appear dimmed. If you are viewing the last message in the System Log, the **>** and **>|** arrow buttons appear 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 of 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 maximum 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 ipics_logs.zip 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.

Viewing the Cisco IPICS RCS Logs

Cisco IPICS provides the ability to view the latest radio controls service (RCS) log information in the RCS Logs window. The Recent RCS Log Entries pane in the **Serviceability > RCS Logs** window contains the log information that shows information about the serial RCS and the radios that it controls. The information that is contained in these logs can help you to troubleshoot problems that you might encounter with serial radio control.

Tip 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 **RCS 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.

This section includes the following topics:

- Understanding the System Log Severities, page 12-10
- Searching the System Logs By ERROR or WARNING Messages, page 12-11
- Downloading System Logs, page 12-12

Understanding the RCS Log Severities

The RCS 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 12-10 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 12-10 RCS Log Entry Types

Log Entry Type	Purpose
TRACE	Detailed debug information about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational messages about noteworthy events, such as the start of a scheduled policy.
WARN	Warning messages about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.
ERROR	Messages that are 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.

Table 12-10 RCS Log Entry Types (continued)

Log Entry Type	Purpose
FATAL	An unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires you to take immediate action to fix the specified error. 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. 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 RCS logs. Cisco recommends that you do not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Searching the RCS Logs By ERROR or WARNING Messages

To visually identify the type of status messages that display in the Recent RCS 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 RCS 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 > RCS 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 RCS 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 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 the arrow buttons to navigate and view each ERROR or WARNING message:

- Click **| <** to find the first message in the RCS Log.
- Click **<** to move backward one message in the RCS Log.
- Click **>** to move forward one message in the RCS Log.
- Click **> |** to move to the last message in the RCS Log.

Note If you are viewing the first message in the RCS Log, the **| <** and **<** arrow buttons appear dimmed. If you are viewing the last message in the RCS Log, the **>** and **> |** arrow buttons appear dimmed.

Downloading RCS Logs

Cisco IPICS displays the most current RCS log information in the Recent RCS Log Entries pane and allows you to download all of the RCS logs to your PC.

Cisco IPICS saves the log information in sequential log files, starting with rcs.log and continuing with rcs.log.1 through rcs.log.10.

- Cisco IPICS records RCS log information in the ipics.log file and continues to add data to it until the file reaches a maximum size of approximately 1 MB.
- When the rcs.log file reaches its maximum size, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new rcs.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 rcs.log.1 to rcs.log.10, in addition to the most recent rcs.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 rcs.log files.

The system logs are located in the following directory:

/opt/cisco/rcs/logs

To download the RCS logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > RCS Logs**.

Step 2 Click **Download** at the bottom of the window, under the **Recent RCS Log Entries** pane.

The File Download dialog box displays.

Step 3 Click **Open** to open the rcs_logs.zip 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 rcs.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.

APPENDIX A

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. For more information, see the RMS tasks that are described in Chapter 2, "Performing Cisco IPICS System Administrator Tasks."

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, IDC users may hear a busy tone when they attempt to activate a channel or VTG because of configuration discrepancies.
- If you have more than one RMS component configured in the server, make sure that you configure each RMS according to the instructions that are documented in this appendix.

Note Be aware that Cisco IPICS provides support only for RMS components that are configured, as described in this appendix.

This appendix contains information about how to configure the RMS, and includes the following topics:

- Configuring Security Features, page A-1
- Connecting and Configuring T1/E1 Controllers, page A-4

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:

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.

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, see 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*>

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).

Router(config)# **crypto key generate rsa**

When you are prompted to enter the number of bits in the modulus, enter **768**.

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 SSH version 2, enter the following commands:

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, see your Cisco IOS documentation.

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 IDC 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.

Note For a complete list of supported interface cards and RMS routers, see *Cisco IPICS Compatibility Matrix*.

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-4
- RMS IP Address Selection Guidelines, page A-6
- Configuring T1/E1 Controllers, Interfaces, and Voice Parameters, page A-7

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-5.

- Typically, an E1 controller will support 30 ds0s, but your controller may support fewer ds0s, depending on the number of available DSPs.

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-5.

- 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)

  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-7. 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-7.

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
  - The server and the IDC components use this address to connect to the RMS

Note Cisco recommends that you specifically configure the Loopback0 interface when there is more than one IP path to the RMS. However, you may configure an interface other than Loopback0 if the following criteria is met:

– The IP address that you assign to the interface matches the IP address of the RMS in the Cisco IPICS RMS configuration. For configuration information about assigning this IP address, see Step 11 in the "Configuring T1/E1 Controllers, Interfaces, and Voice Parameters" section. (Make sure that you substitute the interface that you are configuring for the Loopback0 interface that is documented in this step.)

– The SIP **bind control source-interface** and **bind media source-interface** commands specify the interface that you configured. For configuration information about binding the source address for signaling and media packets to the IP address of the interface, see Step 12 in the "Configuring T1/E1 Controllers, Interfaces, and Voice Parameters" section. (Make sure that you substitute the interface that you configured for the Loopback0 interface that is documented in this step.)

– If you configure an interface other than Loopback0, remember to substitute the interface that you use with the Loopback0 references that appear in related documentation.

- 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 IDC PTT button to the time that the media is established between the remote IDC 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.

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:

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.

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, see your Cisco IOS documentation.

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-5.

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
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
```

```
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
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:

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**

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, see *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

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

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-6.

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-6.

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)# **ip address trusted list**

Router(cfg-iptrust-list)# **ipv4** *ip_address subnet_mask*

where:

ip_address specifies the IP address that should have access to the Cisco IPICS SIP connections
subnet_mask specifies the 30-bit subnet mask that is associated with the IP address

Repeat this **ipv4** command as needed for each IP address and mask.

Router(cfg-iptrust-list)# **exit**

c. Router(conf-voi-serv)# **allow-connections sip to sip**

This command specifies that connections between SIP endpoints are allowed.

d. Router(conf-voi-serv)# **sip**

This command enables Session Initiation Protocol (SIP) configuration mode.

e. 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.

Note

- When you enter the **bind control source-interface Loopback0** command, make sure that there are no active voice calls on the RMS.
- To verify that there are no active voice calls on the RMS, enter the **show call active voice brief** command from the RMS command line. The command output must indicate 0 total call legs, as shown below:
  Total call-legs: 0
- To verify that the **bind control source-interface Loopback0** command was successful, enter the **show run** command from the RMS command line. Look for the presence of the **bind control source-interface Loopback0** in the running configuration output.
- If the **bind control source-interface Loopback0** command is not present in the running configuration output, it was not successfully applied. In this situation, you will encounter a fast busy tone when you call the dial engine directory number. In addition, the Cisco IOS SIP debug logs show a SIP 403 (forbidden) message from the dial engine.
- To resolve this situation, enter the **shutdown** <*voice-port*> command in voice-port configuration mode to take the voice ports for a specific voice interface card offline. Enter this command for any voice ports that may be online. Then, reenter the **bind control source-interface Loopback0** command, followed by the **no shutdown** <*voice-port*> command to bring your voice ports back online. Enter this command for any voice ports that you brought offline.

f. 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:

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)# **media-inactivity-criteria rtcp**

This command specifies the use of RTCP for media inactivity (silence) detection.

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

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

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

Step 17 Configure the list of codecs that Cisco IPICS will support by entering the following commands:

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 Configure the SIP user agent as follows.

These commands enable the RMS to accept the G.729 codec for SIP IDC connections.

Router(config)# **sip-ua**
Router(config)# **g729-annexb override**

Step 19 Create the following inbound dial peer by entering the following commands.

These commands configure the voice dial peer and turn off voice activity detection (VAD) on the default SIP IDC connection.

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)# **session protocol sipv2**
Router(config-dial-peer)# **incoming called-number .**
Router(config-dial-peer)# **no vad**
Router(config-dial-peer)# **dtmf-relay rtp-nte**
Router(config-dial-peer)# **voice-class codec 1**

To enable Tone Remote Control (TRC) functionality for remote IDC users, you must also configure the following commands as part of this dial-peer command:

Router(config-dial-peer)# **rtp payload-type nte-tone 108**
Router(config-dial-peer)# **rtp payload-type lmr-tone 107**

Note For information about how to obtain the Cisco IOS software that supports the Tone Remote Control functionality, contact ask-ipics-support@external.cisco.com.

Step 20 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 IDC direct dial feature, you do not need to configure this dial peer.

Tip 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 Communications Manager or Cisco IOS SIP Provider IP address***>**
Router(config-dial-peer)# **session transport tcp**
Router(config-dial-peer)# **dtmf-relay rtp-nte**

where:

Cisco Unified Communications Manager or Cisco IOS SIP Provider IP address specifies the IP address of your SIP provider.

These commands configure the voice dial peer that enables the IDC 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 IDC direct dial capability, you can change this dial peer or add additional dial peer entries to allow for other destination patterns, as needed.

Note If you have more than one RMS component configured in the server, make sure that you perform the direct dial configuration, as documented in Step 20 and Step 21, for each RMS. When more than one RMS component is configured in the server, Cisco IPICS may use any one of these configured components, depending on load conditions, to set up the SIP connection for the direct dial functionality.

For more information about configuring the IDC direct dial feature, see the "Managing Direct Dial Numbers" section on page 8-29. For information about using the IDC direct dial feature, see *Cisco IPICS Dispatch Console User Guide* for this release.

Step 21 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 IDC direct dial feature, or if you do not use Cisco Unified Communications Manager 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 Communications Manager and are used to authenticate this user. For more information, see the "Configuring Cisco Unified Communications Manager as the SIP Provider" section on page 8-32.

Step 22 Enter the following command to reset the router command prompt:

Router(config)# **no prompt**

Step 23 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 24 Execute the following command to save your changes:

Router# **copy running-config startup-config**

Step 25 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 26 To resolve this problem, disconnect the loopback cable from the router; then, reconnect it.

The LP LED should now be off.

Step 27 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

e1 3/1 is up
No alarms detected
```

Note Cisco IPICS supports the use of Land Mobile Radio (LMR) gateways, the functionality of which 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.

APPENDIX B

Using Cisco IPICS for External Notifications

The Cisco policy engine notification action, which is described in Chapter 6, "Using the Cisco IPICS Policy Engine," contacts designated recipients and provides them with information that you specify. Those recipients must be configured in Cisco IPICS.

You can also use Cisco IPICS to send notifications to recipients who are not configured in Cisco IPICS. This type of notification is called an *external notification* and does the following:

1. Simultaneously calls many external users at telephone numbers that Cisco IPICS obtains from a file that you specify.
2. Plays a designated message to each user who answers the call.
3. Captures results of each call in a log file that you can review at any time.

You invoke an external notification by sending an HTTP request or by posting a Common Alerting Protocol (CAP) .xml file to the appropriate server.

This appendix describes how to set up Cisco IPICS for external notifications and how to invoke external notifications. It includes these sections:

- Requirements for Implementing External Notifications, page B-1
- Invoking External Notifications, page B-3
- Retrieving External Notification Results, page B-5
- Reviewing External Notification Results, page B-8
- XML File Parameters for External Notifications, page B-8

Requirements for Implementing External Notifications

To use Cisco IPICS for external notifications, you must configure a dial engine, designate a list of recipients, and designate a message file to play to the recipients.

The following sections describe these requirements in detail.

Dial Engine

A dial engine is a Cisco IPICS server the system to which you send the request to invoke an external notification and that handles dialing out and playing messages to external notification recipients. This server enables distribution of the call load so that notifications to a large number of recipients can be made efficiently. Any Cisco IPICS server in a network can be a dial engine.

To configure a Cisco IPICS server as a dial engine, you edit a .xml configuration file on that server and set the dialEngine sub-element attributes for the dial engine. To do so, perform the following procedure:~~

Procedure

Step 1 On the Cisco IPICS server that you want to be the dial engine, edit the dedicated-dial-engines.xml file, which is stored in this folder:

/opt/cisco/ipics/tomcat/current/webapps/ipics_server/WEB-INF/classes

Step 2 In the dedicated-dial-engines.xml file, uncomment the "dialEngine" sub-element, and set the following attributes for the dial engines:

- id—Set a unique identifier for a dial server (the identifier can be the host name of the server)
- bulkNotifyApp—Set to BulkNotifyDialer
- host—IP address or host name of the dial engine

Step 3 Save the dedicated-dial-engines.xml file.

Step 4 Restart the Cisco IPICS service by entering the following command from the root user ID:

service ipics restart.

Recipient List

A recipient list is a .xml file that contains a list of each person who should receive the external notification message. To invoke an external notification that contacts these recipients, you must know the URL of the server on which the recipient list resides.

A recipient list should be in the format that is shown in this section and should follow these guidelines:

- "id" is required and must be unique for each recipient.
- "name" is optional.
- "contacts" is a list of recipients in the order that they should be called.
- "phone type" is optional.
- "dn" is required. The dn value is sent to the voice gateway exactly as entered.

The following is an example of a valid recipient list:

