



Configuration Guide for Cisco Unified Videoconferencing 3515 MCU12 and MCU24 Release 5.1

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

Customer Order Number:
Text Part Number: OL-11896-01



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

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

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)



Preface vii

- Purpose vii
- Audience vii
- Organization vii
- Document Conventions viii
- Obtaining Documentation viii
 - Cisco.com viii
 - Product Documentation DVD ix
 - Ordering Documentation ix
- Documentation Feedback ix
- Cisco Product Security Overview ix
 - Reporting Security Problems in Cisco Products x
- Product Alerts and Field Notices x
- Obtaining Technical Assistance xi
 - Cisco Technical Support & Documentation Website xi
 - Submitting a Service Request xii
 - Definitions of Service Request Severity xii
- Obtaining Additional Publications and Information xii

CHAPTER 1

- Introducing the Cisco Unified Videoconferencing 3515 MCU Interface** 1-1
 - About the Cisco Unified Videoconferencing 3515 MCU Administrator Interface 1-1
 - About Administrators and Operators 1-3
 - Viewing Administrators and Operators 1-3
 - Adding Administrators and Operators 1-3
 - Editing Administrator and Operator Settings 1-4
 - Deleting Administrators and Operators 1-5
 - Viewing LED Information for the 3515 MCU 1-5
 - Viewing General Information About the 3515 MCU 1-5
 - Updating Your License 1-6
 - Viewing Software Version Details 1-7
 - Setting the Time and Date on the MCU 1-7
 - Setting the MCU Location 1-8
 - Viewing Address Settings for the 3515 MCU 1-8

- Changing Address Settings 1-9
- Changing the Administrator Interface Web Server Port for the 3515 MCU 1-9
- Configuring Security for the 3515 MCU 1-10
- Registering the Online Help for the 3515 MCU 1-10
 - Netscape Navigator Users 1-11

CHAPTER 2

- Basic Configuration for the Cisco Unified Videoconferencing 3515 MCU 2-1**
 - Viewing the Status Tab for the Cisco Unified Videoconferencing 3515 MCU 2-1
 - Configuring Settings for the 3515 MCU 2-2
 - Setting the User Interface Language 2-2
 - Setting the Unit Identifier 2-3
 - Setting an Operator Number 2-3
 - Configuring DTMF Control 2-3
 - Configuring Themes 2-4
 - Configuring Quality of Service 2-5
 - Configuring MCU Dynamic Layouts 2-6
 - Configuring MCU Alert Indications 2-7
 - Viewing Media Processors for the 3515 MCU 2-10
 - Viewing the Event Log for the 3515 MCU 2-10
 - Saving Configuration Settings for the 3515 MCU 2-11
 - Importing Configuration Settings for the 3515 MCU 2-12

CHAPTER 3

- Advanced Configuration for the Cisco Unified Videoconferencing 3515 MCU 3-1**
 - Configuring Conference Management Settings for the 3515 MCU 3-1
 - Configuring Delimiter Settings for the 3515 MCU 3-2
 - Disconnecting Participants on Communications (ICMP) Failure for the 3515 MCU 3-3
 - Sending Advanced Commands for the 3515 MCU 3-3
 - Opening a Telnet Terminal for the 3515 MCU 3-7

CHAPTER 4

- Protocols and the Cisco Unified Videoconferencing 3515 MCU 4-1**
 - Configuring H.323 Gatekeeper Settings for the Cisco Unified Videoconferencing 3515 MCU 4-1
 - Configuring H.323 Gatekeeper Protocol Configuration 4-1
 - Configuring Advanced H.323 Gatekeeper Protocol Settings 4-2
 - Integrating SIP with the Cisco Unified Videoconferencing 3515 MCU 4-3
 - Configuring SIP Proxy Settings 4-3
 - Configuring Advanced SIP Proxy Settings 4-4
 - About the MCU Dial Plan 4-5

Configuring the Cisco Unified Videoconferencing 3515 MCU to Use Cisco Unified CallManager	4-8
Viewing SCCP Protocol Configurations	4-8
Configuring the SCCP Protocol	4-9
Configuring a TFTP Server	4-9
Adding a Cisco Unified CallManager	4-10
Viewing Advanced SCCP Protocol Settings	4-10
Configuring Advanced SCCP Protocol Settings	4-11

CHAPTER 5

Cisco Unified Videoconferencing 3515 MCU Services 5-1

About Services	5-1
Working with Services on the 3515 MCU	5-2
Creating a New Service	5-2
Creating a New SCCP Service	5-3
Customizing Services	5-3
Configuring the Maximum Call Rate	5-4
Configuring the Maximum Layout	5-4
Configuring Standard Definition Advanced Video Settings	5-4
Configuring High Definition Advanced Video Settings	5-6
Configuring Welcome Screen Settings	5-6
Configuring 3G Layout Settings	5-7
Configuring Advanced Audio Settings	5-7
Configuring Data Collaboration Support	5-8
Configuring Presentation View	5-9
Configuring Encryption Support	5-10
Configuring Advanced Management and Security for the 3515 MCU	5-11
Configuring PIN Settings	5-11
Configuring Service Dial-out Policies	5-12
Configuring Service Indication Settings	5-12
Configuring Port Reservations and Limits	5-13
Configuring Support for Far End Camera Control	5-14

CHAPTER 6

Using the Cisco Audio Message Utility 6-1

Introduction	6-1
Launching the Cisco Audio Message Utility	6-2
Playing a Message	6-2
MCU Messages	6-2
Procedure	6-6
Recording a Message	6-6
Replacing a Message	6-7

- Uploading a Message to a Device 6-8
- Viewing Message Details 6-8
- Exiting the Utility 6-9
- About Express Setup 6-9
- Using Express Setup 6-9



Preface

Revised: November 27, 2006, OL-11896-01

Purpose

This guide describes how to configure the Cisco Unified Videoconferencing 3515 MCU12 and the Cisco Unified Videoconferencing 3515 MCU24 unit.

Audience

This guide is intended for network administrators who are configuring the web user interface of the Cisco Unified Videoconferencing 3515 MCU12 and the Cisco Unified Videoconferencing 3515 MCU24.

Organization

This manual is organized as follows:

Chapter	Description
Chapter 1, “Introducing the Cisco Unified Videoconferencing 3515 MCU Interface”	Provides a general overview of Cisco Unified Videoconferencing 3515 MCU web user interface.
Chapter 2, “Basic Configuration for the Cisco Unified Videoconferencing 3515 MCU”	Describes the basic configuration options in the Cisco Unified Videoconferencing 3515 MCU Administrator interface.
Chapter 3, “Advanced Configuration for the Cisco Unified Videoconferencing 3515 MCU”	Describes the more advanced configuration options in the Cisco Unified Videoconferencing 3515 MCU Administrator interface.
Chapter 4, “Protocols and the Cisco Unified Videoconferencing 3515 MCU”	Describes the options available for using the Cisco Unified Videoconferencing 3515 MCU with different protocols.

Chapter	Description
Chapter 5, “Cisco Unified Videoconferencing 3515 MCU Services”	Describes how to use services on the Cisco Unified Videoconferencing 3515 MCU.
Chapter 6, “Using the Cisco Audio Message Utility”	Describes how to use the Cisco Audio Message Utility.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

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

Documentation Feedback

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

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For nonemergencies — psirt@cisco.com

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

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



Tip

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

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

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

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

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

Product Alerts and Field Notices

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

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

<http://www.cisco.com/techsupport>

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

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



Note

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



Tip

Displaying and Searching on Cisco.com

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Introducing the Cisco Unified Videoconferencing 3515 MCU Interface

This section describes the following topics:

- [About the Cisco Unified Videoconferencing 3515 MCU Administrator Interface, page 1-1](#)
- [About Administrators and Operators, page 1-3](#)
- [Viewing LED Information for the 3515 MCU, page 1-5](#)
- [Viewing General Information About the 3515 MCU, page 1-5](#)
- [Viewing Address Settings for the 3515 MCU, page 1-8](#)
- [Changing the Administrator Interface Web Server Port for the 3515 MCU, page 1-9](#)
- [Configuring Security for the 3515 MCU, page 1-10](#)

About the Cisco Unified Videoconferencing 3515 MCU Administrator Interface

In the Cisco Unified Videoconferencing 3515 MCU Administrator interface, you can configure management policies, media processing, call management protocols, and services. [Table 1-1](#) explains the tabs that appear in the Cisco Unified Videoconferencing 3515 MCU Administrator interface.

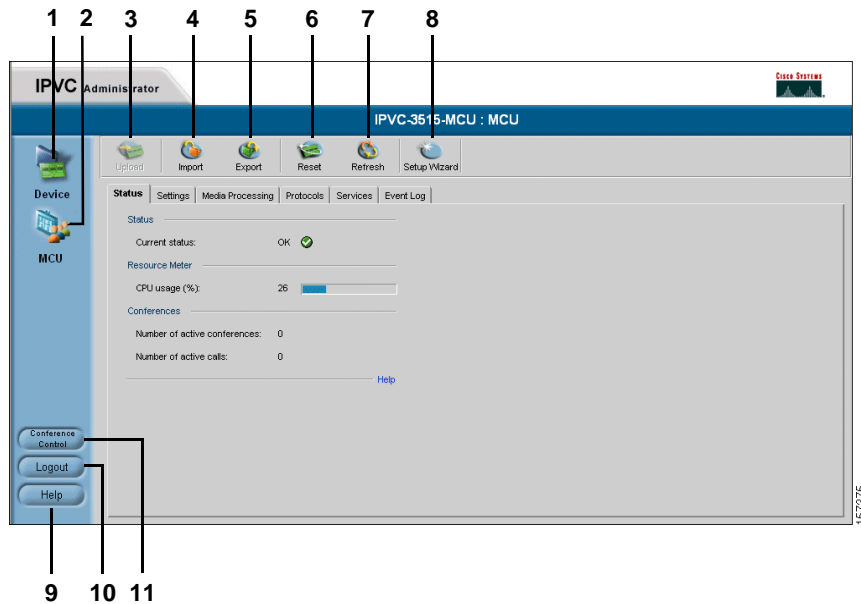
Table 1-1 *MCU Administrator Interface Tabs*

Tab Name	Description
Status	Enables you to view resource usage information and the number of calls and conferences currently in progress.
Settings	Enables you to define the MCU mode of operation.
Media Processing	Enables you to view the data and video processors and servers currently registered with the MCU and access the web interface (if available) of registered devices to modify settings.
Protocols	Enables you to set the gatekeeper IP address and the Session Initiation Protocol (SIP) registrar address for routing calls to the MCU from H.323, Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP) endpoints.

Table 1-1 MCU Administrator Interface Tabs (continued)

Tab Name	Description
Services	Enables you to view, configure and edit the services that the MCU provides.
Event Log	Enables you to monitor MCU alarm events.

Figure 1-1 and Table 1-2 display and list the elements in the MCU Administrator interface.

Figure 1-1 MCU Administrator Interface Elements**Table 1-2** MCU Administrator Interface Elements

Number	Description
1	Device button
2	MCU button
3	Upload button
4	Import button
5	Export button
6	Reset button
7	Refresh button
8	Set Up Wizard button
9	Help button
10	Logout button
11	Conference Control button

About Administrators and Operators

Users must have authorization to access the MCU interface. You can also require users to have Operator-level access to perform management functions during conference calls.

- [Viewing Administrators and Operators, page 1-3](#)
- [Adding Administrators and Operators, page 1-3](#)
- [Editing Administrator and Operator Settings, page 1-4](#)
- [Deleting Administrators and Operators, page 1-5](#)

Viewing Administrators and Operators

In the Users tab in the Device interface, you can view user names that are registered with this MCU and their access level. [Table 1-3](#) lists the elements that appear in the Users tab.

Table 1-3 User Tab Elements

Field	Description
Name	The user login name
Access Level	The access privilege assigned to the user.
Telnet/FTP	Indicates whether the user is authorized to use Telnet or FTP to access the MCU. Telnet and FTP access is intended for maintenance of the MCU.

Adding Administrators and Operators

In the Users tab in the Device interface, you can add Administrators and Operators.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **Device**.
 - Step 2** Click the **Users** tab.
 - Step 3** Click **Add**.
The Add User dialog box appears.
 - Step 4** In the User name field, enter the name you want the Administrator or Operator to log in with.
 - Step 5** In the Access Level field, choose the required authorization level for this user:
 - Administrator—Allows this user to launch the Administrator interface, use the Conference List that has links to web pages of current conferences, share conference chair control with another user, and access this device through Telnet, FTP, and the Cisco Upgrade Utility. You can assign up to ten users Administrator authorization.
 - Operator—Allows this user to share conference chair control with another user and to access the Conference List that has links to web pages of current conferences. Up to 50 users can be assigned Operator authorization.
 - Step 6** In the Password field, enter the password this user uses to log in with.

Passwords can contain a maximum of 32 characters and can include the “a-z”, “A-Z” and “0-9” characters only.

- Step 7** In the Confirm password field, re-enter the password you entered in step 6.
 - Step 8** Select **Enable for Telnet/FTP** to allow this user to access this device through Telnet and FTP. Telnet and FTP access is intended for maintenance of the MCU
 - Step 9** On the toolbar, click **Upload**.
-

Editing Administrator and Operator Settings

In the Users tab in the Device interface, you can edit the settings for a user with Administrator or Operator-level access.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **Device**.
 - Step 2** Click the **Users** tab.
 - Step 3** Click the user you want to edit settings for.
 - Step 4** Click **Edit**
The Edit User dialog box appears.
 - Step 5** In the User name field, enter the name you want the Administrator to log in with.
 - Step 6** In the Access Level field, choose the authorization level for this user:
 - Administrator—Allows this user to launch the Administrator interface, use the Conference List that has links to web pages of current conferences, share conference chair control with another user, and access this device through Telnet, FTP, and the Cisco Upgrade Utility. You can assign up to ten users Administrator authorization.
 - Operator—Allows this user to share conference chair control with another user and to access the Conference List that has links to web pages of current conferences. Up to 50 users can be assigned Operator authorization.
 - Step 7** In the Password field, enter the password this user uses to log in with.
 - Step 8** In the Repeat Password field, re-enter the password you entered in step 6.
 - Step 9** Select **Enable for Telnet/FTP** to allow this user to access this device through Telnet and FTP.
 - Step 10** On the toolbar, click **Upload**.
-

Deleting Administrators and Operators

You can delete users with Administrator or Operator-level access from the MCU system.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **Device**.
 - Step 2** Click the **Users** tab.
 - Step 3** Click the user you want to delete and then click **Delete**.
-

Viewing LED Information for the 3515 MCU

In the LED Monitoring tab in the Device interface, you can monitor the status of all the MCU front panel LED indicators. The LEDs are displayed in diagrams reproducing the layout of the MCU front panel.

Procedure

- Step 1** In the MCU interface, on the sidebar, click **Device**.
 - Step 2** Click the **LED Monitoring** tab.
 - Step 3** Place the mouse cursor over the required LED in the LED Monitoring tab to view a description of that LED.
-

Viewing General Information About the 3515 MCU

The Basics tab in the Device section of the MCU interface, you can view and configure general information about the MCU.

Procedure

- Step 1** In the MCU interface, on the sidebar, click **Device**.
- Step 2** Click the **Basics** tab.
[Table 1-4](#) describes the elements that appear in the Basics tab.

Table 1-4 Device Basic Tab Elements

Field	Description
Device name	Identifies the model number of the device.
Location	User-configured description about the device. Click this field to enter a new description, and then click Upload on the toolbar.
Serial number	The serial number that the factory assigned to the device.
Hardware version	The version number of the current hardware configuration.
Software version	The first two digits of the version number of the software installed on the device. Click the Details button to view details of the versions of software components installed on the device.
Date/Time	The date and time that the Cisco Unified Videoconferencing 3515 MCU clock reports.

Related Topics

- [Updating Your License, page 1-6](#)
- [Viewing Software Version Details, page 1-7](#)
- [Setting the Time and Date on the MCU, page 1-7](#)
- [Setting the MCU Location, page 1-8](#)

Updating Your License

You use the Basics tab to update your MCU license.

Procedure

-
- Step 1** On the sidebar, click **Device**.
- Step 2** Click the **Basics** tab.
- Step 3** Click **Update**.
- The Licensing and Registration dialog box appears.
- Step 4** Access the Cisco web site to register before requesting a new license key by clicking the **Click here to register at the web site** link, or by copying the URL that appears in the lower half of the screen into your browser.
- Step 5** Enter your new license key in the New license key field and click **Upload** to activate the new license key.
-

Viewing Software Version Details

You use the Basics tab to view expanded software version information.

Procedure

- Step 1** On the sidebar, click **Device**.
 - Step 2** Click the **Basics** tab.
 - Step 3** Locate the Software version field and click **Details**.
The Version Details dialog box appears.
-

Setting the Time and Date on the MCU

In the Basics tab, you can set the date and time that the MCU keeps.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **Device**.
- Step 2** Make sure the Basics tab is selected.
- Step 3** Next to the Date/Time field, click **Change**.
The Change Time dialog box appears. The date and time the MCU reports appear in the Set time to field.
- Step 4** In the Change field, select the unit of time that you want to change.