```
<users>
  <user id="5" name="Kim Smith">
    <contacts>
      <phone type="mobile" dn="14085554444" />
      <phone type="home" dn="14085555555" />
    </contacts>
  </user>
  <user id="7" name="Bob Jo">
    <contacts>
      <phone type="work" dn="1342433534" />
      <phone type="home" dn="14085543255" />
    </contacts>
  </user>
</users>
```

Message File

A message file is a .wav file in pulse code modulation (PCM) or CCITT u-Law format that contains the recorded message to play to recipients. Cisco recommends that the message be no longer than 90 seconds.

To invoke an external notification that plays this message, you must know the URL of the server on which the message file resides.

Invoking External Notifications

You can invoke a notification action by sending an HTTP get request to the dial engine or by posting a valid CAP .xml file over HTTP to the dial engine.

Invoking an External Notification by Sending an HTTP Request

To invoke an external notification with an HTTP request, send the following request to the server that is designated as the dial engine:

http://<*Dial_Engine_Server*>:8080/ipics_server/BulkNotify?
method=httpNotify?capId=<*CAP_ID_#*>&userListURL=<*User_List_URL*>
&waveFileURL=<*Wave_File_URL*>
&announcementText=<*Announcement_Text*>
&questionWaveURL<*number*>=<*Question_Wave_URL*>

where:

- <*Dial_Engine_Server*> is the fully qualified hostname or the IP address of the Cisco IPICS server that includes the dial engine.
- <*CAP_ID_#*> is a unique identifier that you assign to this invocation request.
- <*User_List_URL*> is the HTTP URL from which the recipient list can be retrieved.
- <*Wave_File_URL*> is the HTTP URL from which the message file can be retrieved.
- (Optional) <*Announcement_Text*> is the text that displays on Cisco Unified IP Phones.
- <*number*> is the question number. This value must start with 1 and increment by values of one.
- (Optional) <*Question_Wave_URL*> is the HTTP URL from which the question file can be retrieved. The retrieved question file name must conform to the following format:

  Question<*number*>_<*dtmf_choices*>.wav

  where:

  – <*number*> is the question number. This number must match the number in the questionWaveURL attribute.

  – <*dtmf_choices*> is the number of allowable keypad digits that the phone recipients can enter, as shown in the following questionWaveURL parameter examples:

  - An HTTP request with the parameter &questionWaveURL1=Question1_1234.wav plays audio to which the phone recipient can respond by pressing 1, 2, 3, or 4 on their keypad.

  - An HTTP request with the parameter &questionWaveURL2=Question2_12.wav plays audio to which the phone recipient can respond by pressing 1 or 2.

- An HTTP request that contains the parameter &questionWaveURL3=Question3_1.wav plays audio to which the phone recipient can only respond by pressing 1. You can use this type of request to confirm that a user has received this notification.

Note Parameter that include spaces or special characters must use standard HTTP escape codes.

Invoking an External Notification by Posting a CAP XML File

You can invoke an external notification by posting a valid CAP .xml file to this URL:

http://<*Dial_Engine_Server*>:8080/ipics_server/BulkNotify?method=capNotify?&cap=<*CAP_XML*>

where:

- <*Dial_Engine_Server*> is the host name or IP address of the Cisco IPICS server that includes the dial engine.
- <*CAP_XML*> is a valid CAP file

To use this notification method, the following guidelines must be followed:

- A resource with the resource description IPICSUserList must exist. The Uniform Resource Identifier (URI) for this resource must specify the HTTP URL of the server from which the recipient list can be retrieved. The mimeType for this resource must be text/xml.
- A resource with the resource description IPICSWaveFile must exist. The URI for this resource must specify the HTTP URL of the server from which the message file can be retrieved. The mimeType for this resource must be audio/wav.
- (Optional) A resource with the resource description AnnouncementText may exist. The URI for this resource must specify the HTTP URL of the server from which the text message can be retrieved. The mimeType for this resource must be text/plain.
- (Optional) A resource with the resource description QuestionWaveURL<number> may exist. The URI for this resource must specify the HTTP URL of the server from which question file can be retrieved. Please see HTTP invocation section for further info on how to specify Question files. The mimeType for this resource must be audio/wav.

The following is an example of a valid CAP file:

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
<identifier>5</identifier>
<sender>mycontact@mycompany.com</sender>
<sent>2003-06-11T22:39:00-07:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<source>SW</source>
<scope>Public</scope>
<info> <category>Rescue</category>
<event>Earthquake</event>
<urgency>Immediate</urgency>
<severity>Severe</severity>
<certainty>Likely</certainty>
<eventCode>
<valueName>SAME</valueName>
<value>CAE</value>
</eventCode>
<senderName>San Jose Earthquake Prevention</senderName>
```

```
<headline>SJ Earthquake</headline>
<description>Earthquake in SJ Downtown</description>
<contact>Earthquake Prevention – 408-555-1212</contact>
<resource>
<resourceDesc>IPICSUserList</resourceDesc>
<uri>http://ipics-server:8080/BulkCapSimulator/BulkCapSimulator?method=userList</uri>
</resource>
<resource>
<resourceDesc>IPICSWaveFile</resourceDesc>
<uri>http://ipics-server:8080/BulkCapSimulator/BulkCapSimulator?method=waveFile&amp;p=anno
uncement</uri>
<mimeType>audio/wav</mimeType>
</resource>
<resource>
<resourceDesc>QuestionWaveURL1</resourceDesc>
<uri>http://ipics-server:8080/BulkCapSimulator/BulkCapSimulator?method=waveFile&amp;p=q1</
uri>
<mimeType>audio/wav</mimeType>
</resource>
<resource>
<resourceDesc>AnnouncementText</resourceDesc>
<uri>http://ipics-server:8080/BulkCapSimulator/BulkCapSimulator?method=announcementText</u
ri>
<mimeType>text/plain</mimeType>
</resource>
<area>
<areaDesc>San Jose, Ca</areaDesc>
<geocode>
<valueName>SAME</valueName>
<value>006037</value>
</geocode>
</area>
</info>
</alert>
```

Retrieving External Notification Results

After you invoke an external notification, you can retrieve a file that displays the results of that notification. To obtain the results of an external notification, send the following request to the Cisco IPICS server that includes the dial engine functionality:

http://<*Dial_Engine_Server*>:8080/ipics_server/BulkNotify? method=incidentStatus&capId=<*CAP_ID_#*>
&statusType=<SUMMARY | DETAILED>

where:

- <*Dial_Engine_Server*> is the host name or IP address of the Cisco IPICS server that includes the dial engine.
- <*CAP_ID_#*> is the unique identifier number of the invocation request for which you are requesting results
- SUMMARY or DETAILED is the level of the status information that you want to receive.

A summary type of SUMMARY provides basic information about the incident including the start time, completion time, and status of the notification. A summary type of DETAILED provides a list of the users that were successfully reached, and how they responded to the questions that you provided.

The following is an example of output from a DETAILED-level status .xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<NotificationStatus>
<Incident capId="5">
<Status>SUCCESSFULLY_FINISHED</Status>
<StartTime>Mon Nov 19 15:25:07 PST 2007</StartTime>
<FinishTime>Mon Nov 19 15:25:17 PST 2007</FinishTime>
<UserSummary failedToNotify="0" successfullyNotified="1" totalUsers="1">
<User id="1028">
<Contacts>
<Phone dialNumber="1029" extn="" shared="false">
<Status>SUCCESSFUL</Status>
<Time>Tue Dec 04 16:35:55 PST 2007</Time>
<QuestionResponses>
<Response promptId="q1">
<Value>1</Value>
</Response>
</QuestionResponses>
</Phone>
</Contacts>
</User>
<User id="1028-3">
<Contacts>
<Phone dialNumber="1028" extn="" shared="true">
<Status>SUCCESSFUL</Status>
<Time>Tue Dec 04 16:35:50 PST 2007</Time>
<QuestionResponses>
<Response promptId="q1">
<Value>1</Value>
</Response>
</QuestionResponses>
</Phone>
</Contacts>
</User>
<User id="1028-1">
<Contacts>
<Phone dialNumber="1028" extn="" shared="true">
<Status>SUCCESSFUL</Status>
<Time>Tue Dec 04 16:35:50 PST 2007</Time>
<QuestionResponses>
<Response promptId="q1">
<Value>1</Value>
</Response>
</QuestionResponses>
</Phone>
</Contacts>
</User>
<!-- End detailed summary>
</UserSummary>
</Incident>
</NotificationStatus>
```

Table B-1 describes the summary report fields that display in the .xml file.

Table B-1 .xml File Summary Report Fields

Field	Description
Incident	This element contains the capId attribute. The capId attribute represents the unique identifier number of the invocation request for which you are requesting results.
Status	This element represents the status of the invocation request. Valid entries in this field are SUCCESSFULLY_FINISHED, PROCESSING, ABORTED_NO_CONFIGURED_DE, ABORTED_TIMEOUT_WAITING_ON_DE, ABORTED_FAILED_UPLOAD_PROMPT_TO_DE, ABORTED_PROMPT_DOWNLOADED_TRANSCODE_FAILURE, ABORTED_USER_LIST_PARSE_ERROR and ABORTED_UNKNOWN.
StartTime	This element represents the date and time that the invocation request started.
FinishTime	This element represents the date the time that the invocation request completed.
UserSummary	The UserSummary element contains the following attributes: • failedToNotify provides you with the number of the participants that could not be notified. • successfullyNotified provides you with the number of the participants that were successfully notified. • totalUsers provides you with the total number of users in the notification.

If you specify a detailed report, the XML file contains the additional fields that Table B-2 describes.

Table B-2 .xml File Summary Additional Report Fields for Detailed Report

Field	Description
User id	This element represents the ID of the phone number that was called. If more than one user shares a phone number, the shared attribute is set to true; otherwise it is set to false.
Phone	The Phone element contains the following attributes: • The dialNumber field represents the phone number that was called. • The extn field represents the extension of the number that was called. If the number does not contain an extension, this field is blank. • The shared field indicates whether the number is shared by more than one user. If the shared field is set to true, the number is shared by multiple recipients; otherwise it is set to false.
Status	This element represents the status of the call. Valid fields are SUCCESSFUL, NO_ANSWER, BUSY, INVALID, NO_RESOURCE, ANSWERED_NO_ACKNOWLEDGEMENT and UNSUCCESSFUL.

Table B-2 .xml File Summary Additional Report Fields for Detailed Report (continued)

Field	Description
Time	The time that the end user device received the notification.
QuestionResponses	The QuestionResponses element contains the following fields: • Response promptId is the ID of the question that you configured in the HTTP invocation request. This ID corresponds to the number in the name of the .wav file. For example, if the .wav file had the name Question1_<*dtmf_choices*>.wav, the response promptId is q1. • Value is the number that the user pressed on the dial pad.

Note If you do not specify the summaryType parameter, Cisco IPICS uses SUMMARY, as the default value.

Reviewing External Notification Results

Cisco IPICS captures and stores the results of calls that it makes when an external notification executes. This information is stored in the ipics.log file, which is stored on the Cisco IPICS server in this folder:

/opt/cisco/ipics/tomcat/current/logs

To stop/terminate an external notification with an HTTP request, send the following request to the server that is designated as the dial engine:

http://<*Dial_Engine*>:8080/ipics_server/BulkNotify?method=stopNotification&capId=<*CAP_ID_#*>

where

- <*Dial_Engine*> is the host name or IP address of the dial engine.
- <*CAP_ID_#*> is a unique identifier that you assign to this invocation request.

XML File Parameters for External Notifications

The dedicated-dial-engines.xml file includes the configurable parameters that Table B-3 describes.

Cisco recommends that you do not change these values unless it is required by your network configuration. For example, if your network has high latency that causes calls to exceed a timeout value, you could increase the timeout value.

In addition, Cisco recommends that you do not modify any of the other values in this XML file, specifically the following files: maxDialEngineWaitForDialing, maxDialEngineWaitForAck, maxDialEngineWaitForIPPhone, and maxDialEngineWaitForOnCall.

Table B-3 New Configurable Parameters in dedicated-dial-engines.xml File

Value	Description
connectTimeout	This value represents the maximum timeout value, in milliseconds, for the primary dial engine to connect to the dedicated dial engine. If the primary dial engine does not connect to the dedicated dial engine within the specified time, Cisco IPICS reports this error in the ipics.log file as a dial engine failure and requeues the notification request. To view the ipics.log file, navigate to the Serviceability > System Logs window in the Cisco IPICS Administration Console, and view the information that displays in the
dialEngineFailure CapForDuration	This value represents the time window, in milliseconds, that Cisco IPICS counts multiple dial engine failures as a single dial engine failure. If you use the default value of 500, Cisco IPICS counts any dial engine failures that occur during a half-second time window as one dial engine failure.
initialEngineFaliure ReattemptDuration	This value represents the time, in milliseconds, that Cisco IPICS waits before contacting the primary dial engine after a dial engine failure (for example, if there are no dial engine resources available to send the notification). **Note** Each subsequent retry attempt doubles this value. If you use the default value of 2000, and Cisco IPICS cannot complete a notification action because of a primary dial engine failure, Cisco IPICS waits 2 seconds before contacting the dial engine to retry the notification action. If Cisco IPICS detects another dial engine failure, it waits 4 seconds before contacting the dial engine. A successful dial engine call resets this value to the configured value.
maxDialEngine FailureWaitTimeCap	This value represents the maximum cumulative time, in milliseconds, that Cisco IPICS attempts to contact the dial engine. This value prevents the initialEngineFaliureReattemptDuration value from incrementing to infinity, which can cause the dial engine to become unusable. If Cisco IPICS cannot contact the dial engine within the specified time, Cisco IPICS stops the external notification and reports the error in the ipics.log file.
maxDialRetryCount	This value represents the maximum number of times that Cisco IPICS attempts to resend a notification action to a user if the initial attempt does not succeed (for example, if a phone was busy or did not answer).
maxWaitForAcquiring DialEngine	This value represents the maximum time, in milliseconds, that the primary dial engine waits before stopping an external notification if no dedicated dial engines are available.
phoneDialReadTimeout	This value represents the maximum timeout value, in milliseconds, for the dedicated dial engine to respond to a user dial request from the primary dial engine. If the dedicated dial engine does not respond to the primary dial engine within the specified time, the notification action stops and Cisco IPICS reports the error in the ipics.log file.

Table B-3 New Configurable Parameters in dedicated-dial-engines.xml File (continued)

Value	Description
promptUploadRead Timeout	This value represents the maximum timeout value, in milliseconds, for the dedicated dial engine to completely upload media (for example, a .wav file) from the primary dial engine. If the dedicated dial engine does not upload the media within the specified time, the notification action stops and Cisco IPICS reports the error in the ipics.log file.
redialPeriod	This value represents the time, in milliseconds, that Cisco IPICS waits to resend a notification action to a user if the initial attempt does not succeed.

APPENDIX C

Configuring System Event E-Mail Notifications

This appendix describes system event e-mail notifications and how to enable or disable them, and includes the following sections:

- Understanding System Event E-Mail Notifications, page C-1
- Enabling System Event E-Mail Notifications, page C-1
- Disabling System Event E-Mail Notifications, page C-2
- Changing System Event Trigger Values, page C-3

Understanding System Event E-Mail Notifications

The system administrator can log in to the Administration Console to access major system event information. However, the system administrator should be notified when major system events occur, even when not logged in to the Administration Console. You can configure the IPICS server to send system event notifications to the system administrator when any of the following major system events occur:

- The 1 minute load average exceeds 5
- The 5 minute load average exceeds 3
- Memory usage exceeds 75%
- User CPU usage exceeds 70%
- System CPU usage exceeds 40%
- I/O wait exceeds 40%
- The node manager process starts or stops
- The server HA state changes (active/standby)
- Any partition is more than 90% full, except for the /documents partition which sends notifications after it is 75% full.

Enabling System Event E-Mail Notifications

By default, the IPICS server does not send system event e-mail notifications to the system administrator. To enable system event e-mail notifications, perform the following procedure.

Before You Begin

Collect the following information that you must supply when configuring system event e-mail notifications:

- The hostname or IP address of the Simple Mail Transfer Protocol (SMTP) server that is to be used for sending the notifications.
- The e-mail address or mailing-list alias of the system administrators who are to receive the notifications,

Procedure

Step 1 Log in to the IPICS server bash shell using the root account.

Step 2 At the root prompt, run the **/opt/cisco/ipics/bin/setup_monit_alerts** script.

Step 3 Enter the the IP address or hostname of the SMTP e-mail server.

Step 4 Enter the e-mail address for the system administrator.

The system applies the configuration settings and reinitializes the monit daemon.

The following example configures the IPICS server to send system event e-mail notifications to the SysAdmin@cisco.com e-mail account using the email.cisco.com STMP server.