Note There is no unit to change AM and PM. This designation rolls automatically when the hour rolls past 12 backward or forward. Similarly, seconds roll minutes, minutes roll hours, hours roll days, and days roll months.

- Step 5** In the **Set board time to** field, choose the up or down arrow to change that unit.
The unit you choose changes in the direction you choose: higher (up) or lower (down).
 - Step 6** Repeat step 4 and step 5 for as many units as you want to change.
 - Step 7** Select **NTP enabled** to synchronize the time with a network server clock, and to select time zone settings.
 - Step 8** On the toolbar, click **Upload**.
-

Setting the MCU Location

You can install the MCU anywhere on your network including at a remote site. In the Basics tab, you can describe the current location of the MCU.

Procedure

-
- Step 1** On the sidebar, click **Device**.
 - Step 2** Click the **Basics** tab.
 - Step 3** In the Location field, enter the location information about the MCU that you want to display.
The field displays up to 23 characters.
 - Step 4** On the toolbar, click **Upload** to save to configuration memory.
-

Viewing Address Settings for the 3515 MCU

In the Addressing tab, you can view address information for the MCU such as IP address informations, Domain Name Server (DNS) information and Ethernet port speed and duplex. [Table 1-5](#) describes the elements that appear on the Addressing tab.

Table 1-5 Addressing Tab Elements

Field	Description
IP Address	
IP Address	The IP address assigned to the MCU.
Router IP	The address of the router that the MCU uses.
Subnet Mask	The subnet address that the MCU uses.
DNS	
DNS suffix	The DNS alias that the MCU uses.
Preferred DNS Server	The IP address of the primary DNS server that the MCU uses.
Alternate DNS server	The IP address of the alternative DNS server that the MCU uses.
Ethernet	
Port type	Displays information about the Ethernet connection (read-only).
Port settings	The Ethernet speed and duplex that the MCU uses.
MAC address	Displays the Mandatory Access Control (MAC) code assigned to the MCU (read-only).
Port status	Displays the actual Ethernet speed and duplex the MCU uses on the network (read-only).

Related Topics

- [Changing Address Settings, page 1-9](#)

Changing Address Settings

In the Addressing tab, you can change the following address information for the MCU—IP address information, DNS information and the Ethernet port speed and duplex.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **Device**.
- Step 2** Click the **Addressing** tab.
- Step 3** To change an IP address setting, do any of the following steps:
- In the IP Address field, enter the IP address you want to assign to the MCU.
 - In the Router IP field, enter the IP address of the router you want the MCU to use.
 - In the Subnet Mask field, enter the subnet mask you want the MCU to use.
- Step 4** To change or add DNS information, do the following steps:
- In the DNS suffix field, enter the alias you want to assign to the current MCU.
 - In the Preferred DNS server field, enter the IP address of the primary DNS server that you want the MCU to use.
 - In the Alternate DNS server field, enter the IP address of the back-up DNS server that you want the MCU to use.
- Step 5** In the Port settings field, choose the Ethernet port and duplex speed value you want to set.
- Step 6** On the toolbar, click **Upload**.
-

Related Topics

- [Viewing Address Settings for the 3515 MCU, page 1-8](#)

Changing the Administrator Interface Web Server Port for the 3515 MCU

Port 80 is the default Administrator interface web server port. For additional security, you can modify the web server port in the Web tab.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **Device**.
- Step 2** Click the **Web** tab.
- Step 3** In the Web server port field, enter the port number.

- Step 4** On the toolbar, click **Upload**.
-

Configuring Security for the 3515 MCU

You can configure the access that external programs have to the MCU. These external programs include Telnet, Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP) and ICMP (Internet Control Message Protocol or “ping”).

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **Device**.
- Step 2** Click the **Security** tab.
- Step 3** From the Security mode field, choose the access level you want the MCU to support:
- Standard—Allows SNMP, Telnet, FTP, and ICMP to access the MCU.
 - High (no Telnet or FTP)—Allows access to the MCU only through SNMP and ICMP.
 - Maximum (no Telnet, FTP, SNMP, or ICMP)—Disallows external programs to access the MCU.
- Step 4** In the SNMP Read community and Write community fields, enter default strings used to enable SNMP communication between the MCU and an external application such as the Cisco Upload Utility.
-

Registering the Online Help for the 3515 MCU

The online help files for the MCU Administrator and Conference Control interfaces are shipped on the Cisco Unified Videoconferencing Software CD-ROM. To use the online help, you must install the help files for the MCU in a shared directory on your network and register the directory location in the Administrator interface.

If you wish to install the online help on a shared network location and link it to the MCU Administrator, perform the following steps:

Procedure

- Step 1** Copy the online help library from the Cisco Unified Videoconferencing Software CD-ROM to a shared folder on a PC on your network.
- Step 2** Log in to the MCU Administrator interface.
- Step 3** In the Online help URL field of the Board Web tab, enter the directory path to the help files you installed on your PC.

The path must have the form:

`file://computerName\sharedDirectory`

where `computerName` is the name of the computer on the network and `sharedDirectory` is the path to the Online Help folder on the CD-ROM. For example:

file://myComputer\Shared\Online Help

- Step 4** Click Upload in the Cisco Unified Videoconferencing 3545 MCU Administrator toolbar, followed by Refresh.
- Step 5** You may need to log out and log back in to the MCU Administrator for the change to take effect.
-

Netscape Navigator Users

Online help files located on the local network and accessed using Netscape Navigator 4.x must be located on a mapped network drive.



Basic Configuration for the Cisco Unified Videoconferencing 3515 MCU

This section describes the following topics:

- [Viewing the Status Tab for the Cisco Unified Videoconferencing 3515 MCU, page 2-1](#)
- [Configuring Settings for the 3515 MCU, page 2-2](#)
- [Viewing Media Processors for the 3515 MCU, page 2-10](#)
- [Viewing the Event Log for the 3515 MCU, page 2-10](#)
- [Saving Configuration Settings for the 3515 MCU, page 2-11](#)
- [Importing Configuration Settings for the 3515 MCU, page 2-12](#)

Viewing the Status Tab for the Cisco Unified Videoconferencing 3515 MCU

The Status tab in the MCU interface displays information about MCU resource usage and performance. [Table 2-1](#) lists the information in the Status tab.

Table 2-1 **Status Tab Sections**

Section Name	Description
Status	Indicates the current operational state of the MCU as follows: <ul style="list-style-type: none">• Error—Indicates that the MCU is not registered to a gatekeeper, or that the web connection is down.• OK.
Resource Meter	<ul style="list-style-type: none">• CPU Usage (%) field—Indicates the percentage of MCU resources currently occupied. We recommend that this value not exceed 90 percent.
Conferences	<ul style="list-style-type: none">• Number of active conferences—Indicates the number of conferences currently hosted on the MCU.• Number of calls—Indicates the current number of calls on the MCU.

Configuring Settings for the 3515 MCU

In the Settings tab, you can perform the tasks described in the following sections:

- [Setting the User Interface Language, page 2-2](#)
- [Setting the Unit Identifier, page 2-3](#)
- [Setting an Operator Number, page 2-3](#)
- [Configuring DTMF Control, page 2-3](#)
- [Configuring Themes, page 2-4](#)
- [Configuring Quality of Service, page 2-5](#)
- [Configuring MCU Dynamic Layouts, page 2-6](#)
- [Configuring MCU Alert Indications, page 2-7](#)

Setting the User Interface Language

In the Basics section of the Settings tab, you can configure the language that the MCU supports. [Table 2-2](#) lists the languages that the MCU supports.

Table 2-2 Supported Languages in the MCU User Interface

Language	Administrator Interface	Conference Control Interface	Text Overlay on Conference Video
English	*	*	*
Chinese	*	*	*
Japanese	*	*	
Portuguese	*	*	*
Spanish	*	*	*
Russian	*	*	



Note

To view Chinese or Japanese fonts properly in the Administrator interface, the computer (where the web browser is running) should support the appropriate languages. You should set its default language (which you select from the Control Panel > Regional and Language Options menu) accordingly.

Procedure

- Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2 Click the **Settings** tab.
- Step 3 Click the **Basics** button.
- Step 4 In the User interface language field, select the required language.

Setting the Unit Identifier

In the Basics section of the Settings tab, you can set the Cisco Unified Videoconferencing 3515 MCU identifier. This identifies the MCU in the following situations:

- During gatekeeper/SIP registration.
- When inviting endpoints—When inviting endpoints into a conference.
- In text the overlay for the cascaded MCU in cascaded conferences.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Basics** button (if not already selected).
- Step 4** In the MCU Identifier field, enter an identifier (up to a maximum of 15 characters). For example, “London office.”
-

Setting an Operator Number

During a conference, you can invite an Operator to join and provide consultation and support. To do this, in the Basics section of the Settings tab, you set the E.164 number of the designated operator that the MCU dials when a user clicks the Operator button in the Conference Control interface.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Basics** button.
- Step 4** In the Operator field, enter an E.164 number for the operator.
-

Configuring DTMF Control

In the Conference Control section of the Settings tab, you can activate Dual Tone Multi-Frequency (DTMF) and H.243 conference control. DTMF and H.243 conference control allow you to perform the following actions on a conference from the remote control or keypad of your endpoint:

- Take or release Chair Control.
- Mute or unmute your line
- Control your volume
- Block or unblock admission to a conference (Chair Control users only)
- Invite new participants (Chair Control users only).

Procedure

-
- Step 1** In the Administrator interface, click **MCU** (if not already selected).
 - Step 2** Click the **Settings** tab.
 - Step 3** Click the **Conference Control** button.
 - Step 4** Select **Enable DTMF Conference control**.
 - Step 5** In the DTMF Conference Control prefix field, choose a symbol for starting the DTMF conference control session. You can select pound (#) or asterisk (*). The default is *.
 - Step 6** Select **Enable H.243 Conference control**.
-

Configuring Themes

In the Themes section of the Settings tab, you can preview pre-configured video display settings and configure custom themes. You select theme options when configuring services. You can configure a custom theme specifying the text font, color, background color, and border settings for active participants.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
 - Step 2** Click the **Settings** tab.
 - Step 3** Click the **Themes** button.
 - Step 4** Select one of the themes from the Theme field.
 - If you select Classic, you can configure the font size, subframe and border color. Follow step 5 to step 10.
 - If you select Modern, you can configure the font size only. Go to step 6 and then jump to step 10.
 - If you select any other theme, the font size, subframe and border color are automatically set. Go to step 10.
 - Step 5** In the Font background transparency field, choose one of the following settings:
 - None—A solid background against which the text appears.
 - Half—A moderate background against which the text appears.
 - Full—A transparent background against which the text appears.
 - Step 6** In the Font size field, choose a font size:
 - Small
 - Normal
 - Large
 - Step 7** In the Font foreground color, Font background color and Empty subframe color fields, click to select a color for these settings.
 - Step 8** You can display a default border around all participant sub-frames. Select **Display default border** and click to select the default border color.

- Step 9** Select **Display active speaker border** to set a default border for the active speaker.
- Step 10** The Basic font field displays the font currently installed on the MCU. Select **Enable extended font** to enable Asian fonts.

You can view the effects of your settings in the Preview section. This section displays the selected theme settings. This includes a layout with four sub-frames, the theme border highlight colors, active speaker border highlight color, font formatting, screen background color, and text background settings.

Configuring Quality of Service

In the Quality of Service section of the Settings tab, you can assign a priority level to video and voice calls. This section describes how to configure these Quality of Service (QoS) settings using either pre-configured system settings or by creating your own settings.

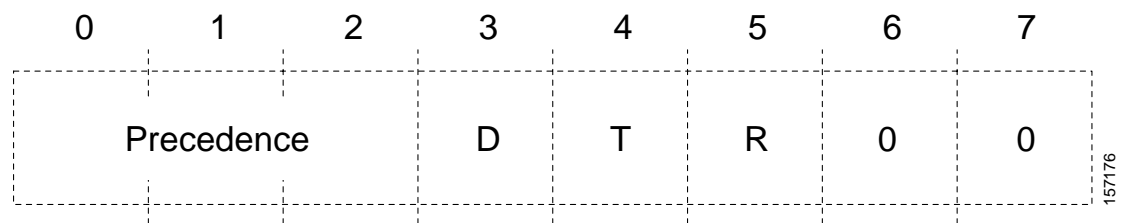
Quality of Service settings involve configuring the MCU to add a Quality of Service (QoS) IP Precedence code in the IP header of outbound packets. Routers on the network that support QoS can give precedence to such coded packets and facilitate the efficient transmission of packets. You can set priority levels on the MCU for voice calls, video calls or both.

The Type of Service (ToS) field in the IP header contains eight bits and indicates the following three abstract quality of service parameters:

- Delay (D)
- Throughput (T)
- Reliability (R)

You use the abstract parameters to choose the actual service parameters when transmitting a datagram through a particular network. The abstract parameters represent the three-way trade off between low delay, high throughput and high reliability. Increasing the performance of one of these parameters might result in reduced performance of the other two. [Figure 2-1](#) represents the ToS field in the IP header.

Figure 2-1 TOS Field in the IP Header



Note

The same fields can also be used to set DiffServ codepoint values

The function of each bit of the ToS field is as follows

- Bits 0-2: Precedence (an independent measure of the importance of the datagram)
- Bit 3: 0 = normal delay, 1 = low delay
- Bit 4: 0 = normal throughput, 1 = high throughput
- Bit 5: 0 = normal reliability, 1 = high reliability
- Bits 6-7: reserved for future use

The possible Precedence settings are as follows:

- 111 = Network Control
- 110 = Internetwork Control
- 101 = CRITIC/ECP
- 100 = Flash Override
- 011 = Flash
- 010 = Immediate
- 001 = Priority
- 000 = Routine

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Quality of Service** button.
- Step 4** In the Quality of service support field, set the required IP ToS value for each media type by clicking one of the following radio buttons:
- None—Select to disable Quality of Service support
 - Default—Select to assign the default IP ToS value for each media type. The default settings represent Cisco recommendations.
 - Custom—Select to assign your own IP ToS value for each media type.
- If you select **Default**, the system automatically enters Quality of Service settings. If you select **Custom**, follow the steps below.
- Step 5** In the Voice Priority field of the Video Calls section, enter a whole number from 0 to 63 to set the priority level of voice packets that the MCU sends out. The default value is 34.
- Step 6** In the Video Priority field of the Video Calls section, enter a whole number from 0 to 63 to set the priority level of video packets that the MCU sends out. The default value is 34.
- Step 7** In the Voice Priority field of the Voice Calls section, enter a whole number from 0 to 63 to set the priority level of voice packets that the MCU sends out. The default value is 46.
-

Configuring MCU Dynamic Layouts

In the Dynamic Layouts section of the Settings tab you can define the exact layout transition order used by conferences.

Dynamic layouts are activated individually for each service. When selected, the conference layout changes automatically as participants join or leave.

Procedure

- Step 1** In the Administrator interface, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.

- Step 3** Click the **Dynamic Layouts** button.
- Step 4** Click a layout image to select or deselect that specific layout.

Configuring MCU Alert Indications

In the Alert Indications section of the Settings tab, you can select which events trigger Simple Network Management Protocol (SNMP) traps. You can also define multiple SNMP servers to which the MCU sends the SNMP traps and configure which events to display in the Event Log tab.

This section describes the following topics:

- [Enabling Cisco Unified Videoconferencing 3515 MCU Alert Indications and Setting Security Levels, page 2-7](#)
- [Configuring SNMP Trap Servers, page 2-9](#)
- [Editing SNMP Trap Servers, page 2-9](#)
- [Deleting SNMP Trap Servers, page 2-10](#)

Enabling Cisco Unified Videoconferencing 3515 MCU Alert Indications and Setting Security Levels

In the Alert Indications section of the Settings tab, you can configure which alerts will be enabled and set a severity level for each one.

[Table 2-3](#) lists alert indications as well as the SNMP trap associated with them.

[Table 2-4](#) lists the structure of the standard *coldStart* and *warmStart* traps (as defined in RFC 1907) and the standard *linkDown* and *linkUp* traps (as defined in RFC 1573).

Table 2-3 *MCU Alert Indications*

Event Type	Trap is sent when...
Abnormal disconnect	A call disconnects for a reason other than normal, busy, or no answer.
Authentication failure	The conference PIN is incorrect.
Call disconnected by remote endpoint	A call disconnects normally by a remote endpoint.
Corrupt WEB data	Corrupt web files are present in the MCU.
Gatekeeper registration state change	A change occurs in the registration status of the MCU with the gatekeeper.
General alarm	A system failure is detected.
Incompatible software version install	An attempt to burn a version of the MCU software onto incompatible hardware occurs.
Loss of Ethernet	The network returns after going down. Indicates the time at which the network was restored.
MP lost	Communication with a registered media processor has broken.
MP registration failure	The media processor registration to the MCU failed.
Max resource meter	A high CPU level (85%) is reached in the MCU.
Network problem	A problem occurs on the network.