```
[root]# /opt/cisco/ipics/bin/setup_monit_alerts
Enter the SMTP e-mail server host name: email.cisco.com
Enter the e-mail address to send system alerts to: SysAdmin@cisco.com
Reinitializing monit daemon

Applying changes to HA partner...
Welcome to Cisco IPICS 4.5(1)
building file list ... done

sent 78 bytes received 20 bytes 196.00 bytes/sec
total size is 11131 speedup is 113.58
Welcome to Cisco IPICS 4.5(1)
Reinitializing monit daemon
```

Disabling System Event E-Mail Notifications

To disable the IPICS server from sending system event e-mail notifications, perform the following procedure.

Procedure

Step 1 Log in to the IPICS server bash shell using the root account.

Step 2 Enter the **rm -f /etc/monit.d/email.monitrc /etc/monit.d/alerts.monitrc** command to delete the email.monitrc and alerts.monitrc files.

Step 3 Enter the **monit reload** command to reinitialize the monit daemon.

The following example disables the IPICS server from sending system event e-mail notifications:

```
[root]# rm -f /etc/monit.d/email.monitrc /etc/monit.d/alerts.monitrc
[root]# monit reload
```

What to do Next

If you want to re-enable system event e-mail notifications, run the **/opt/cisco/ipics/bin/setup_monit_alerts** script to regenerate the deleted files (email.monitrc and alerts.monitrc). For more information, see the "Enabling System Event E-Mail Notifications" section.

Changing System Event Trigger Values

You can change the values at which system events are triggered. This allows you to adjust the sensitivity for system events and, therefore, adjust the number of system event notifications that you will receive. For example, if your system is configured to trigger an event when CPU usage is greater than 75%, you can do either of the following:

- Decrease the CPU usage value (for example, 65%) to make the system event more sensitive, which will result in more system event notifications being generated and sent.
- Increase the CPU usage value (for example, 85%) to make the system event less sensitive, which will result in fewer system event notifications being generated and sent.

Perform the following procedure to change system event trigger values:

Before you begin

You need the following information to complete the procedure:

- Hostname or IP address of the IPICS server
- IPICS server bash shell root credentials

Procedure

Step 1 Log in to the IPICS server bash shell using the root account.

Step 2 Enter the **vi /etc/monit.d/alerts.monitrc** command to open the alerts.monitrc file:

The VI editor opens and displays the contents of the alerts.monitrc file in command mode. The alerts.monitrc file contains a list of the system events and trigger values. For example, the list might look something like this:

```
check system localhost
    if loadavg (1min)     >   5 then alert
    if loadavg (5min)     >   3 then alert
    if memory usage       > 75% then alert
    if cpu usage (user)   > 90% then alert
    if cpu usage (system) > 40% then alert
    if cpu usage (wait)   > 40% then alert
```

Step 3 Enter insert mode and change one or more of the system event trigger values.

Step 4 Press the **ESC** key to exit insert mode.

The VI editor enters command mode.

Step 5 Enter **:q** to save the updated alerts.monitrc file and exit the VI editor.

Step 6 Enter the **monit reload** command to reinitialize the monit daemon.

Step 7 Enter the **monit status** command to verify your changes.

APPENDIX D

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 Communications Manager or for Cisco Unified Communications Manager Express. In addition, users in a deployment that includes Cisco Unified Communications Manager must subscribe to the Cisco IPICS service by using the Cisco Unified Communications Manager User Options application.

The total number of Cisco Unified IP Phones, LMR and multicast ports, IDC 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 2-63.

This appendix includes the following topics:

- Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager, page D-1
- Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager Express, page D-3
- Subscribing to the Cisco IPICS Service, page D-3
- Moving the Logout Softkey Location on a Cisco Unified IP Phone, page D-3
- Using the Cisco IPICS Service on a Cisco Unified IP Phone, page D-4

Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager

This section describes how to configure the Cisco IPICS service in Cisco Unified Communications Manager. After you configure Cisco IPICS as an available service, IP phone users can subscribe to the service by using the Cisco Unified Communications Manager 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 Communications Manager Administration and about setting up phone services, see the Cisco Unified IP Phone Services configuration information in *Cisco Unified Communications Manager Administration Guide* for your Cisco Unified Communications Manager version.

You can configure whether the Cisco IPICS service requires users to log in before accessing the service from a Cisco Unified IP Phone. If there are users who you do not want to require to log on, you can configure a separate service that bypasses the log in for each of these users.

To configure the Cisco IPICS service as an available service in Cisco Unified Communications Manager, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, take one of these actions:

- For Cisco Unified CallManager 3.x or 4.x—Choose **Feature > Cisco IP Phone Services**.
- For Cisco Unified Communications Manager 5.x or later—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 Communications Manager 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 URL of the Cisco IPICS service in either of the following format. If you are using the Cisco IPICS high availability feature, enter the URL twice, once for the primary server and once for the secondary server.

- If you want to require users to log in before accessing the service, enter:

  http://<*ipics server IP address*>**/ipics_server/servlet/ IPPhoneManager**

  Replace *ipics server IP address* with the IP address of the Cisco IPICS server.

- If you do not want to require a user to log in before accessing the service, enter the following for the user:

  http://<*ipics server IP address*>**/ipics_server/servlet/ IPPhoneManager?method=LOGIN&user=**<*userID*>**&PIN=**<*pin*>

  Replace *ipics server IP address* with the IP address of the Cisco IPICS server, userID with the digit ID of the user, and pin with the digit password (PIN) of the user who will not need to log in.

Step 3 (Optional) If you are configuring a service for a user who does not have to log in to use it, configure these parameters in the Service Parameter Information area:

- method—Set this parameter to LOGIN and designate it as required.
- user—Set this parameter to the Cisco IPICS digit ID of the user and designate it as required.
- PIN—Set this parameter to the Cisco IPICS digit password (PIN) of the user and designate it as required.

Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager Express

To configure Cisco IPICS as an available service in Cisco Unified Communications Manager Express, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IOS router that runs Cisco Unified Communications Manager Express.

Step 2 Type this command to access the enable prompt:

```
Router> enable
```

Step 3 Enter the following commands to provision a router that is running Cisco Unified Communications Manager Express with the URL of the Cisco IPICS IP Phone service so that Cisco Unified IP Phones can function as Cisco IPICS PTT devices:

```
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.

Moving the Logout Softkey Location on a Cisco Unified IP Phone

When a Cisco Unified IP Phone user finishes using the Cisco IPICS service, the user presses the **Logout** softkey on the phone. By default, a user must press the **Back** softkey after exiting a channel or VTG to access the **Logout** softkey. However, you can configure a phone to display the **Logout** softkey when a user is connected to a channel or VTG. To do so, add the following parameter to the Cisco IPICS Service URL:

buttonLayout=logoutOnPTT

Note If you configure this parameter, a user may need to press the **More** softkey on some phone models to see **Logout**.

Subscribing to the Cisco IPICS Service

Cisco Unified IP Phone users in a deployment that includes Cisco Unified Communications Manager 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 Communications Manager Express. Cisco Unified Communications Manager 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 Communications Manager" section on page D-1.

To subscribe to the Cisco IPICS service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco Unified Communications Manager User Options web site.

For more information about accessing the Cisco Unified Communications Manager User Options web site, and for additional information about the phone features for your phone model, see the Cisco Unified IP Phone documentation.

Step 2 From the Cisco Unified Communications Manager User Options Menu, choose your device type or profile from the drop-down list.

Step 3 From the Cisco Unified Communications Manager User Options Menu, choose **Configure your Cisco IP Phone Services**.

Cisco Unified Communications Manager 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 Communications Manager 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 Unified IP Phone, the prerequisites that are described in Table D-1 must be met:

Table D-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 Communications Manager" section on page D-1 or the "Configuring Cisco IPICS as a Phone Service for Cisco Unified Communications Manager Express" section on page D-3.

Table D-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 4-2. 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 3-9.
Users in a Cisco Unified Communications Manager environment must subscribe to the Cisco IPICS service.	See the "Subscribing to the Cisco IPICS Service" section on page D-3.

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.
- The Cisco IPICS operator configures the digit ID and digit password (PIN) that are used to log into the Cisco IPICS service, or configures the system so that these login credentials are not required. For more information, see the "Managing Dial Login Information for a User" section on page 3-9.
- The channels and VTGs that display in the menu are those that are available for a user when the Cisco IPICS service starts. To view an updated list of channels, press the **Update** softkey. The Cisco IPICS server does not automatically download channel or VTG information to the phone.
- 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 3-9.) Channels that do not meet this requirement do not display on the phone.
- A Cisco Unified IP Phone receives a list that is 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.
- By default, a phone automatically logs out of the Cisco IPICS service after 30 minutes of inactivity. (You can configure this setting in the Administration > Options window. For more information, see the "Managing Cisco IPICS Options" section on page 2-77.)
- 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 user can send and receive audio on all of the phones.
- 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, see the Cisco Unified IP Phone documentation.

- You can customize the softkeys on the Cisco Unified Wireless IP Phone 7920/7921 to enable direct access to the Services menu. For details, see the Cisco Unified Communications Manager documentation.
- 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. See your Cisco IP Phone documentation for specific instructions.

Step 2 Choose the **Cisco IPICS** service, then press the **Select** softkey.

If the Cisco IPICS service is configured to prompt for login credentials, continue to Step 3.

If the Cisco IPICS service is not configured to prompt for login credentials and if more than one channel or VTG is assigned to you and activated for your use, Cisco IPICS displays the list of these channels and VTGs. In this case, go to Step 4.

If the Cisco IPICS service is not configured to prompt for login credentials and if only one channel or VTG is assigned to you and activated for your use, the channel or VTG becomes active automatically. In this case, go to Step 5.

Step 3 Enter your digit ID and digit password (PIN); then, press the **Submit** softkey.

If more than one channel or VTG is assigned to you and activated for your use, Cisco IPICS displays the list of these channels and VTGs. In this case, continue to Step 4.

If only one channel or VTG is assigned to you and activated for your use, it becomes active automatically. In this case, go to Step 5.

Step 4 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 5 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 6 When you are done talking, release the **PTT** softkey to return to listen-only mode.

Step 7 When you are done using the Cisco IPICS service, take one of these actions:

- If the **Logout** softkey appears, press that key. On some phone models, you must press the **More** softkey to see **Logout**.
- Press the **Back** softkey and then press the **Logout** softkey.

APPENDIX E

Generating SSL Certificates

SSL certificates on a Cisco IPICS server expire after three years and must be replaced. Complete the following instructions to manually generate SSL certificates on a Cisco IPICS server.

Caution This procedure automatically restarts the Cisco IPICS server software. Perform this procedure only when restarting the Cisco IPICS server software will not interrupt critical operations.

Note If the Cisco IPICS servers are configured with high availability (HA), you must temporarily disable HA before you generate the SSL certificates. You must generate the certificates on both the primary and standby servers, and then reenable HA before installing the certificates on the iPhone.

To generate SSL certificates, perform the following procedure.

Procedure

Step 1 (HA configurations only) Unconfigure HA on the active Cisco IPICS server as described in the "Unconfiguring HA" section on page 10-6.

Step 2 At the end of the "Unconfiguring HA" section on page 10-6, complete the optional steps to delete the HA security certificates.

Step 3 Use a secure shell (SSH) client to log in to the primary Cisco IPICS server using the root account.

Step 4 Enter these commands to generate new SSL certificates:

```
[root]# cd /opt/cisco/ipics/security
[root]# sudo -u ipicsadmin ./security-manager unsetup
[root]# sudo -u ipicsadmin ./security-manager setup
[root]# service ipics start
```

Step 5 Wait a few minutes for the Cisco IPICS server software to restart.

Step 6 Log in to the Cisco IPICS administration console again and verify that the server operates correctly.

Note If your web browser displays an error regarding the certificates, go to the browser certificate management page and delete the old trusted certificates.

Step 7 (HA configurations only) Generate SSL certificates for the secondary Cisco IPICS server:

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

b. Repeat Step 3 through Step 5 to generate SSL certificates for the secondary Cisco IPICS server.

Step 8 Log in to the Cisco IPICS Administration Console and reconfigure HA.

See the "Configuring Cisco IPICS Servers for HA" section on page 10-3 for instructions. Be sure to establish trust between the HA servers, as described in Step 8.

APPENDIX F

Multicast Recording

This appendix describes multicast recording and includes the following sections:

- Overview, page F-1
- Voice Recording, page F-1
- Talker ID, page F-1
- Radio Metadata, page F-2
- Telephone, page F-2

Overview

All IPICS voice traffic that pertains to interoperability is represented by a channel, radio or VTG, each of which are configured with a multicast address. All voice traffic appears on its respective multicast address, even if a participant has joined via a unicast session (SIP). Furthermore, all voice traffic appears in the form of Real Time Protocol (RTP) packets using G.711 or G.729 codecs.

Voice Recording

A third party voice recording system can be used to record voice traffic on each multicast address. It can either be configured to continuously record, or be triggered to record by the presence of RTP packets. The recording system must manage the timestamp, datestamp, and duration information. Some recording systems are capable of detecting other external events, such as ring, off-hook, and contact closure. These systems should be configured so that activities start when those events happen.

Talker ID

Media originating from IDCs, serially controlled radios and ISSI gateways may be associated with a talker ID. This metadata can be captured by a recording system for each session. For the duration of the call, talker ID packets appear periodically as RTP packets with payload type 110. A talker ID packet is in the following format:

```
TalkerID
UID:<Integer>
DisplayName:<String>
ChannelID:<Integer>
ChannelName:<String>
```

```
SrcId:<SSRC>
UserID:<String>
```

The UserId field is the login ID of the IDC, when the IDC is transmitting. The end of a talk spurt is marked with an “End-TalkerID” packet. Talker ID packets originating from the LMRG or ISSIG are marked with the UserID field only. In this case it will be the ID of the transmitting radio. Note that there is no alias for radio talker ID. Any aliasing must be done by the recording system via a look-up table if necessary.

Radio Metadata

For serial controlled donor radios and ISSI gateways, certain metadata associated with the talk spurt is available during the call. This is represented within a RTP packet of payload type 109. The packet payload is in the following format:

```
RcsMessageConnectionStatusResponse
channelSelector:<String>
callType:[CHANNEL_OR_TALKGROU_CALL|PRIVATE_CALL|GROUP_CALL]
callState:[RX|TX|IDLE]
talkerId:<String>
```

Other data related to the radio or gateway is also present in this packet and is not relevant to the media. The recording system must be configured to gather these radio control packets.

Telephone

Metadata related telephone related talk sessions are available in IPICS/IPPE activity logs and Call Manager logs. The recording system must correlate RTP sessions with these logs. For detailed telephony audio recording capabilities, the recording system can integrate directly with Cisco Unified Communication Manager (CUCM).

APPENDIX G

Frequently Asked Questions

This appendix contains frequently asked questions and answers relating to the Cisco IPICS server and its various components and includes the following sections:

- Cisco IPICS Server and Administration Console, page G-1
- Cisco IPICS Licenses, page G-3
- RMS Components, page G-4
- Locations, page G-5
- Resources, page G-5
- Cisco IPICS Policy Engine, page G-6
- Push-to-talk Channels, page G-10
- Radio Communications, page G-11
- VTGs, page G-12
- Ops Views, page G-13
- Serviceability, page G-14
- Cisco Unified IP Phones, page G-14

Cisco IPICS Server and Administration Console

Q. Can I specify a timeout period for my Cisco IPICS Administration Console browser session?

A. Yes, you can specify a browser session timeout period by changing the value in the Cisco IPICS Session Timeout Period setting in the **Administration > Options** window. The default specifies 30 minutes. The range of values that you can use includes zero to 99999. (A value of zero specifies that the browser never times out.)

For more information about Cisco IPICS options, see the "Managing Cisco IPICS Options" section on page 2-77.

Q. Can I use pop-up blocker software with Cisco IPICS?

A. The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have 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 administrative tasks in Cisco IPICS, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.

Q. Do windows in the Cisco IPICS Administration Console update automatically?

A. No. 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, you can update your browser window and retry the operation.

Q. How do I update my browser window?

A. 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 or update the window.

Note Cisco IPICS does not support the use of the browser Refresh button to refresh a window in the Administration Console.

Q. What does an asterisk (*) denote in the Administration Console graphical user interface (GUI)?

A. An asterisk in the GUI indicates a required field.

Q. What do the Cisco IPICS roles define and to whom are they assigned?

A. Each Cisco IPICS user is assigned one or more roles. Roles define the Cisco IPICS features that a user can access and the functions that a user can perform. The following list describes the roles that are available in Cisco IPICS:

- User—Provides the ability to maintain personal information, download the IDC client application, specify communication preferences that are used to configure audio devices, activate a policy, and view associated policies.

Note Every Cisco user is assigned the User role, although the users may also have additional roles assigned to them.

- System administrator—Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. Also creates, edits, or deletes ops views, manages Cisco IPICS licenses and IDC versions, performs activities relating to the dial engine, activates policies, views certain policies, and monitors the status of the system and its users via the activity log files and the Dashboard.
- Ops view administrator—Provides 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.
- Operator—Responsible for setting up and managing users and user groups, granting access to Cisco IPICS and the IDC, assigning user channels, roles and ops views, and creating and managing policies.
- Dispatcher—Responsible for setting up inactive VTGs, activating VTGs to begin conferences, and adding or removing participants in inactive and active VTGs. Creates and manages policies. Also monitors active VTGs and events and can mute and unmute IDC users, as necessary.
- All—Equivalent to being assigned each of the other Cisco IPICS roles.

Q. When should I back up my database?

A. For optimum performance, Cisco recommends that you back up your database during periods of low activity or other off-peak hours. If you perform a back up during periods of high activity, the length of time that it takes to complete this operation can be significantly increased. For more information, see the "Backing up the Cisco IPICS Server Database" section on page 11-2.

Q. Can I restore data from one server to another?

A. You can restore data from one server to another only if both servers are running the same version of Cisco IPICS software. If the software versions of the two servers differ, the database schema might not be the same; therefore, the restore operation could fail, or you could encounter unpredictable errors when you perform tasks in the Administration Console. For more information, see the "Restoring Data from a Database Backup" section on page 11-9.

Cisco IPICS Licenses

Q. How are license ports and DS0 loopback port resources counted in Cisco IPICS?

A. To use the Cisco IPICS solution, you must first upload and install one or more licenses. Cisco IPICS supports the following licenses:

- LMR port license—Cisco IPICS uses this license when PTT channels are enabled.

Cisco IPICS also uses a single LMR license when a radio channel is enabled. However, when subsequent radio channels are configured within the radio, those channels do not use separate licenses. Cisco IPICS uses only one LMR license per enabled radio channel.

- Multicast port license—Cisco IPICS uses a single multicast port license when a VTG is activated.
- IDC users license—Cisco IPICS uses a single IDC license each time that an IDC user logs in to the system. If an IDC user logs in multiple times, Cisco IPICS uses a license when a channel is enabled.
- Cisco Unified IP Phone users license—Cisco IPICS uses a single Cisco Unified IP Phone license each time that a Cisco Unified IP Phone user (IDC xml client) logs in to the system.
- Dial user license—Cisco IPICS uses a single PSTN (dial user) license in each of the following scenarios:

  - Cisco IPICS uses one license for an active inbound call

  - Cisco IPICS uses one license for an active outbound call

Cisco IPICS uses a single DS0 loopback pair in the following scenarios:

  - For each remote channel on an IDC

  - 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

- Ops view license—Cisco IPICS uses a single ops view license for each configured ops view.
- Cisco IPICS base server license—A Cisco IPICS base server license displays as enabled or disabled in the **Administration > License Management** window to indicate whether the license is activated.
- Policy engine base license—A policy engine base license displays as enabled or disabled in the **Administration > License Management** window to indicate whether the policy engine is activated.

Q. Why would a VTG suddenly become active or inactive?

A. If a VTG unexpectedly becomes active or inactive, the change in status could be caused by a policy that has executed and forced a change to the VTG state. Make sure that you have sufficient licenses in Cisco IPICS to avoid a sudden change in status.

RMS Components

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, Cisco IPICS allows you to configure more than one RMS in the same location.

Q. If I have more than one RMS component configured in the server, do all RMS components need to be configured alike?

A. If you have more than one RMS component configured in the server, make sure that you configure each RMS according to the instructions that are documented in Appendix A, "Configuring the Cisco IPICS RMS Component." Be aware that Cisco IPICS provides support only for RMS components that are configured as described in that document.

Q. How do I configure an RMS router for T1 or E1 connectivity?

A. When you configure an RMS router for T1 or E1 connectivity, there are specific guidelines that you must follow to ensure successful operation of your RMS. For these details, see Appendix A, "Configuring the Cisco IPICS RMS Component."

Q. Must timeslot 24 (for a T1 controller) and timeslot 31 (for an E1 controller) always be configured?

A. Yes, timeslot 24 (for a T1 controller) and timeslot 31 (for an E1 controller) must always be configured even if you a fractional T1 or E1 controller. Typically, a T1 controller supports 24 ds0s and an E1 controller supports 30 ds0s, but your controller may support fewer ds0s, depending on the number of digital signal processors (DSPs). For more detailed information, see the Appendix A, "Configuring the Cisco IPICS RMS Component."

Q. How do I select RMS IP addresses?

A. When you select the IP addresses for the RMS, there are specific guidelines that you must follow and interfaces that you must configure to ensure successful interoperability with Cisco IPICS components. For the details about RMS configuration, see Appendix A, "Configuring the Cisco IPICS RMS Component."

Q. Must the IP addresses that I configure for my interfaces be routable?

A. Yes, 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 IDC PTT button to the time that the media is established between the remote IDC 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. For detailed information, see Appendix A, "Configuring the Cisco IPICS RMS Component."

Q. How do I configure an inbound dial peer in the RMS?

A. When you configure an inbound dial peer in the RMS, there are specific values that you should enter. Although Cisco IOS supports other values for some of the fields in the configuration, Cisco recommends that you configure the values exactly as they are documented in Appendix A, "Configuring the Cisco IPICS RMS Component."

Locations

Q. Why are some channels designated as remote?

A. A channel is designated as remote when it is in a different multicast domain than the user who is accessing it. In this case, the channel uses the resources of the RMS to create a SIP-based connection to the Cisco IPICS server.

Q. What does the remote designation mean for an IDC location?

A. The remote location is available only to IDC users. When an IDC user chooses **REMOTE** from the Location drop-down list, 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 2-27.

Q. If I have only 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 is not 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 no 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 2-27.

Resources

Q. How many resources (voice ports, multicast addresses) do I need in Cisco IPICS?

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 resources 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

Cisco IPICS Policy Engine

Q. How do I access the telephony user interface (TUI)?

A. You can access the TUI from a touch-tone telephone. From the phone, you can access the TUI in the following 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 7, "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 group, 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.

Q. Are there any guidelines that I should follow when using the TUI?

A. There are some usage guidelines that you should be aware of when using the TUI. A few of these guidelines are described in the following list:

- 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.
- After you authenticate, the system announces the available menu options, such as joining a group, invoking a policy, or accessing the system menu.
- A menu times out if you do not respond within the predefined allowable period of time. In most instances, this period of time is three seconds and includes a maximum retry limit of three. 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.
- 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 group. (As the call is being dialed out, the system does not play any sounds.)
- 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 group, press 1. Then, you can press 1 to select an assigned group to join by spelling out the group name, or press 2 to listen to the list of assigned groups and then selecting from that list. (If you know the name of the group that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available groups.) To confirm your selection, press 1. To cancel your selection, 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 invoke, 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 selection, press 2. To return to the previous menu, press *.

For more information and for a complete list of TUI guidelines, see the "Guidelines for using the TUI" section on page 6-21.

Q. Can an internal party dial the Cisco IPICS dial engine telephony user interface (TUI)?

A. Yes, an internal party can dial the dial engine TUI as long as you have configured a SIP provider in your network.

The Cisco IPICS policy engine requires that a SIP provider be configured in your network to use the dial-in, dial-out, or IDC direct dial features. A SIP provider handles calls to and from the policy engine.

You must use Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider and enter the required configuration information, as described in the "Configuring SIP" section on page 8-24.

For information about the compatible hardware and software versions that are supported for use with Cisco IPICS, see *Cisco IPICS Compatibility Matrix*.

If the SIP provider is a Cisco Unified Communications Manager, then you must configure a route pattern for the SIP trunk.

If the SIP provider is a supported Cisco IOS gateway, you must make sure that you configure a dial peer that routes the call to Cisco IPICS.

Note The dial number (DN) that you want to use to allow dial-in access must be assigned to an ops view (typically the System ops view). For more information, see the "Performing Ops Views Tasks" section on page 7-11.

Q. Which codecs do the dial engine support?

A. The dial engine supports only G.711 u-law. For more information, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

Q. What is an action as it relates to a policy?

A. 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 the following list:

- Invite to VTG—This action is an invitation policy type that calls designated users and invites them to join a VTG by responding to TUI prompts. This action can be activated only through the TUI when you break out of an existing VTG.
- Activate VTG—This action is a multi-purpose policy type that activates designated, preconfigured VTGs.
- Notification—This action is a multi-purpose policy type that contacts designated recipients according to notification instructions that you specify.
- VTG Add Participants—This action is a multi-purpose policy type that adds the designated participants to the designated VTG.
- Dial Out—This action is a multi-purpose policy type that calls designated users according to their configured dial preferences to invite them to join the designated VTG.

For more information about policy actions, see the "Managing Actions for a Policy" section on page 6-5.

Q. Which types of notification actions can I use with the Cisco IPICS policy notification feature?

A. The Cisco IPICS policy notification features includes the following notification action types:

- Email Notification—This type of notification sends a message that you enter to the e-mail, short message service (SMS), and pager addresses that are configured as communication preferences for each user that you designate as a recipient.
- IP Phone Notification—This type of notification displays a designated message on supported Cisco Unified IP Phones.
- Dial Notification—This type of notification calls out to designated users and plays the selected prompt or sends a message to the Cisco Unified IP Phones of the designated users and plays automatically on the speaker of the phone.
- Talk Group Notification—This type of notification plays out the selected prompt to all users in the VTG.

Q. What types of messages can I send when I configure a new policy notification action?

A. The policy notification action includes the following message options:

- Email—This notification option sends a message that you enter to the e-mail, SMS, and pager addresses that are configured as communication preferences for each user that you designate as a recipient.
- IP Phone Text—This notification option displays a designated message on supported Cisco Unified IP Phone models. The telephone numbers of each phone must be configured as a dial preference for the associated user.
- Dial—The policy engine executes a Dial notification action as follows:

  - If the Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured in the SIP Configuration menu, the system checks whether each designated user has an associated Cisco Unified IP Phone that is configured in Cisco Unified Communications Manager. If a user does have an associated phone, the system plays the designated message on the speaker of the phone.

  - If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured but a user does not have an associated Cisco Unified IP Phone, or if the phone of a user is busy, the system calls the user as specified in the communication preferences for the user and plays the designated message.

  - If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are not configured, the system calls the user as specified in the dial preferences for the user and plays the designated message.
- Talk Group—This notification option plays the selected prompt to all participants in the selected VTG.
- Dial Engine Script—This notification option executes the designated dial engine script once for each designated recipient.

For more detailed information about notification actions, see Chapter 6, “Using the Cisco IPICS Policy Engine.”

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, 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 Communications Preferences tab 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 7-18.

Q. Can a dispatcher enter specific notification information when sending a notification to VTG participants?

A. Yes, Cisco IPICS includes the capability for the dispatcher to enter specific subject and body text when sending notifications to participants in a VTG from the **VTG Management > Virtual Talk Groups** window. For more information, see the "Notifying and Dialing Out to Participants, and Setting IDC Attributes in an Active VTG" section on page 5-19.

Q. Can a notification action be sent to recipients who are not configured as users in Cisco IPICS?

A. Yes, the Cisco IPICS policy engine includes an external notification action which sends notification actions to designated recipients who are not configured as Cisco IPICS users and provides them with information that you specify.

The external notification feature is not configurable via the Cisco IPICS Administration Console. Instead, you must configure one or more dedicated dial engines, designate a list of recipients, and designate a message file to play to the recipients.

To configure a a Cisco IPICS server as a primary dial engine, you edit a .xml configuration file on that server and set the dialEngine sub-element attributes for each dedicated dial engine, including the primary dial engine.

A recipient list is a .xml file that contains a list of each person who should receive the external notification message.

Note To invoke an external notification that contacts these recipients, you must know the URL of the server on which the recipient list resides.

A message file is a .wav file in pulse code modulation (PCM) or CCITT u-Law format that contains the recorded message to play to recipients. Cisco recommends that the message be no longer than 90 seconds.