Table 2-3 *MCU Alert Indications (continued)*

Event Type	Trap is sent when...
Overheating	The configured temperature thresholds for the device are exceeded. Overheating can cause serious damage to the functioning of the device.
Power-down	The MCU is shutting down.
Power-up	The MCU has begun operation.
Services table is changed	The service table has been modified.

Table 2-4 *Standard SNMP Trap Event Types*

Event Type	Trap is sent when...
Cold start	The MCU has been reset using the button on the front panel.
Warm start	A reset of the MCU has been performed using the Administrator interface.
Link down	Standard SNMP MIB trap indicating that the network connection is down with details about the cause and time of connection loss.
Link up	Standard SNMP MIB trap indicating that the network connection has been reestablished.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Alert Indications** button.
- Step 4** In the Events section, select the check boxes in the **Enabled in the Event Log** column for all the events that you want to display in the event log.
- Step 5** For each event you enable, choose one of the following severities in the Severity column:
 - Cleared—Enumeration 0. One or more previously reported alarms have been cleared.
 - Information—Enumeration 1. Notification of a non-erroneous event.
 - Critical—Enumeration 2. A service-affecting event has occurred and requires immediate corrective action.
 - Major—Enumeration 3. A service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.
 - Minor—Enumeration 4. A non-service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.
 - Warning—Enumeration 5. A potential or impending service-affecting event has been detected, but no significant events have occurred yet. Action should be taken to further diagnose and correct the problems to prevent the condition becoming more serious.



Tip

You can click the **Select All** button to select all events or the **Clear All** button to clear all events.

Configuring SNMP Trap Servers

In the Alert Indications section of the Settings tab, you can define the IP address, port, and enabled traps for multiple SNMP trap servers to which the MCU sends the SNMP traps, and specify which events to display in the Event Log tab.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Alert Indications** button.
- Step 4** In the SNMP Traps Server section, click **Add**.
The SNMP Trap Servers Properties dialog box appears.
- Step 5** In the SNMP Trap server address field, enter the address for the SNMP trap server.
- Step 6** In the Port field, enter the port of the SNMP trap server. The default port for SNMP servers is 162.
- Step 7** In the Enabled traps section, select which traps you want to enable:
- To disable a trap, click it in the Enabled traps area and then click **Remove**.
 - To enable a trap, click it in the Disabled traps area and then click **Add**.
 - To enable all traps, click **Add All**.
 - To disable all traps, click **Remove All**.
- Step 8** Click **Upload** to save your settings.
The configured SNMP trap server appears in the SNMP Trap Servers section.
-

Editing SNMP Trap Servers

In the Alert Indications section of the Settings tab, you can edit a configured SNMP trap server.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Alert Indications** button.
- Step 4** In the SNMP Trap Servers section, click the configured SNMP trap server and then click the **Edit** button.
- Step 5** Click **Upload** when you finish your edits.
-

Deleting SNMP Trap Servers

You can delete configured SNMP trap servers in the Alert Indications section of the Settings tab.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Alert Indications** button.
- Step 4** In the SNMP Trap Servers section, click the configured SNMP trap server and then click **Delete**.
-

Viewing Media Processors for the 3515 MCU

In the Media Processing tab, you can view the list of data and video processors and servers currently registered with the MCU and access the web interface (if available) of registered devices to modify settings. The Media Processing tab includes the following columns and fields:

- **Type**—This column displays the types of media processors registered with the current MCU. The following types can appear in this column:
 - **MCU**—The MCU itself which is responsible for the signaling (H.323/SIP) and audio portions of a call.
 - **EMP**—The video processor responsible for the video portion of a call.
- **IP Address**—This column displays the IP address of the device on which the media processor operates.
- **Description**—This column displays a user-defined description of the media processor.
- **Total**—This field displays the total number of media processor units currently registered.

Viewing the Event Log for the 3515 MCU

The Event Log tab displays a list of reported alarm events. These events are configured in the Alert Indications section of the Settings tab.

The Event Log tab displays the following information:

- **Event ID**—Displays the identifier for the specified alarm event.
- **Type**—Displays the type of event.
- **Time**—Displays the date and time when the reported event occurred.
- **Severity**—Displays the severity of the reported event.
- **Message**—Displays the error message used to report the event

Saving Configuration Settings for the 3515 MCU

You can save MCU configuration settings to a file and then export this file to a storage device on your network. You can use the saved configuration file to restore the settings to the current MCU or to configure a similar MCU.

An exported configuration file saves most of the current Device section settings and all of the current MCU section settings.

You must use the Export button on the toolbar to save the configuration settings to a file. The Export button appears only when MCU section settings are activated. When you save a configuration file, the current Device section settings are saved in the file. If you want to change these settings for export, click **Upload** on the toolbar to save these settings to configuration memory prior to saving the configuration file.

Procedure

-
- Step 1** In the MCU interface, on the sidebar, click **Device**.
- Step 2** Make sure that the settings in the Basics, Addressing, Web and Users tabs are correct.



Note Date parameters are not saved to the configuration file.

- Step 3** Click **Upload** to save these settings.
- Step 4** On the sidebar, click **MCU**.
- Step 5** Review each of the configuration pages to ensure that these are the configuration settings you want to save.
- Step 6** Click **Upload** to save these settings.
- Step 7** On the toolbar, click **Export**.



Note A dialog box appears indicating that you are navigating away from the page without saving the changes. Select the option to continue.

The File Download dialog box appears.

- Step 8** Save the configuration settings file to your chosen location. The file extension *.ini* is automatically appended to the file name.
-

Importing Configuration Settings for the 3515 MCU

You can import the settings of a saved MCU configuration file from a storage device on your network. You can use the saved configuration file to restore the settings to the current MCU or to configure another MCU.

Procedure

- Step 1** In the MCU interface, on the sidebar, click **MCU**.
- Step 2** On the toolbar, click **Import**.
The Import a Configuration File page appears.
- Step 3** Click **Browse**.
The Choose file dialog box appears.
- Step 4** Navigate to and select the configuration file you want to import.



Note The file must have an *.ini* extension.

- Step 5** Click **Open**.
The file path appears in the File Name field.
- Step 6** Click **Import**.



Note You can verify the settings by clicking **MCU** or **Device** on the sidebar. However, to save the settings in either section, you must click **Upload** to save them before viewing the next section.

- Step 7** Click **Upload** to save the settings in configuration memory.



Note Uploading the file resets the device.



Advanced Configuration for the Cisco Unified Videoconferencing 3515 MCU

This section describes the following topics:

- [Configuring Conference Management Settings for the 3515 MCU, page 3-1](#)
- [Configuring Delimiter Settings for the 3515 MCU, page 3-2](#)
- [Disconnecting Participants on Communications \(ICMP\) Failure for the 3515 MCU, page 3-3](#)
- [Sending Advanced Commands for the 3515 MCU, page 3-3](#)
- [Opening a Telnet Terminal for the 3515 MCU, page 3-7](#)

Configuring Conference Management Settings for the 3515 MCU

In the Advanced section of the Settings tab, you can configure settings for conference registration with the gatekeeper and determine how participants can create and join conferences.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Advanced** button.
- Step 4** Select **Register conference ID** to register existing conference IDs with the gatekeeper and SIP server to enable participants dialing in to a conference from remote locations to connect to the target conference on the MCU. This setting is deselected by default.



Note When working with SIP, you must configure a registrar.

- Step 5** In the Conferences can be created using field, choose one of the following methods through which conferences can be created:
 - Scheduler only—Enables conference creation only using a conference scheduling application
 - Scheduler, Web and Control API—Enables conference creation using a conference scheduling application, the Conference Control interface, or an external application that uses the MCU API.

- Scheduler, Web, Control API and dial-in (default)—Enable all the conference creation methods listed above, as well as dial-in for ad-hoc conference creation.
- Step 6** Select **When using the web, only operators or administrators can create a conference** to grant conference creation authorization only to users with Administrator or Operator privileges. If you want users with all levels of access to be able to create a conference, leave this option deselected.
- Step 7** In the Participants can join the conference using field, choose one of the following methods through which participants can join a conference:
- Invite only—Participants can join a conference only when the MCU dials that participant.
 - Invite and dial-in—Participants can join a conference either by MCU invitation or by dialing directly using a conference ID.
- Step 8** In the Ad hoc conferences terminate when field, choose the method through which dial-in (ad hoc) conferences terminate:
- Last participant leaves—The conference terminates when the last participant leaves the conference.
 - Conference creator leaves—The conference terminates when the conference creator leaves the conference.
- Step 9** In the External conference authorization policy field, choose one of the following MCU authorization policies for creating or joining conferences:
- None—No authorization required.
 - Notify—The MCU notifies an external application such as a conference scheduler that accesses or controls MCU resources about conference creation or joining.
 - Authorize—The MCU requests authorization from an external application such as a conference scheduler which accesses or controls MCU resources to create conferences or allow participants to join conferences.
-

Configuring Delimiter Settings for the 3515 MCU

You can specify a conference PIN or invite multiple participants as part of the string for dialing into the MCU.