Note To invoke an external notification that plays this message, you must know the URL of the server on which the message file resides.

The external notification action performs the following actions:

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

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

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

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

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

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

  For more information, see Appendix B, "Using Cisco IPICS for External Notifications."

Q. When Cisco IPICS dials out to users, does the 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 entry of an incorrect digit ID or PIN and/or the occurrence of a timeout because 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 6-17.

Q. Is there a way to export and track the history of executing and executed policies in Cisco IPICS?

A. Yes, Cisco IPICS includes the ability to export executing and executed policy history to a Microsoft Excel format that you can download. To download the execution status history, navigate to the **Policy Management > Execution Status** window and click the **Download Execution Status** button. You can either open the file or save the file to a location of your choice and then open it by using Microsoft Excel. For more information, "Viewing Information about Executing or Executed Policies" section on page 6-17.

Q. How do you integrate the dial engine into an existing network that runs an earlier version of Cisco Unified Communications Manager and does not have native SIP trunk support?

A. This integration can be accomplished by using a Cisco IOS router that runs Cisco Unified Communications Manager Express as the SIP provider and configuring an H.323 Intercluster Trunk (ICT) between the Cisco Unified Communications Manager and the SIP provider. For detailed information, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine,"and the *Solution Reference Network Design (SRND)* (latest version).

Q. Is there any special SIP configuration required when executing policies that use the IP Phone Text Notification action or the Dial Notification action to send a message to a Cisco Unified IP Phone?

A. Yes, you must enter configuration information for the Cisco Unified Communications Manager in the **Dial Engine > SIP Configuration** window. For detailed information, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

Push-to-talk Channels

Q. What is a push-to-talk (PTT) channel?

A. A PTT channel, also referred to as a *channel*, is a communications path that allows users to communicate with each other. In Cisco IPICS, a channel defines and describes the specific content stream of the channel regardless of the source of that content.

PTT channels appear on the IDC and on Cisco Unified IP Phones. For more information about the IDC, see *IPICS Dispatch Console User Guide* for this release.

Note In Cisco IPICS, a channel can also refer to a radio control interface (radio or radio channel), which also has an audio stream.

Q. Can a channel be assigned to multiple locations in Cisco IPICS?

A. Yes. Channels achieve media connectivity by being mapped to a multicast address and port in a location. When a channel is assigned to multiple locations, it can have more than one media connection. The media connection count in the **Serviceability > Dashboard** window reflects the total number of media connections. For more information, see the "Viewing the Information in the Dashboard Window" section on page 12-1.

Q. Are there any guidelines that I should follow when selecting multicast IP addresses that are to be used for channels?

A. Yes. 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, "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-36.

Note Two channels that are in the same location cannot have the same multicast address. For more information, see the "Managing Locations" section on page 2-27.

Radio Communications

Q. What is tone control?

A. Tone control (also referred to as *Tone Remote Control* (TRC)) refers to the use of inband tone sequences to control a radio that is connected to an LMR gateway (typically a base station). In Cisco IPICS, you can use tone control to perform various functions, such as modifying or tuning a channel to a different radio frequency (RF), changing the transmit power level, and enabling or disabling radio built-in encryption. TRC uses well-defined audio sounds (also referred to as *tones*) to change the behavior of a device. A tone-keyed radio system requires that a specific tone be present on the incoming analog (e-lead) port. If this tone is not present, the radio does not transmit audio.

For more information, see Chapter 9, "Managing Radios and Radio Descriptors."

Q. What are tone sequences?

A. Each radio channel that you configure in the Cisco IPICS Administration Console represents a physical radio that you can configure with one or more tone sequences. Tone sequences control various tones and functionality on the radio. Each tone sequence includes the frequency or frequencies, volume (power), duration, and other parameters that are necessary to generate a specific tone and invoke a specific action on the radio.

For more information, see Chapter 9, "Managing Radios and Radio Descriptors."

Q. How can tone-controlled radios be used with Cisco IPICS?

A. Cisco IPICS provides support for tone-controlled radios by enabling the definition of radio channels in the Cisco IPICS server configuration. The IDC sends RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis. At the LMR gateway, these packets get converted into audible tones via the configured ear and mouth (E&M) interface to the physical radio to provide tone control for radios.

For more information, see Chapter 9, "Managing Radios and Radio Descriptors."

Q. What are stateful and momentary control sequences on a tone-controlled radio?

A. Cisco IPICS enables the following controls on a tone-controlled radio:

- Stateful controls—Control functions can display on the IDC as single channel selector buttons or as stateful control sequences. Stateful control sequences are comprised of multiple states, where each state displays as a separate channel selector (tone control) button on the IDC. An example of a stateful control sequence is the power level of a radio.
- Momentary controls—Momentary tones begin to play when the IDC user presses the associated button. After the user presses a momentary control button, the button appears to be pressed momentarily before it appears raised again.

Q. What are descriptor files and how are they used in Cisco IPICS?

A. There are two types of descriptor files in Cisco IPICS:

- Radio descriptor files—Radio descriptors are .xml files that contain commands that are used to control functions on a radio. These files contain channel selectors that are used to change the frequency on a radio and control functions that allow for stateful and momentary controls of the radio.
- Tone descriptor files—Tone descriptors are .xml files that define commands and over-the-air signals that can be associated to one or more Cisco IPICS channels. Commands can be referenced by any radio descriptor and signals can be associated to any channel.

See the "Managing Radio Descriptors" section on page 9-21 for more information.

VTGs

Q. What is a VTG?

A. A VTG, or virtual talk group, enables multiple participants on various channels to communicate by using a single multicast address. Participants in a VTG can include users, user groups, channels (PTT and radio), channel groups, and other VTGs. An active VTG is a VTG in which all the participants have live connections with each other. For more information about VTGs, see Chapter 5, "Performing Cisco IPICS Dispatcher Tasks."

Q. Can more than one dispatcher log in to Cisco IPICS at the same time?

A. Yes, Cisco IPICS allows more than one dispatcher to log in to the system at a time. This scenario 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 ops views feature provides a mechanism to support this scenario by segmenting views. With ops views, a dispatcher sees and can control only the VTG participants that have been assigned to the particular ops view to which the dispatcher also belongs.

Q. What is the difference between an inactive VTG and an active VTG?

A. An inactive VTG lets you create various arrangements of members (users, channels, and VTGs), without committing network resources or affecting VTGs that are in progress (active VTGs). A dispatcher can activate an inactive VTG at any time, which brings the VTG participants together into a live conference.

When you modify an inactive VTG, no changes occur in system resources or in the communication between participants until you activate that VTG. When you make changes to an active VTG, the original attributes of the VTG (inactive VTG) remain unchanged.

You can view information about any VTG by clicking the VTG name that displays in the **VTG Management > Virtual Talk Groups** window. Information about the VTG displays in a separate window.

For more information about inactive and active VTGs, see Chapter 5, "Performing Cisco IPICS Dispatcher Tasks."

Ops Views

Q. What is an ops view?

A. An ops view, or operational view, allows segmentation of resources that authorized Cisco IPICS users may see on the Cisco IPICS Administration Console. With ops views, you can organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other.

Note Ops views does not affect the way in which channels and VTGs display on the IDC or Cisco Unified IP Phones.

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 another operator user ID 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. For more detailed information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

Q. What is a SYSTEM ops view?

A. The SYSTEM ops view is an ops view that the Cisco IPICS server displays 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.

Q. Which Cisco IPICS roles are allowed to create new ops views?

A. Only a 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 **Administration > License Management** window in the Administration Console. For more information about viewing ops view ports, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

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 a user, the user has the ability to remove the associated resource but cannot modify it in any other way. For more information about ops views, see Chapter 7, "Configuring and Managing Cisco IPICS Operational Views."

Serviceability

Q. How can I view serviceability and diagnostic information in Cisco IPICS?

A. To view real-time serviceability and diagnostic system information in Cisco IPICS, you can navigate to the Serviceability drawer and the following windows:

- Dashboard—This window provides you with Cisco IPICS system and resource information. For more information, see the "Viewing the Information in the Dashboard Window" section on page 12-1.
- 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 additional diagnostic information. For more information, see the "Viewing Cisco IPICS Server Diagnostic Information" section on page 12-6.
- System Logs—This window displays logging information for Cisco IPICS. This information can be useful for troubleshooting or debugging your system. For more information, see the "Viewing the Cisco IPICS System Logs" section on page 12-9.

Cisco Unified IP Phones

Q. Can I specify a timeout period for a Cisco Unified IP Phone, so that the phone times out after a period of inactivity?

A. Yes, you can specify whether an IP phone times out after a configured period of inactivity, forcing the user to log in again, by changing the value in the Cisco Unified IP Phone Timeout Period setting in the **Administration > Options** window. For more detailed information about Cisco IPICS options, "Managing Cisco IPICS Options" section on page 2-77.

Q. Can I bypass the login for an IP phone user so that the user can more quickly access the Cisco IPICS service?

A. Yes. If there are users who you do not want to require to log in, you can configure a separate service, in Cisco Unified Communications Manager, that bypasses the log in for each of these IP phone users.

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

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

For detailed information, see Appendix D, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

Q. Is there a way to configure an IP phone to display the Logout softkey on the main display screen while users are connected to a channel or VTG?

A. Yes. On some model IP phones, you can add a special parameter to the Cisco IPICS Service URL configuration to enable the display of the Logout softkey while IP phone users are connected to a channel or VTG.

This setting allows the Logout softkey to display such that users do not need to press the **Back** softkey, after exiting a channel or VTG, to access it.

Note If you configure this parameter, a user may need to press the **More** softkey on some phone models to see **Logout**.

For more information, see Appendix D, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

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. Are there any guidelines that I should follow when using the Cisco IPICS service on a Cisco Unified IP Phone?

A. There are some usage guidelines that you should be aware of when using the Cisco IPICS service on a Cisco Unified IP Phones. A few of these guidelines are described in the following list:

- To obtain help with using the Cisco IPICS service on a Cisco Unified IP Phone, press the **Help** softkey.

The Cisco IPICS operator configures the digit ID and digit password (PIN) that are used to log into the Cisco IPICS service, or configures the system so that these login credentials are not required. For more information, see the "Managing Dial Login Information for a User" section on page 3-9.

- The channels and VTGs that display in the menu are those that are available for a user when the Cisco IPICS service starts. To view an updated list of channels, press the **Update** softkey. The Cisco IPICS server does not automatically download channel or VTG information to the phone.
- Channels that are 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 and for a complete list of usage guidelines, see Appendix D, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

GLOSSARY

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 IDC is enabled and activated, all of the IDC buttons are operational.

activating A state that becomes effective when you click the **Activate** button on the IDC. The Activate button appears highlighted while the other IDC 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 IDC. Click this button on the IDC 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 An audible tone, such as a siren, warble or chirp, that is used to attract the attention of a radio listener.

alert tone buttons Buttons on the IDC 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 Radio terminology that defines a call as beginning at the moment that you press the transmit key and concluding when you release the transmit key. The term “per call” implies that some form of control causes the radio to select a specific frequency before it transmits audio. Some radios may be configured to automatically return to a predefined RF channel when the call ends.

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. There are many different types of channels in Cisco IPICS, including direct dial, 2-way, VTGs, and radio channels. Channels can be dynamically or statically allocated. Channels may have one or more channel connections that define the source for the channel. *See* PTT channel.

channel capacity The maximum possible information transfer rate through a channel, subject to specified constraints.

channel connection One or more methods by which a content stream can be obtained. For instance, a particular channel may be found on several different multicast addresses in different locations and also on several different radios at different locations.

channel folder A logical grouping of channels

channel select check box Provides the ability to select or deselect the specified channel on the IDC 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 Communications Manager The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified Communications Manager 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 Unified Communications Manager Express Provides call processing for Cisco Unified IP Phones as part of a converged voice and data solution that is empowered by a Cisco router. Offers key system and small private branch exchange (PBX) capabilities available within Cisco IOS software.

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. For information on supported platforms and operating systems, see the IPICS compatibility matrix at http://www.cisco.com/en/US/products/ps6718/products_device_support_tables_list.html

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. An electrical signal that is used to signal when a radio is receiving traffic.

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.

discrete tone Any tone that is sent without any summed or added tone. For example, adding a function tone with a low level guard tone may impact the recognition of the function tone. Contrast with mixed tones.

dispatcher The Cisco IPICS dispatcher is responsible for setting up the VTGs, activating the VTGs to begin conferences, and adding and/or removing participants in inactive VTG and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute IDC 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.

DTMF dual tone multi-frequency. The signal to the phone company that you generate when you press keys on a telephone keypad. With DTMF, each key that you press on your phone (0 through 9, ‘*’ and ‘#’) generates two tones of specific frequencies; one tone is generated from a high frequency group of tones and the other from a low frequency group. Voice gateways often strip these inband tones and present them out-of-band in SIP, H.323, or other messages.

dynamic radio channel (dynamic control) The controls that are used to preset radio characteristics so that channels are available to clients.

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). As the analog interface between a radio and the LMR gateway, 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.

e-lead The ear portion of the E & M interface. The e-lead is the receive path of the LMR gateway.

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 is used in several different contexts. For example, transmission frequency (the band on which the radio sends signals) or the frequency of an audible signal measured in hertz (Hz). All tone control operations require audible tones that fall within a narrow band of a specific frequency and at a specific volume (amplitude).

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.

function tone A tone that follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. Function tones are often referred to as F1, F2, F3, and so on. *See* preamble and high level guard tone.

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.

guard tone The most common guard tones are the high level guard tone (HLGT) and the low level guard tone (LLGT). The HLGT is used to alert the radio that a function tone follows. The LLGT is used as a hold tone or keying tone. *See* tone keyed.

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.

HLGT high level guard done. Also known as awake tone. This tone is set at high volume and is usually the first tone in a preamble. It is used to alert the radio that another tone, usually a function tone, will follow. *See* guard tone.

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

idle tone The tone that a radio may deliver on the m-lead to signal the LMR gateway that there is no incoming traffic. When the idle tone is removed, the LMR gateway deems all signals to be valid voice traffic.

inactive VTG A VTG that is stored for use. The Cisco IPICS server stores inactive VTGs with the information that you enter so that they can be automatically activated by a policy or manually activated by a dispatcher.

inband Traffic that is sent inband is included in the same stream as the real-time traffic protocol (RTP). Inband signals can be encoded signals and RFC 2833 signals.

incident An event that you identify in Cisco IPICS and for which various users can coordinate responses by using the IDC

incident VTG A talk group that consists of the users, channels, and radios that are associated with an incident.