In the Advanced section of the Settings tab, you can configure the conference PIN delimiter and the multiple invite delimiter.

Procedure

-
- Step 1** In the Administrator interface, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Advanced** button.
- Step 4** In the PIN delimiter field, enter the characters used as a separator between the conference ID and conference PIN when dialing into a conference. A conference is created with this PIN if no conferences already exist with the specified number. Valid delimiters include the pound sign (#) and asterisk (*). The default PIN delimiter setting is three asterisks (***)

- Step 5** In the Invite delimiter field, enter the characters used to separate participant numbers in multiple participant invitation. Valid delimiters include the pound sign (#) and asterisk (*). The default invite delimiter setting is two asterisks (**).
-

Disconnecting Participants on Communications (ICMP) Failure for the 3515 MCU

When the MCU sends audio or video data to an unreachable endpoint, the network notifies the MCU using the ICMP protocol. The MCU can detect ICMP messages and disconnect the endpoint automatically. You enable automatic endpoint disconnection in the Advanced section of the Settings tab. If this option is not selected, the MCU ignores ICMP error packets.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Advanced** button.
- Step 4** Select **Disconnect participants on communication (ICMP) failure**.
- Step 5** In the Disconnect on field, make one of the following selections:
- **Audio failure**—The call disconnects only if the audio connection fails. The call continues if the video connection fails and the audio connection remains. This is the default setting.
 - **Audio or video failure**—The call disconnects if either the audio or video connection fails.
-

Sending Advanced Commands for the 3515 MCU

In the Advanced section of the Settings tab, you can send text-based commands used for the enhanced control of the MCU. Advanced commands are not case-sensitive.



Note

We recommend that only advanced users or users who have consulted with Cisco Customer Support perform actions involving advanced commands.

[Table 3-1](#) lists all available advanced commands.

Table 3-1 List of Available Advanced Commands

Command	Description	Parameters	Default
Conference control Web refresh interval	Indicates the length of time (in seconds) after which the Conference Control interface refreshes automatically.		10
DTMF forwarding	Indicates the target of DTMF forwarding.	to all—All endpoints in the conference. to gateways—To gateways only. to none—DTMF is disabled.	none
Enable in-band DTMF detection	Enables support for in-band DTMF signaling.	Always or Only during IVR	Always
First audio announcement interval (msec)	Indicates the length of time (in milliseconds) between the start of the conference and the first audio announcement.		Disabled
Font align	Determines whether text overlay (TOL) on a video screen is positioned away from picture borders.	All—Text positioned away from horizontal and vertical borders. Horizontal—Text positioned away from horizontal borders and centered horizontally. Vertical—Text positioned away from vertical borders and centered vertically. None—Text is always positioned bottom center.	All
G.728 mode	Determines the form of encoding for the G.728 audio codec RTP header.	Non-standard—For use if you experience audio problems when using VCON endpoints with the G.728 audio codec. Standard—For normal G.728 use with all endpoints except VCON products.	

Table 3-1 List of Available Advanced Commands (continued)

Command	Description	Parameters	Default
H323 hide stack	Disables H.323 stack prints.		H.323 Stack printing is disabled by default.
H323 show stack	Enables H.323 stack prints. These print the protocol stack info and errors and are useful for debugging stack issues		
H323 show status	Prints a snapshot of H.323 stack-related information.		
Handle DTMF after XML notification	Instructs the MCU to send DTMF signals to an external server and other specified destinations.	no—MCU sends DTMF signals to the external server only. yes—MCU sends DTMF signals to the external server and to the destination set by the DTMF forwarding advanced command.	
NTP synchronization period	Sets the Network Time Protocol synchronization period (in seconds) between the EMP and the NTP server.		21600
Notify level	Sets the MCU log notify level filter	Fatal—MCU cannot continue to provide service (unrecoverable error). Error—User functionality problem (for example, call connect failure or no resources available). Warning—User functionality problem but the MCU can continue to provide service. Info—Status prints for Customer Support use. Advanced—Like Info but more detailed. Debug 1 through Debug 4—Debug levels.	Debug 3

Table 3-1 List of Available Advanced Commands (continued)

Command	Description	Parameters	Default
QualiVision Settings hide	Disables the QualiVision Settings section in the Settings tab.		The QualiVision Settings section is hidden by default.
QualiVision Settings show	Enables the QualiVision Settings section in the Settings tab.		
SCCP hide stack	Disables SCCP stack prints.		
SCCP show status	Prints a snapshot of SCCP stack related information.		
Set MTU size	Determines the maximum packet size across the network.		1500
Set terminal baud rate	Sets the baud rate of a serial terminal.	High (57600) Low (9600)	Low (9600)
Support RFC 2833 capability	Enables support for in-band DTMF signaling via packets within the audio channel as defined in the RFC 2833 standard.	disable or enable	enable

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Settings** tab.
- Step 3** Click the **Advanced** button.
- Step 4** Click **Commands**.
- The Advanced Commands dialog box appears.
- Step 5** In the Command field, enter a command or choose one from the Available Commands field.
- Step 6** In the Parameters field, enter a parameter value for the command (where applicable) or choose one from the Available Parameters field.
- Step 7** Click **Send**.
- The results of the advanced command appear in the Response field, indicating whether or not the MCU received and executed the command. If you send an invalid command, a “bad parameter” or “NOT FOUND” message appears.
-

Opening a Telnet Terminal for the 3515 MCU

In the Advanced section of the Settings tab, you can open a Telnet terminal to log error and troubleshooting information.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
 - Step 2** Click the **Settings** tab.
 - Step 3** Click the **Advanced** button.
 - Step 4** Click **Telnet**.
 - Step 5** A separate browser opens with a Telnet terminal. When you finish with your Telnet session, click **Disconnect**.
-



Protocols and the Cisco Unified Videoconferencing 3515 MCU

In the Protocols tab, you can configure the MCU to work with H.323, Session Initiation Protocol (SIP), and Skinny Client Control Protocol (SCCP) call-routing devices. The following sections detail the three types of call-routing devices you can configure the MCU to work with:

This section describes the following topics:

- [Configuring H.323 Gatekeeper Settings for the Cisco Unified Videoconferencing 3515 MCU, page 4-1](#)
- [Integrating SIP with the Cisco Unified Videoconferencing 3515 MCU, page 4-3](#)
- [Configuring the Cisco Unified Videoconferencing 3515 MCU to Use Cisco Unified CallManager, page 4-8](#)

Configuring H.323 Gatekeeper Settings for the Cisco Unified Videoconferencing 3515 MCU

In the Protocols tab, you can view and configure settings for H.323 gatekeeper and SIP call routing devices. The following sections detail the tasks you can perform in the Protocols tab:

- [Configuring H.323 Gatekeeper Protocol Configuration, page 4-1](#)
- [Configuring Advanced H.323 Gatekeeper Protocol Settings, page 4-2](#)

Configuring H.323 Gatekeeper Protocol Configuration

In the Protocols tab, you can configure the protocol settings of an H.323 gatekeeper to set how the MCU and the gatekeeper interact.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Make sure the H.323 button is selected.
The H.323 Protocol Configurations dialog box appears.

- Step 4** Select **Enable H.323 protocol** to enable the MCU to operate with the H.323 protocol.
- Step 5** In the Gatekeeper Address field, enter the IP address of the gatekeeper.
- Step 6** In the Gatekeeper Port field, enter the port number of the gatekeeper. The default port is 1719.
- Step 7** Select **Strip local gatekeeper zone prefix if it appears in incoming calls** if you want the MCU to strip the gatekeeper zone prefix from the dialed string of an incoming call. For example, if the zone prefix is 01 and you have selected this option, the MCU removes 01 from every dial string beginning 01. Do not use this feature if the gatekeeper is already set to perform zone stripping.
- Step 8** If you did not perform step 7, skip to step 9. Otherwise, in the Local Zone Prefix field, enter the gatekeeper zone you want to strip.
- Step 9** Click **Upload**.



Warning

Changing gatekeeper settings does not reset the MCU, but might disconnect active calls.



Tip

In the Edit H.323 Protocol Configurations dialog box, you can click **Go to Gatekeeper** to connect to a third-party gatekeeper that uses a web interface.

Configuring Advanced H.323 Gatekeeper Protocol Settings

In the Protocols tab, you can configure advanced settings for MCU communication with an H.323 gatekeeper.

Before You Begin

Make sure the basic H.323 gatekeeper protocol settings are correct. See the [“Configuring H.323 Gatekeeper Protocol Configuration”](#) section on page 4-1 for more information.

Procedure

- Step 1** In the H.323 Protocol Configurations dialog box click the Advanced H.323 Settings button. The Advanced H.323 Setting dialog box appears.
- Step 2** In the RAS Port field, enter the port on which the MCU conducts RAS registration messaging with the gatekeeper. The default port is 2719.
- Step 3** In the Signaling Port field, enter the port on which the MCU carries call signaling messages to and from the gatekeeper. The default port is 2720.
- Step 4** In the Registration refresh every field, enter the interval (in seconds) between registrations of the MCU to the gatekeeper. The default value is 60 seconds.
- Step 5** In the MCU Registration Mode field, choose the mode of registration with the H.323 gatekeeper.
- MCU—Use this setting to connect H.323 calls via the MCU.
 - Gateway—Use this setting to register the MCU as a gateway. This option enables the MCU to work with a Cisco MCM gatekeeper. This is the default setting.

- Step 6** Select **Enable Fast Start** to speed up the connection time between the MCU and incoming calls received through the gatekeeper. Channel setup messages are encapsulated within Q.931 setup messages. When you enable this option, the MCU offers Fast Start channels to any outgoing call and attempts to select from channels offered in incoming calls.
- Step 7** Select **Enable H.245 tunneling** to enable H.245 tunneling during call setup and connection between the MCU and incoming calls received through the gatekeeper.



Note The H.245 tunneling feature works only with endpoints and gatekeepers that support H.245.

- Step 8** Click OK.

Integrating SIP with the Cisco Unified Videoconferencing 3515 MCU

This section describes how to configure the MCU and use different dialing plans for working in a Session Initiation Protocol (SIP) environment. The section describes the following topics:

- [Configuring SIP Proxy Settings, page 4-3](#)
- [Configuring Advanced SIP Proxy Settings, page 4-4](#)
- [About the MCU Dial Plan, page 4-5](#)

Configuring SIP Proxy Settings

You can configure settings for SIP registrar profiles which set how the MCU and the registrar interact.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Make sure the SIP button is selected.
The SIP Protocol Configurations dialog box appears.
- Step 4** Select **Enable SIP protocol** to enable MCU communication with the SIP proxy.
- Step 5** In the Default SIP domain field enter the SIP domain of the MCU as defined in the SIP server. An example of a SIP domain is company.com.
- Step 6** Select **Using Microsoft LCS** to enable the MCU to work with Microsoft Office Live Communication Server (LCS).
- Step 7** In the SIP Server section, choose one of the following options:
- Select **Locate server automatically (using DNS)** if you wish the MCU to automatically locate one of the SIP proxy servers that are present in the domain.



Note The Locate servers automatically (using DNS) option will only work if you have configured a valid IP address in the Board | Addressing | Preferred DNS server or Alternate DNS server field.

- Select **Specify address** and enter the following:
 - An IP address or host name of the SIP proxy, for example proxy.company.com.
 - In the port field enter the communication port number of the SIP proxy address.
 - In the type field select the transport connection type for sending messages to the SIP proxy according to the type supported by the SIP proxy—UDP or TCP. This field is mandatory. The default is UDP.
- Step 8** Select **Treat as outbound proxy** if you wish the MCU to send all the SIP messages to the configured SIP proxy server. This is optional. The default is unchecked.
- Step 9** Select **Use Registrar** if you wish the MCU to register with the SIP registrar using the name defined in the Registration name field, and to send service information to the registrar.
- Step 10** If you selected Use Registrar in step 9, enter the following information:
 - In the Address field enter the IP address or the host name of the SIP registrar. This field is mandatory.
 - In the port field enter the communication port number of the SIP registrar address.
 - In the type field select the transport connection type for sending registration requests to the registrar according to the type supported by the SIP registrar—UDP or TCP. This field is mandatory. The default is UDP.
- Step 11** In the Local signaling port field enter the number of the signaling port on which the MCU communicates with the SIP proxy. The default is 5060.

Configuring Advanced SIP Proxy Settings

In the Protocols tab, you can configure advanced settings for MCU communication with a SIP Proxy.

Before You Begin

Make sure the basic SIP proxy settings are correct. See the [“Configuring SIP Proxy Settings” section on page 4-3](#) for more information.

Procedure

- Step 1** In the SIP Protocol Configurations dialog box click **Advanced SIP Settings**.
The Advanced SIP Setting dialog box appears.
- Step 2** In the “From” header field select an addressing format that the MCU will use for the information sent in the “From” header of messages for outgoing calls.
 - Select **Use local signaling IP address** if you wish the MCU to use its local signaling IP address.
 - Select **Use fully qualified domain name (FQDN)** if you wish the MCU to use the FQDN. Enter the fully qualified domain name of the MCU, for example, mcu.company.com.

- Step 3** In the “Contact” header field select the addressing format that the MCU will use for the information sent in the “Contact” header of messages for outgoing calls.
- Select **Use local signaling IP address** if you wish the MCU to use its local signaling IP address.
 - Select **Use fully qualified domain name (FQDN)** if you wish the MCU to use the FQDN. Enter the fully qualified domain name of the MCU, for example, mcu.company.com.
- Step 4** Select **Use proxy digest authentication** to enable MCU authentication with a SIP proxy server using user name and password. Authentication is performed as defined in RFC 2617. This field is disabled by default.
- Step 5** If you selected Use proxy digest authentication in step 4, enter the following:
- In the User name field enter the MCU user name. The user name must match the name defined on the SIP proxy server.
 - In the Password field enter the MCU user password. The user password must match the password defined on the SIP proxy server.
- Step 6** Select **Use registrar digest authentication** to enable MCU authentication with a SIP registrar server using user name and password. Authentication is performed as defined in RFC 2617. This field is disabled by default.
- Step 7** If you selected Use registrar digest authentication in step 6, enter the following:
- In the User name field enter the MCU user name. The user name must match the name defined on the SIP registrar server.
 - In the Password field enter the MCU user password. The user password must match the password defined on the SIP registrar server.
- Step 8** Select **Enable Video Fast Update** to enable transport of Video Fast Update (VFU) requests to SIP endpoints.
- Step 9** Select **Support reliable provisional response (RFC 3262)** to enable the remote endpoint to request that the source endpoint sends an acknowledgment on receipt of 10x SIP messages.
- Step 10** Select **Use ‘Empty Invite’ when sending Invite messages to endpoints** to enable the remote endpoint to indicate preferred audio and video channels.
- Step 11** Click **OK**.
-

About the MCU Dial Plan

You can configure the MCU on a SIP network in one of the following two ways:

- The MCU functions as a User Agent Client (UAC) which provides video, voice and data conference services.
- The MCU is defined as a separate domain that provides conferences services.

The following sections describe these configurations:

- [About Outgoing Calls from the MCU, page 4-6](#)
- [About Incoming Calls to the MCU, page 4-6](#)
- [Configuring the MCU as a UAC, page 4-6](#)
- [Configuring the MCU to Perform as a Separate SIP Domain, page 4-7](#)

About Outgoing Calls from the MCU

Making outgoing calls from the MCU is the same whether it operates as a UAC or as a separate SIP domain. All MCU outgoing SIP messages are sent through the proxy. The proxy activates an address resolution algorithm by consulting with a registrar or a DNS server or any other location server and routes the message to the correct destination.

**Note**

If the user does not specify a domain in the dialing string, the MCU appends the default domain to the dialed string. You can configure the default domain in the SIP section of the Protocols tab. See the [“Configuring SIP Proxy Settings” section on page 4-3](#) for more information.

About Incoming Calls to the MCU

The MCU dial plan for incoming calls varies according to whether the MCU is configured as a UAC registered to the domain registrar or as a separate SIP domain.

**Note**

Whether working as a UAC or separate SIP domain, you can dial into the MCU from a UAC by dialing a `conference.id@mcu.ip.address` URI and the call should always reach the MCU.

Configuring the MCU as a UAC

In the Protocols tab, you can configure the MCU to function as a UAC. When configured as a UAC, the MCU registers all services and conferences with a registrar. We recommend that you configure the MCU as a UAC when working with a scheduler or in an environment that does not require ad hoc conference creation. In this configuration, the UAC can only dial directly into the MCU by using a conference ID that has previously registered with the registrar.

Ad hoc conference creation using conference services, familiar in an H.323 environment, is not supported in a SIP environment. When a SIP UAC dials into the MCU to a conference that does not yet exist, the proxy cannot resolve the MCU address because the dialed conference ID is not registered with a registrar.