Incident Dispatch Console (IDC) Standalone PC-based software application that provides PTT functionality so that users with a variety of communication devices can participate in an event.

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.

Key (a radio) causes the radio to transmit. *See* tone keyed.

kilohertz (kHz) A unit of frequency that denotes one thousand Hz.

L

latch The IDC 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.

LLGT low level guard tone. This tone is used as a hold tone or keying tone. *See* guard tone.

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.

This term is often used interchangeably between a handheld or vehicle-mounted device and a stationary transmitter. Stationary devices are typically referred to as base stations.

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.

LMR gateway Land Mobile Radio gateway. Refers to the router E&M interface that converts IP traffic from digital to analog for use by radios.

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.

mixed tone Two tones that are mixed together. DTMF is an example of a mixed tone. To be transmitted properly, tone signals must be mixed with the LLGT. *See* DTMF.

m-lead The mouth portion of the E&M interface. The m-lead is the transmit path of the LMR gateway.

Mobile Client Standalone application that runs on an Apple iPhone, provides access to an incident VTG and supporting media, and allows users to add journals, videos and pictures to an incident.

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 IDC 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 IDC for audio transmission.

mute The functionality that enables a dispatcher to mute an IDC 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.

near end The device or devices that are physically connected to the Ethernet or an RS-232 link. Compare with far end, which refers to devices on the other side of the broadcast. A base station that is connected to an LMR gateway is a near end device while a handheld radio that receives over-the-air signals from the base station is a far end device.

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 IDC 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 IDC 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.

IDC ID The unique ID that the Cisco IPICS server generates for each IDC to track requests between the IDC and the server and to verify and manage concurrent IDC 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.

preamble The sequence of tones that precede a transmission. The preamble generally includes the HLGT and the function tone.

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.

The action that keys a radio or causes the radio to transmit. On the Cisco router, the e-lead, or key tone, is used to signal the radio to transmit.

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 IDC 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 control service The logical element in the Cisco IPICS system that can tune a radio to the desired channel without manual intervention. Refers to a serial control entity.

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 IDC 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.

RFC 2833 The Internet Engineering Task Force (IETF) specification that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. Using RFC 2833 a packet can be compactly composed to play a series of tones, including DTMF, in a specific sequence that includes specified durations and volume levels.

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 IDC 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 IDC 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 that transmit real-time data, such as audio, video, or simulation data, over multicast or unicast network services.

RTCP Real-time Transport Control Protocol. The standard for notifying senders and receivers of important events or transmission statistics. The most common forms of RTCP are the sender report and the receiver report.

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 an IDC 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.

serial controlled radio A type of control for a radio that uses out-of-band signaling (usually RS-232). *See* radio control service.

service delivery area *See* coverage.

signal The detectable transmitted energy that carries information from a transmitter to a receiver.

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.

statically configured tone control Every stream of data that flows to the LMR gateway can be applied with a preamble and/or guard tone by using a static configuration in the LMR gateway. When traffic is sent on a multicast address, the radio automatically switches (because of the preamble) to the specific radio channel that is requested by the tone control sequence.

stored VTG Also referred to as inactive VTG.

subchannel A channel that shares the same multicast address as another channel or channels. These multiple source streams (channels) may be present on a single radio channel. On the IDC, you access these channels by pressing the channel selector buttons on the radio channel.

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 IDC 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 using inband tone sequences to change the behavior of a radio end point. An inband tone can be used to control functions, such as modifying (retuning) the radio frequency (RF channel), changing the transmit power level, and monitoring a channel. The most basic form of tone control (tone keyed) is used to key the radio. With the Cisco IPICS solution, the radio that is being controlled is directly connected to the LMR gateway E&M leads.

tone frequency A specific form of a function tone. The tone that is used to signal the radio to select a frequency. These audible tone frequencies are generated in the router and combined in a specific sequence to perform a tone control function.

tone keyed A tone keyed radio requires the presence of a specific tone on the incoming analog (e-lead) port. Without this tone, the radio cannot transmit. The tone is generally used to prevent spurious transmission that may occur because of injected noise.

tone signaling Any form of over-the-air audible signals that are intended to terminate at the far end. Examples include alerting tones, DTMF tones, and paging tones.

transmit indicator On the ID, 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.

tune (a radio) To change the current send and receive frequencies on a radio. This task is usually accomplished via a preset with some form of radio control.

U

user The Cisco IPICS user may set up personal login information, download the IDC application, 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 IDC, 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 IDC 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 IDC 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 IDC 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 IDC that shows the current volume level on the channel in a graphical format.

volume up/down buttons The buttons on the IDC 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.

W

wavelength The representation of a signal as a plot of amplitude versus time.

wideband channel Channels that occupy more than 20 kHz.

INDEX

Symbols

* (asterisk), in Cisco IPICS Administration Console windows 1-9, 1-12

A

About, in Administration Console 1-14

accessing

- Activity Log Management window 2-72
- Activity Log Options window 2-76
- Administration Console 1-11
- Channels window 2-3
- Descriptors window 9-35
- Dial Engine drawer 8-1
- Download IDC window 4-2
- IDC Installer window 2-94
- IDC Regions window 2-96
- IDC Versions window 2-87
- Incidents window 2-59
- License Management window 2-64
- Locations window 2-31
- Multicast Pool window 2-34
- My Profile window 4-1
- online help 1-14
- Ops View window 7-2
- Options window 2-77
- Policy Management drawer 6-1
- Radios window 9-7
- RMS window 2-39
- UMS window 2-50
- User Groups window 3-29
- Users window 3-2
- Virtual Talk Groups window 5-1

action

- activate VTG 6-5
- definition 6-1
- deleting 6-12
- dial-out 6-6, 6-11
- in multi-purpose type policy 6-8
- invite to VTG 6-5, 6-8
- managing 6-5
- notification 6-5
- overview 6-5
- reactivating 6-19
- VTG add participants 6-6, 6-10

activating

- policy 6-16

RMS 2-44

VTG 5-12, 6-8

active

channel state in Channel window, described 2-7

incident 2-58

multicast address 2-35, 2-38

VTG, managing 5-2, 5-11

active users

fields, described 2-69

viewing information for 2-69

activity log

described 2-72

downloading 2-73

downloading, archived 2-74

managing 2-71

managing activity types per ops view 2-75

options per ops view 2-75

types 2-75

understanding the Activity Log Management window 2-72

viewing 2-73

activity log retention period, setting
described 2-78

adding

alert tone set 2-91

channel 2-5

channel group 2-22

locations 2-32

multicast address to multicast pool 2-36

radio 9-8

radio and tone descriptors 9-36

regions 2-96

RMS 2-45

sequence of multicast addresses to multicast pool 2-36

UMS 2-56

user 3-4

user group 3-31

VTG 5-6

address

e-mail, of user 3-8

information for user 3-7

multicast address 2-35

of user, in user profile 4-4

street, of user in Users window 3-8

Address Information tab 3-7

Administration Console

accessing 1-11

Authentication window 1-11

client system requirements 1-11

displaying current data 1-10

exiting 1-12

logging in 1-11

logging out 1-12

obtaining information about 1-14

online help 1-14

overview 1-8

refreshing 1-10

timeout 1-14

advanced IDC permissions 3-12
advanced IDC permissions, field described 4-6
alerting tones
See alert tones
alert notification 6-7
alert tones
adding 2-91
associating ops views 2-92
creating alert tone sets 2-90
deleting 2-93
managing 2-89
viewing or editing alert tone sets 2-92
allow complex key setting
end devices for users 3-12
IPICS options 2-86
user profile 4-6
allow latch
channel 2-12
field in user profile 4-6
in IDC tab 3-12
radio 9-13
allow secure channel patch
end device for users 3-12
IPICS options 2-86
user profile 4-6
all role, described 1-7, 3-8
archived incident
archive file name 2-79
configuring 2-78
maximum file size 2-78
retention period 2-78
run archive at 2-79
associating
alert tones to ops views 2-92
channel with user 3-18
ops views with user group 3-33
ops view with user 3-25
phone with user 3-19
policy with user 3-20, 6-15
radio with user 3-22
user with policy 3-20, 6-15
Associations tab 3-12
audio, disable 3-12
audio client 1-6
Authentication window 1-11

B

backup and restore operations
overview 11-1
performing 11-1
browser
guidelines for using 1-10
memory issues 1-11
pop-up windows, disabling blocking 1-10
refreshing windows 1-10

C

calculating DSPs A-12

CAP XML file, for external notification B-4

caveats 9-6

changing status of VTG 5-12

channel

- active state 2-14
- active status 2-7
- adding
  - new 2-5
  - to VTG template 5-5
- allow association to users, field described 2-6
- allow latch, described 2-12
- allow use in VTGs field, described 2-7
- associated 3-23
- associated ops view, field described 2-11
- associating
  - radio signals with user 2-18
  - to ops views 2-16
  - user with 3-18
  - with user 2-17
- available 3-23, 3-33
- changing status 2-14
- channel color, field described 2-12
- channel region, field described 2-12
- channel selector, field described 2-10
- deleting
  - from a channel group 2-25
  - from system 2-20
- described 2-2
- descriptor, field described 2-10
- disabled status 2-7
- disabling 2-14
- editing information 2-5
- enabled status 2-7
- enable latch, field described 2-12, 9-13
- enable VAD, field described 2-12
- enabling 2-14
- IDC region field described 2-12
- in inactive VTG 5-5
- listen only, field described 2-12
- location 2-9
- location, field described 2-9
- mixing secure and non-secure in VTG 5-5
- multicast address, field described 2-9
- multicast address port, field described 2-9
- name, field described 2-6
- radio, field described 2-10
- removing
  - from channel group 2-25
  - from system 2-20
- RX mute during PTT, field described 2-11
- search for in VTG window 5-24
- secure, field described 2-6
- status 2-7
- type, field described 2-8
- unavailable for VTG 5-22

viewing
associations 2-19
information 2-5
Channel dashboard
elements 12-3
overview 12-3
channel group
adding
new 2-22
to VTG template 5-5
associated ops view, field described 2-23
associated VTG 2-25
associated VTG status 2-25
associating ops views to 2-26
channels in 2-2
deleting 2-27
deleting a channel from 2-25
described 2-2
editing information 2-23
name 2-23
removing
channel from 2-25
from system 2-27
viewing
associations 2-25
information 2-23
Channel Selector Permissions 3-23
channel selectors
associated channel field, described 9-5
enabled status check box 9-5
label 9-5
Cisco 10-3
Cisco IOS documentation 1-xxii
Cisco IPICS
Administration Console 1-8
database
backing up 11-3
logs 11-14
restoring 11-9
deployment options 1-3
getting started 1-1
hardware components 1-3
initial configuration 1-1
IP multicast address guidelines for 2-36
logging in to 4-1
Login window 4-1
overview 1-1, 1-3
Restrict Operator Role assignments 2-79
role 1-7
server 1-4
session timeout period setting 2-78
setting up 1-1
software components 1-3
Cisco IPICS policy engine
See policy engine
Cisco IPICS server
Administration Console 1-8
described 1-4

SSL certificate on E-1

usage guidelines 1-9

Cisco IPICS service

about D-1

configuring

for Cisco Unified Communications Manager D-1

for Cisco Unified Communications Manager Express D-3

disabling log in D-2

subscribing to D-3

using D-4

Cisco IPICS session timeout 2-78, 2-79

Cisco IPICS session timeout period, setting described 2-78

Cisco IP Interoperability and Collaboration System

See Cisco IPICS

Cisco router

function in a Cisco IPICS deployment 1-6

Cisco Security Agent documentation 1-xxii

Cisco Unified Communications Manager

configuring as SIP provider 8-32

configuring Cisco IPICS service for D-1

documentation 1-xxi

function in a Cisco IPICS deployment 1-6

Cisco Unified Communications Manager Express

configuring as SIP provider 8-35

configuring Cisco IPICS service for D-3

documentation 1-xxi

Cisco Unified IP Phone

accessing Cisco IPICS service from D-4

allow latch 3-12

audio 3-12

dial login for 3-9

digit ID 3-10, 4-4

digit password 3-10

disable 3-10

documentation 1-xxi

high availability, affect on 10-8

latching 3-12

listen only 3-12

managing for user 3-10

mute 3-10

subscribing to Cisco IPICS service D-3

timeout period setting 2-78

unmute 3-10

user in VTG 5-14

using as a PTT device D-1

client

log out, setting described 2-84

maximum video size, setting described 2-84

update poll, setting described 2-83

cluster view daemon, trace file 8-3

codec

field described 2-10

for policy engine 8-29

radio 9-9

communications preferences
configuring 3-14
described 3-13
managing 3-13
complex key setting
end devices for users 3-12
IPICS options 2-86
connection type, multicast address 2-35, 2-38
control function permissions 3-23
control functions 3-24
controllers
configuring T1/E1 controllers A-4
on RMS 2-43
copying a user 3-4
customized script prompts
codec 8-12
deleting 8-14
described 8-11
downloading 8-13
renaming 8-14
uploading 8-12
viewing list of 8-12
Customized Script Prompts window 8-12

D

Dashboard window, overview 12-1
database
backing up 11-3
choosing a backup destination 11-8
manually starting database server 11-19
options
changing 11-6
default 11-6
restoring 11-10
restoring 11-9
troubleshooting
backup procedure 11-15
restore procedure 11-15
database log 10-14
Database Management window
overview 11-2
tabs inside of 11-2
database replication block state 10-14
database updates 10-14
DDRBLOCK 10-14
deactivated
RMS 2-44
RMS status 2-43
VTG 5-13
deactive, incident 2-58
DEBUG-level error messages 12-10, 12-13
debug trace level 8-3
dedicated-dial-engines.xml file B-2
default language folder 8-8
default tone sequences, configuring 9-6
deleting
action from policy 6-12

alert tones 2-93
channel
from channel group 2-25
from system 2-20
channel group 2-27
descriptors 9-38
IDC
regions 2-97
versions 2-89
incident 2-63
languages 8-9
locations 2-33
multicast address 2-38
policy 6-16
radio 9-18
radio and tone descriptors 9-38
RMS 2-48
spoken names prompts 8-20
trigger from policy 6-14
UMS 2-57
user 3-28
user group 3-35
VTG 5-11
deployment, of Cisco IPICS 1-3
descriptors
deleting 9-38
managing radio and tone 9-21
updating 9-37
diagnostic information
downloading 12-8
viewing 12-6
Diagnostics window
diagnostic summary pane, described 12-8
elements 12-6
overview 12-1, 12-6
dial engine
codec 8-29
configuring B-2
described 8-1
for external notification B-2
parameters 8-28
services
obtaining information about 8-2
status 8-2
trace file 8-3
Dial Engine drawer, accessing 8-1
dial engine script
See scripts 8-21
Dial Engine Script notification 6-7
dial-in
assigning to ops view 7-13
configuring SIP provider for 8-32
SIP trunk 8-34
dial-in floor 6-22
dialing out to participants in an active VTG 5-19
dial-in phone
disable 3-10

high availability, affect on 10-8
listen only 3-12
managing for user 3-10
mute 3-10
unmute 3-10
dial login
configuring 3-9
described 3-9
Dial Login tab 3-9
Dial notification 6-7
dial-out
action 6-6, 6-11
configuring SIP provider for 8-32
SIP trunk 8-34
dial preferences
configuring 3-14
described 3-14, 4-7
order of 3-17
dial prefix 8-30
digit ID 3-10, 4-4
digit password (PIN) 3-10, 4-5
direct dial
adding numbers 8-31
deleting numbers 8-32
described 8-29
dial prefix 8-30
updating numbers 8-31
viewing information about numbers 8-31
Direct Dial Management window 8-30
direct dial numbers
managing 8-29
viewing list 8-30
disable
Cisco Unified IP Phone 3-10
IDC attributes in an active VTG 5-19
latch in User Details window 5-17
UMS 2-55
user 3-27
disable audio, in user profile 4-6
disabled channel 2-7
disabled user 3-27
disable IDC activity log upload, setting described 2-84
disable RMS comparator, setting described 2-77
disabling
audio 3-12
dial-in phone 3-10
end device 3-10
IDC 3-10
listen only 3-12
radio 9-17
voice activation detection (VAD) 3-12
dispatcher role
described 1-7, 3-8
responsibilities 5-1
documentation
Cisco IOS 1-xxii
Cisco Security Agent 1-xxii

Cisco Unified Communications Manager 1-xxi

Cisco Unified Communications Manager Express 1-xxi

Cisco Unified IP Phones 1-xxi

session initiation protocol (SIP) 1-xxii

downloading

activity logs 2-73

archived activity logs 2-74

IDC 4-2

DS0

destination 2-47

disabling 2-47

enabling 2-47

in loopback 2-46

source 2-47

status 2-47

ds0 groups, configuring A-4

dspfarm

calculating DSPs A-12

checking configuration A-12

DSP resource pool A-12

enabling A-12

DSPs A-12

dump

memory trace 8-6

threads trace 8-6

E

E1 timeslots A-5

e-mail

address of user 3-8

notification

action 6-6

preference 3-14, 4-7

system event C-1

enable

IDC attributes in an active VTG 5-19

latch in User Details window 5-17

radio 9-17

UMS 2-55

user 3-27

enabled

channel 2-7

user 3-27

enable voice activity detection (VAD), field described 2-12

enabling

Cisco Unified IP Phone 3-10

dial-in phone 3-10

end device 3-10

IDC 3-10

listen only 3-12

UMS 2-55

voice activation detection (VAD) 3-12

end device

audio 3-12

described 3-10
disable 3-10
listen only 3-12
managing for user 3-10
mute 3-10
unmute 3-10
ERROR-level error messages 12-10, 12-13
event, also called active VTG 5-2
executed policy, information about 6-17
executing policy, information about 6-17
expiration date, of password 3-7
bulk notification
See external notification
external notification
configuring dial engine B-1
deploying B-1
description B-1
dial engine B-1, B-2
failover, affect on 10-8
invoking
CAP XML file B-4
HTTP request B-3
options B-3
message file B-3
overview B-1
recipient list B-2
requirements B-1
results of B-8
notification
See external notification

F

failover
affect on Cisco Unified IP Phone 10-8
affect on dial-in user 10-8
affect on external notification 10-8
affect on IDC 10-6
affect on IDC and connected devices 10-2
affect on mobile client 10-8
affect on policy 10-8
local critical process failure 10-2
lost heartbeat message failure 10-2
manual 10-3, 10-9
file size, of archived incident 2-78
floor, for dial-in 6-22

G

G.711 2-10
G.729 2-10
gateway 1-5
General Information tab 3-7, 3-9
guidelines
for using IP multicast addresses with Cisco IPICS 2-36
managing active VTGs 5-11

managing inactive VTGs 5-5

multicast address 2-36

server usage 1-9

H

HA

See high availability (HA)

hangover time 9-10

hardware components, of Cisco IPICS 1-3

help, in Administration Console 1-14

high availability (HA)

active server 10-1

affect of failover on IDC and connected devices 10-2

Cisco Unified IP Phone, affect on 10-8

configuring 10-3

description 10-1

dial-in user, affect on 10-8

failover

local critical process failure 10-2

lost heartbeat message failure 10-2

manual 10-3

IDC connections, affect on 10-6

license 2-64

manual failover 10-9

mobile client, affect on 10-8

overview 10-1

redundant server location 10-2

split brain scenario

definition 10-3

resolving 10-10

standby server 10-1

synchronizing server time 10-8

UMS 2-53

unconfiguring 10-6

High Availability Window 10-4

host name, of RMS 2-43

HTTP request, for external notification B-3

I

icons, in users window 3-32

icons in Users window 3-3

ID, of user 3-5

IDC

activity log update, setting frequency 2-86

adding alert tone sets 2-91

advanced permissions 3-12

alert tones, *See* alert tones

allow latch 3-12

audio 3-12

changing the state of versions for updates 2-89

client log out, setting described 2-84

creating alert tone sets 2-90

deleting versions 2-89

described 1-3, 1-4

dialer preference 3-14, 4-7

Dialer Preferences 3-15
disable 3-10
downloading current version 4-16
failover, affect on 10-2
high availability affect on 10-6
installer, generating 2-94
latching 3-12
listen only 3-12
log files 3-10, 3-11
log in after failover 10-7
logout, forced 2-69
log upload frequency, setting described 2-85
managing for user 3-10
managing the configuration 2-93
mandatory update 2-88
maximum video size, setting described 2-84
mute 3-10
operation caveats when configuring tone sequences 9-34
recommended update 2-88
regions 2-96
  adding 2-96
  managing 2-95
  maximum 2-95
  See also regions
send logs on rollover, setting described 2-85
tab 3-12
unmute 3-10
update poll, setting described 2-83
user in VTG 5-14
versions
  changing state 2-88
  uploading 2-88
versions, managing 2-86
voice activation detection (VAD) 3-12
IDC alert tones
  See alert tones
IDC Installer window 2-94
idcsetup.exe 2-94
idle status, for multicast address 2-35, 2-38
IN_SERVICE 8-2
inactive
  VTGs 5-4
  VTGs, guidelines 5-5
incident
  Activated, field described 2-61
  activating 2-62
  active 2-58
  Address, field described 2-61
  changing status 2-62
  configuring archive 2-78
  current participants, fields described 2-61
  Deactivated, field described 2-61
  deactivating 2-62
  deactive 2-58
  definition 2-58
  deleting 2-63

description, field described 2-61
editing information 2-60
ID, field described 2-61
Incident VTG, field described 2-61
management 2-58
name, field described 2-61
Ops View, field described 2-61
overview 2-58
removing 2-63
state, field described 2-61
VTG 2-58
Incident dashboard
elements 12-4
overview 12-3
Incidents window
accessing 2-58, 2-59
understanding 2-59
INFO-level error messages 12-10, 12-13
Informix database, manually starting 11-19
invitation policy type
adding 6-11
described 6-4
updating 6-11
invitation type policy, actions in 6-5
invite to VTG action 6-5
IP address, of RMS 2-43
IP address selection guidelines A-6
ipics.log
downloading 12-12
error types 12-10, 12-13
ipics.log file B-8
IPICS Connect 9-20
IPICS Dispatch Console
See IDC
IP multicast address, guidelines for using with Cisco IPICS 2-36
IP Phone Text notification 6-6

L

languages
adding 8-9
default language folder 8-8
deleting 8-9
for prompts 8-8
for scripts 8-8
naming requirement 8-8
of TUI prompts 6-21
renaming 8-9
viewing list of 8-8
Languages window 8-8
latch
allow 3-12
disable 3-12
enable 3-12
LDAP
configuring 2-98
general settings 2-98

license
described 2-63
for policy engine 6-1
installed files 2-67
managing a Cisco IPICS 2-63
summary 2-64
time-bound, described 2-68
usage per ops view 2-66
License dashboard
elements 12-5
overview 12-5
license file, uploading 2-68
Linux user roles 1-8
listen only
in channel 2-12
in IDC tab 3-12
in radio 9-14
in user profile 4-6
LMR gateway 1-5
location
adding 2-32
associations 2-28
deleting 2-33
described 2-27
multicast address 2-35, 2-38
of RMS 2-42, 2-53
predefined 2-27
radio 9-9
RMS 2-45
summary of access types and connections 2-31
UMS 2-56
user 4-5
viewing or editing 2-32
locking, user account 3-27
log files
downloading 12-12, 12-15
IDC 3-10
in RCS Logs window 12-13
in System Logs window 12-9
managing activity 2-71
obtaining 3-11
log in, disabling for Cisco IPCS service D-2
log out
forced
from IDC 2-69
from mobile client 2-69
from Administration Console 1-12
offline client expiration 2-84
logs, managing activity 2-71
loopback
configuring 2-46
creating 2-46
disabling DS0 in 2-47
DS0
destination 2-47
source 2-47
status 2-47
dynamically allocated 6-2

enabling DS0 in 2-47
number 2-46
on RMS 2-43
removing 2-48
state 2-46
viewing information about 2-46

M

managing
activity log options per ops view 2-75
inactive VTGs 5-4
radio and tone descriptors 9-21
mandatory update, for IDC 2-88
maximum activity logs, setting described 2-78
member, adding to user group 3-32
merging RMS configuration 2-49
message file, for external notification B-3
mobile client
high availability, affect on 10-8
logout, forced 2-69
multicast address
adding address to multicast pool 2-36
adding a sequence of addresses to multicast pool 2-36
address 2-37
address and port 2-35
assignment 2-36
channel 2-9
connection type 2-35, 2-38
conventions 2-9, 2-36, 2-37
deleting 2-38
editing information 2-37
guidelines 2-36
in multicast pool 2-33
location 2-35, 2-38
port 2-38
recommended range 2-36
status 2-35, 2-38
used by 2-35, 2-38
viewing information 2-37
multicast communications guidelines 2-36
multicast domain 2-27
multicast pool
adding multicast address to 2-36
deleting multicast address from 2-38
described 2-33
multi-purpose type policy
actions in 6-5, 6-8
activating 6-16
adding 6-8
described 6-4
trigger 6-12
updating 6-8
mute
Cisco Unified IP Phone 3-10
dial-in phone 3-10
end device 3-10
IDC 3-10

client 3-10
user in VTG 5-15
My Profile window, described 1-11

N

name
of user 3-5, 3-7
of user group 3-34
New Users window 3-4
notification
action 6-5
alert 6-7
configuring 6-9
Dial 6-7
Dial Engine Script 6-7
e-mail
action 6-6
system event C-1
external, *See* external notification
IP Phone Text 6-6
overview 6-6
system event C-1
Talk Group 6-7
notification preferences
configuring 3-14
described 3-14, 4-7
notifying participants in an active VTG 5-19

O

old digit password, changing 4-4
online help, accessing 1-14
operational, RMS status 2-43
Operational Views
See ops views
operator role
described 1-7, 3-8
responsibilities 3-1
restricting assignments 2-79
ops view administrator role, described 1-7, 3-8
ops views
accessible to 7-5
affecting VTGs 7-10
allocating dial ports, described 7-18
assigning a dial number (DN) 7-13
assigning to user 7-20
associated 3-25
associating
channel groups with 2-26, 7-20
channels with 7-20
to channels 2-16
user group with 3-33
user with 3-25
available 3-25
belongs to 7-4
benefits 7-4
caveats 7-7

channels 7-20
creating 7-3
determining dial port allocation 7-19
dial-in numbers 7-13
dial port pools 7-18
overview 7-1
resources 7-4
system 7-1
to which user belongs 3-24
to which user group belongs 3-33
understanding VTGs 7-8
user roles 7-6
viewing
details 7-16
resources 7-15
Ops View to User Association window 3-25
Options window 2-77
order, of dial preferences 3-17
OUT_OF_SERVICE 8-2

P

pager, notification preference 3-14, 4-7
PARTIAL_SERVICE 8-2
participant
adding to VTG 5-13
in VTG 5-13
removing from VTG 5-13
password
Apply User Account Lockout setting 2-82
Apply User Password Expiration setting 2-81
changing 4-3
expiration date 3-7
Failed Password Attempt Expiration Hours setting 2-83
Maximum Invalid Login Attempts Allowed setting 2-83
Minimum Digit Password Length setting 2-80
Minimum Lower Case Letter Count setting 2-80
Minimum Numeric Character Count setting 2-80
Minimum Password Length setting 2-79
Minimum Special Character Count setting 2-81
Minimum Upper Case Letter Count setting 2-80
Password Expiration Notification setting 2-82
Password Expiration setting 2-81
Password History Count setting 2-81
RMS 2-45
user 3-5, 3-7
patch secure channels
end device for users 3-12
IPICS options 2-86
user profile 4-6

phone
associated 3-20
associating user with 3-19
available 3-20
Phone Associations window 3-20
phone service D-1
PIN, digit password
defined 3-10
in user profile 4-5
Policies window
described 6-3
displaying 6-3
policy
action, *See* action
activating 6-16
adding 6-4
associated 3-21
associating user with 3-20, 6-15
available 3-21
definition 6-1
deleting 6-16
deleting action from 6-12
deleting trigger from 6-14
executed 6-17
executing 6-17
failover, affect on 10-8
invitation type
actions in 6-5
adding 6-11
described 6-4
updating 6-11
multi-purpose type
actions in 6-5
adding 6-8
described 6-4
updating 6-8
ops view guidelines 6-4
reactivating 6-19
scheduled 6-18
system resources for 6-4
trigger 6-12
type 6-5
viewing information about 6-17, 6-18
Policy Associations window 3-21
policy engine
license requirement 6-1
Policies window 6-3
policy, *See* policy 6-1
roles that can access 8-1
SIP provider 8-32
tracing 8-3
Policy Management drawer, accessing 6-1
pop-up windows 1-10
port
channel 2-9
conventions 2-9, 2-37, 2-38
multicast address 2-38
preferences, system, setting in Options window 2-77

primary server
description 10-1
See also high availability (HA)
prompts
customized script, *See* customized script prompts
described 8-1
languages
See also language
languages, about 8-8
managing 8-7
repository 8-8
spoken name, *See* spoken name prompts
standard script, *See* standard script prompts
PTT channel
See channel
PTT channel group
See channel group

R

radio
adding
to system 9-8
to VTG template 5-5
Allow association to users, check box described 9-10
allow latch, described 9-13
Allow use in VTGs, check box described 9-11
associating
signals with channels 2-18
user with 3-22
with user from Radios window 9-15
channel 9-2
codec field described 9-9
control functions 3-24
default tone sequences 9-6
deleting 9-18
description, field described 9-9
descriptor file, described 9-22
designating permissions for 3-23
editing information 9-14
enabling or disabling 9-17
frequency channels, described 9-4
hangover time, field described 9-10
IDC caveats when configuring tone sequences 9-34
listen only, field described 9-14
location, field described 9-9
managing
descriptors 9-21
overview 9-2
multicast address, field described 9-9
multicast port, field described 9-9
name, field described 9-8
overview 9-1
Pooled Resource, field described 9-9
radio color, field described 9-14
region, field described 9-14

removing 9-18
RX mute during PTT, field described 9-13
search for in VTG window 5-24
secure radio, field described 9-9
tone and signaling sequences, described 9-22
tone descriptors, described 9-21
type, field described 9-8
viewing information 9-14
voice delay, field described 9-10
radio channel
managing 9-2
See also radio
radio color, field described 9-14
radio control service
See RCS
radio descriptors 9-22
deleting 9-38
described 9-22
format example 9-23
IDC operation caveats 9-34
managing 9-21
updating 9-37
radio preferences 3-14, 4-7
rcs.log
file 12-15
rcs.log, downloading 12-15
RCS logs
downloading 12-15
entry types 12-13
overview 12-13
viewing 12-13
RCS Logs window
described 12-13
log entry types 12-13
reactivate
action 6-19
policy 6-19
VTG 5-22
recipient list
for external notification B-2
format B-2
recommended update, for IDC 2-88
recording, spoken names prompts 8-18
recovering, system administrator 3-28
recurrence, of trigger 6-14
redundant server 10-2
refreshing, Administration Console 1-10
regions
adding 2-96
deleting 2-97
viewing or editing 2-97
removing
channel 2-20
channel from channel group 2-25
channel group 2-27
incident 2-63
radio 9-18
RMS 2-48

UMS 2-57

user 3-28

user group 3-35

VTG 5-11

repository 8-8, 8-21

required information, in Cisco IPICS windows 1-9, 1-12

rerecording, spoken names prompts 8-18

restoring a backed-up database 11-9

Restrict Operator Role assignments, setting described 2-79

retention period 2-78

RMS

activating 2-41, 2-44

adding 2-45

calculating DSPs A-12

configuration, merging 2-49

configuring

managing 2-49

security features A-1

T1/E1 controllers, interfaces, and voice parameters A-7

connectivity guidelines A-4

controllers 2-43

deactivated status 2-43, 2-44

deactivating 2-41, 2-44

deleting 2-48

described 1-5

ds0 groups A-4

dspfarm configuration A-12

E1 timeslots A-5

editing information 2-41

host name 2-43

IP address 2-43

IP address selection

Ethernet interface A-6

guidelines A-6

Loopback0 interface A-6

Vif1 interface A-6

location 2-42

loopback 2-43

managing

configuration 2-49

overview 2-39

merging configuration 2-49

name 2-42

operational status 2-43

removing 2-48

security features A-1

status 2-43

status of routers in RMS window 2-40

stopping

state 2-44

status 2-43

T1 timeslots A-4

unconfigured status 2-43

unreachable status 2-43

updating

configuration 2-49

information in Cisco IPICS 2-49
viewing information 2-42
RMS/UMS dashboard
overview 12-6
RMS dashboard
elements 12-6
RMS polling frequency, setting interval 2-77
role
all 1-7, 3-8
assigning 3-8
changing 3-8
Cisco IPICS 1-7
described 3-8
dispatcher 1-7, 3-8, 5-1
Linux user 1-8
operator 1-7, 3-1, 3-8
ops view administrator 1-7, 3-8
system administrator 1-7, 2-1, 3-8
user 1-7, 4-1
roles, field described 4-3
router
See RMS
router media service
See RMS
RX mute during PTT
on channel 2-11
on radio 9-13

S

scheduled policy, information about 6-18
scripts
adding 8-22
BulkNotifyDialer 8-21
changing information about 8-22
deleting 8-23
described 8-1
dial engine 8-21
IppeDialin 8-21
IppeDialout 8-21
IppeRecording 8-21
languages 8-8
managing 8-21
repository 8-21
system 8-21
viewing information about 8-22
viewing list of 8-21
searching in Virtual Talk Groups window 5-23
secondary server
description 10-1
high availability license on 2-64
See also high availability (HA)
secure channel patch
end device for users 3-12
IPICS options 2-86
user profile 4-6
secure radio 9-9

Serial Radio Control Interface (SRCI)
accessing 9-18
channel selectors 9-20
IPICS Connect 9-20
overview 9-3
radio display and controls 9-19
radio information 9-18
server, Cisco IPICS 1-4
server logs, viewing 12-9, 12-13
server time, synchronizing for high availability 10-8
server usage guidelines 1-9
Serviceability drawer, overview 12-1
services, obtaining information about 8-2
session initiation protocol (SIP), documentation 1-xxii
setting up Cisco IPICS 1-1
short message service (SMS), notification preference 3-14, 4-7
short name for channel, field described 2-6
SHUTDOWN 8-2
SIP, configuring for Policy Engine 8-24
SIP provider
Cisco IOS 8-35
Cisco Unified Communications Manager 8-32
Cisco Unified Communications Manager Express 8-35
configuring for Cisco IPICS 8-32
described 8-32
software components, of Cisco IPICS 1-3
specifying order 3-18, 4-10, 4-12
split brain scenario
definition 10-3
resolving 10-10
spoken names prompts
changing information about 8-20
deleting 8-20
described 8-14
downloading 8-17
for user 3-25
recording 8-18
replacing .wav file 8-18
rerecording 8-18
uploading 8-16
viewing list of 8-15
Spoken Names window 8-15
SSL certificate, creating on Cisco IPICS server E-1
standard script prompts
described 8-10
uploading 8-11
viewing list of 8-10
Standard Script Prompts window 8-10
standby server
description 10-1
See also high availability (HA)
status
channel 2-7
DS0 2-47
multicast address 2-35, 2-38

Status Details window 8-2
stopping, RMS status in RMS window 2-43
sub-VTG 5-5
system administrator role
described 1-7, 2-1, 3-8
responsibilities 2-1
System dashboard, overview 12-2
system event e-mail notifications C-1
system logs
downloading 12-12, 12-15
entry types 12-10
overview 12-10
viewing 12-9
System Logs window
described 12-1, 12-9
log entry types 12-10
system preferences, setting in Options window 2-77
system status
monitoring 12-9, 12-13

T

T1/E1 controller configuration A-4
T1 timeslots A-4
tab
Address Information 3-7
Associations 3-12
Dial Login 3-9
General Information 3-7, 3-9
IDC 3-12
Talk Group notification 6-7
telephony user interface
See TUI
text to speech
See TTS 8-28
time out, period for Administration Console 1-14
tone broadcast wave files
See alert tones
tone descriptor files, for radios 9-21
tone descriptors
adding 9-36
deleting 9-38
described 9-21
IDC operation caveats 9-34
updating 9-37
tone sequences
description field, described 9-5
enabled state check box 9-5
label 9-5
momentary control 9-5
stateful control 9-5
tone sequences, described 9-21
trace
advanced activities 8-6
cluster view daemon 8-3
configuring, trace files
number 8-4
size 8-4

debug 8-3
default levels 8-5, 8-6
described 8-3
dial engine 8-3
dump
memory trace 8-6
threads trace 8-6
facilities 8-3, 8-5
files 8-3
interpreting trace files 8-7
levels 8-3, 8-4
maximum size of all trace files on systems 8-4
obtaining trace files 8-7
recommendations for 8-3
XDebug (extended debug) 8-3
TRACE-level error messages 12-10, 12-13
transaction log 10-14
trigger
adding 6-13
definition 6-1
deleting 6-14
overview 6-12
recurrence 6-14
updating 6-13
viewing 6-13
TTS
configuring 8-28
overview 8-28
TUI (telephony user interface)
accessing 6-21
activities 6-20
described 6-20
dial-in floor 6-22
dial login for 3-9
digit ID 3-10
guidelines
general 6-21
menu 6-22
logging in 6-21
PIN 3-10
speaking 6-22
type, channel connection 2-8

U

UMS
adding 2-56
deleting 2-57
described 1-5
disabled status 2-55
disabling 2-55
editing information 2-52
Enabled status 2-55
enabling 2-55
high availability 2-53
IP Address 2-52
location 2-53

managing
overview 2-50
name 2-52
removing 2-57
status of 2-50
viewing information 2-52
unconfigured, RMS status 2-43
understanding 7-18
Activity Log Management window 2-72
Channels window 2-3
Descriptors window 9-35
IDC Regions window 2-95
Incidents window 2-59
Ops View window 7-2
Radios window 9-7
RMS window 2-39
UMS window 2-50
Virtual Talk Groups window 5-2
unified media service
See UMS
unlocking a user account 3-27
unmute
Cisco Unified IP Phone 3-10
dial-in phone 3-10
end device 3-10
IDC 3-10
unmuting IDC user in a VTG 5-15
unreachable, RMS status 2-43
updating
descriptors 9-37
radio and tone descriptors 9-37
RMS configuration 2-49
uploading
IDC versions 2-88
license file 2-68
standard script prompts 8-11
used by field, for multicast address 2-35
user
adding
dial preferences in user profile 4-11
IDC preference in user profile 4-10
notification preferences in user profile 4-8
radio preferences in user profile 4-9
to system 3-4
to VTG template 5-5
address
information 3-7
street 3-8
associating
ops views with 3-25
phone with 3-19
policy with 3-20, 6-15
PTT channels with 3-18
radios with 3-22
to PTT channels 2-17
associating radios with, from Radios window 9-15

changing information in user profile 4-2
channel association 4-13
copying 3-4
default location 3-10
deleting
dial preferences in user profile 4-11
from system 3-28
notification preferences in user profile 4-8
radio preferences in user profile 4-9
described 3-1
dial preferences 4-12
digit ID 3-10
digit password (PIN) field 3-10, 4-5
disabled 3-27
downloading IDC 4-16
editing
dial preferences in user profile 4-11
IDC dial preference in user profile 4-10
notification preferences in user profile 4-8
radio preferences in user profile 4-9
enabled 3-27
general information 3-6
in inactive VTG 5-5
list of VTGs in which is a participant 3-26
locking account 3-27
managing
associations 4-12
communications preferences 4-7
profile 4-2
name 3-5, 3-7
ops view for 3-24
order
of dial preferences 4-12
of radio preferences 3-18, 4-10
password 3-7
PIN 3-10
radio preferences 3-18, 4-10
recovering deleted system administrator 3-28
removing 3-28
search for in VTG window 5-24
status 3-27
unlocking account 3-27
updating IDC dialer preferences in user profile 4-10
viewing
associations 4-15
dial preferences 4-11
IDC dialer preferences 4-10
notification preferences 4-8
radio preferences 4-9
user associations
Channels tab, described 4-13
Incidents tab, described 4-14
Phones tab, described 4-14
Policies tab, described 4-15
Radios tab, described 4-13

Virtual Talk Groups tab, described 4-14

User dashboard

elements 12-4

overview 12-4

User Details window

activities 1-12

enabling or disabling latch for IDC user 5-17

user group

adding

members to 3-32

new 3-31

to VTG template 5-5

associating ops views with 3-33

changing name of 3-34

deleting 3-35

described 3-1, 3-29

list of VTGs in which is a participant 3-34

naming recommendation 3-31

ops view for 3-33

removing 3-35

User Groups window

accessing 3-29

described 3-29

User Management drawer, accessing 3-1

user name of RMS field, described 2-43

user profile

account status field, described 4-3

address field, described 4-4

belongs to field, described 4-3

confirm password field, described 4-3

default location 4-5

described 4-2

dial preferences field, described 4-7

digit ID field, described 4-4

first name field, described 4-2

IDC info field, described 4-6

IPICS status field, described 4-3

last name field, described 4-2

new password field, described 4-3

notification preferences field, described 4-6

old digit password field, described 4-4

old password field, described 4-3

password expiration date field, described 4-3

roles field, described 4-3

user name field, described 4-2

User Radio Permissions window 3-23, 3-24

user role

described 1-7

responsibilities 4-1

users

phone associations 4-14

policy associations 4-15

radio associations 4-13

VTG associations 4-14

Users window

accessing 3-2

described 3-2

V

video size, maximum 2-84

viewing

- activity logs 2-73
- and downloading archived activity logs 2-74
- and editing user associations, My Associations window 4-2
- channel associations 2-19
- IDC
  - alert tone sets 2-92
  - regions 2-97
- ops view resources 7-15
- or editing locations 2-32
- user associations 4-15

virtual talk group

- *See* VTG

Virtual Talk Group dashboard

- elements 12-4
- overview 12-4

voice activity detection

- enable field 2-12
- enabling on IDC 5-7, 5-9

voice delay 9-10

VTG

- activating 5-12
- active 5-2, 5-11
- adding
  - channel 5-5
  - channel group 5-5
  - new 5-6
  - participants 5-13
  - radio 5-5
  - to VTG template 5-5
  - user 5-5
  - user group 5-5
  - VTG 5-5
- best practices 5-25
- changing the status of 5-12
- channel in inactive 5-5
- Cisco Unified IP Phone user in 5-14
- deactivating 5-13
- deleting 5-11
- dialing out to participants in active 5-19
- disabling
  - IDC attributes in active 5-19
  - latch in User Details window 5-17
- empty 5-5
- enabling
  - IDC attributes in active 5-19
  - latch in User Details window 5-17
- guidelines for managing
  - active 5-11
  - inactive 5-5
- IDC user in 5-14
- inactive 5-2
- incident 2-58
- in which user group is participating 3-34

list in which user is participating 3-26
managing 5-2
active 5-11
inactive 5-4
modifying 5-9
multicast address used by 2-33
muting an IDC user 5-15
non-secure channel in 5-5
notifying participants in active 5-19
participant in itself 5-5
participants 5-13
reactivating 5-22
removing
from system 5-11
participants 5-13
search for in VTG window 5-24
secure channel in 5-5
seeing as user on Cisco Unified IP Phone D-6
sub-VTG 5-5
unavailable channel 5-22
unmuting an IDC user 5-15
user in inactive 5-5
VTG add participants action 6-6, 6-10
VTG search utility, using 5-23

W

WARN-level error messages 12-10, 12-13

X

X, in Activate VTG Details area 5-22
Xdebug (extended debug) trace level 8-3