The MCU registers each MCU service and conference using the default domain defined in the MCU SIP configuration and SIP proxy server as follows:

- Service: 60@company.com
 - 60—MCU service prefix
 - @company.com—MCU default domain
- Conference: 601234@company.com
 - 601234—MCU conference ID (service prefix + unique conference identifier)
 - @company.com—MCU default domain on which the conference is hosted.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Make sure the SIP button is selected.

The SIP Protocol Configurations dialog box appears.

- Step 4** Select **Use registrar**.
- Step 5** In the Default Domain field, enter the default domain name as defined in the SIP proxy server.
- Step 6** Click the **Settings** tab and then click the **Advanced** button.
- Step 7** Make sure that the Register conference ID check box is selected.



Note The MCU must use the registrar to register conference IDs. Conferences cannot be found if the registrar has no record that they exist, causing all calls to conferences to fail.

Configuring the MCU to Perform as a Separate SIP Domain

You can configure the MCU to perform as a separate domain within the default domain. The default domain is the domain in which the MCU operates as defined in the SIP proxy server. Every SIP request that the proxy receives that ends with the unique domain name of the MCU routes directly to the MCU. The MCU then directs the call to the appropriate conference. Pre-registering the conference IDs with the registrar is not required.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Make sure the SIP button is selected.
The SIP Protocol Configurations dialog box appears.
- Step 4** In the Default Domain field, enter the name of the domain in which the MCU operates.
For example, company.com.
- Step 5** Configure the unique domain name of the MCU in the proxy internal routing tables (if supported) or in the relevant DNS server:
 - For proxy internal routing tables, configure a rule such as:
Every URI of type *(any number)@mcu.company.com should be routed to the MCU IP address.
 - For a DNS server, define a new rule entry of mcu.company.com. The address of this entry is the MCU IP.



Note Make sure that the MCU domain configured in the proxy is different from the default domain. If the MCU default domain is company.com, then configure the MCU domain as mcu.company.com.

Configuring the Cisco Unified Videoconferencing 3515 MCU to Use Cisco Unified CallManager

To set up the Cisco Unified Videoconferencing 3515 MCU to use Cisco Unified CallManager which uses the Skinny Client Control Protocol (SCCP), you must enable the MCU to support SCCP. Then you must identify the Trivial File Transfer Protocol (TFTP) server that you want the MCU to use. This allows the MCU to contact the Cisco Unified CallManager and obtain configuration information specific to that Cisco Unified CallManager. You must also set pertinent MCU parameters for proper operation. You set the MCU-based parameters in the Administrator interface and you can set the Cisco Unified CallManager-based parameters in the Cisco Unified CallManager. The Cisco Unified CallManager-based parameters upload to the MCU and appear in the Administrator interface after contact is made.



Note

When you boot up, the Cisco Unified Videoconferencing 3515 MCU reports EMP resources associated with SCCP conferences to Cisco Unified CallManager. These resources are reserved and subtracted from the remaining MCU resources available to H.323 conferences.

- [Viewing SCCP Protocol Configurations, page 4-8](#)
- [Configuring the SCCP Protocol, page 4-9](#)
- [Configuring a TFTP Server, page 4-9](#)
- [Adding a Cisco Unified CallManager, page 4-10](#)
- [Viewing Advanced SCCP Protocol Settings, page 4-10](#)
- [Configuring Advanced SCCP Protocol Settings, page 4-11](#)

Viewing SCCP Protocol Configurations

In the Protocols tab, you can view existing SCCP protocol configurations.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Click the **SCCP** button.

The SCCP Protocol Configurations dialog box displays the following settings:

- Enable SCCP protocol—Indicates whether or not the SCCP protocol is enabled.
- Active SCCP service prefix—Indicates the current prefix for SCCP services.
- Ports allocated to SCCP—Indicates the number of ports currently available for SCCP use.
- TFTP Servers—The IP address of the primary TFTP server that the MCU uses.
- CallManagers—The IP address of the Cisco Unified CallManager that the MCU uses.

Configuring the SCCP Protocol

In the Protocols tab, you can configure the Cisco Unified Videoconferencing 3515 MCU to support SCCP in Cisco Unified CallManager.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Click **SCCP**.
- The SCCP Protocol Configurations dialog box appears.
- Step 4** Select **Enable SCCP protocol** to allow the MCU to support the SCCP protocol.
- Step 5** In the Active SCCP service prefix field, enter the prefix assigned to the MCU service that you want the Cisco Unified CallManager to use.



Note A default service prefix is automatically entered in this field. If you want to use this service, make sure that this is a valid service prefix for your network environment.

- Step 6** In the Ports allocated to SCCP, enter the number of ports you want to make available for SCCP use.
-

Configuring a TFTP Server

In the Protocols tab, you can configure the TFTP server that you want the MCU to use.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Click **SCCP**.
- The SCCP Protocol Configurations dialog box appears.
- Step 4** In the TFTP Servers section, identify the TFTP server that you want the MCU to use.



Note This information appears automatically when you use the terminal emulator to set a TFTP server address. You can edit this information or add a different TFTP server.

- Step 5** In the TFTP Servers section, click **Add** (or **Edit**).
- The Add (or Edit) TFTP Server dialog box appears.
- Step 6** In the IP address field, enter the IP address of the TFTP server you want the MCU to use to contact the Cisco Unified CallManager.
- Step 7** In the Port field, enter the port number that you want the MCU to use to communicate with the TFTP server.

- Step 8** Click **OK** to save these changes and close the Add (or Edit) TFTP server dialog box.

Adding a Cisco Unified CallManager

In the Protocols tab, you can manually add a Cisco Unified CallManager.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Click **SCCP**.
- The SCCP Protocol Configurations dialog box appears.
- Step 4** Select **Change configuration locally** to manually add another Cisco Unified CallManager and configure SCCP settings for this Cisco Unified CallManager.
- The Add button is activated.
- Step 5** Click **Add**.
- The Add CallManager dialog box appears.
- Step 6** Set the required IP address and port number for the Cisco Unified CallManager and click **OK**.
- The new Cisco Unified CallManager appears in the CallManagers section.
- Step 7** Click **OK** to save your changes.

Viewing Advanced SCCP Protocol Settings

In the Advanced SCCP Settings dialog box, you can view parameters controlling the communication between the MCU and the Cisco Unified CallManager.

[Table 4-1](#) describes the elements that appear in the Edit SCCP Protocol Configuration dialog box.

Table 4-1 Edit SCCP Protocol Configuration Dialog Box

Field	Description
Control Channel	
Local port base	Indicates the communication port that you want the MCU to use to communicate with the Cisco Unified CallManager.
Priority (0-63)	Indicates the Differentiated Services Code Point (DSCP) value the Cisco Unified CallManager specifies that the MCU use for Quality of Service (QoS).
Registration	
Retries	Indicates the number of times the MCU will attempt to register with the Cisco Unified CallManager.

Table 4-1 Edit SCCP Protocol Configuration Dialog Box (continued)

Field	Description
Initial timeout (sec)	Indicates the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on the first attempt to register.
Consequent timeout (sec)	Indicates the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on subsequent attempt to register.
Keep Alive	
Retries	Indicates the number of times the MCU will send the Keep Alive message to the Cisco Unified CallManager before acknowledging that the connection has failed.
Timeout (sec)	Indicates the interval at which the MCU sends Keep Alive messages.
Fail Over	
Recovery mode	Indicates the mode with which the MCU terminates calls when the connection to the Cisco Unified CallManager fails: <ul style="list-style-type: none"> • gracefully—Allows completion of current calls. • immediately—Terminates conference immediately. • timeout—Allows all conferences to continue for the interval specified in the Recovery timeout (sec) field.
Recovery timeout (sec)	Indicates the length of time the MCU allows calls to continue after the connection with the Cisco Unified CallManager fails.

Configuring Advanced SCCP Protocol Settings

In the Advanced SCCP Settings dialog box, you can configure parameters controlling the communication between the MCU and the Cisco Unified CallManager.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Protocols** tab.
- Step 3** Click **Advanced SCCP Settings**.
The Advanced SCCP Settings dialog box appears.
- Step 4** In the Local port base field, enter a value for the communication port that you want the MCU to use to communicate with the Cisco Unified CallManager.

You can use values between 11000 and 16000. The default value is 11000.



Note You must also set this value in the Cisco Unified CallManager.

- Step 5** In the Priority (0-63) field, enter the Differentiated Services Code Point (DSCP) value the Cisco Unified CallManager specifies that the MCU use for Quality of Service (QoS). You must convert the value to decimal notation.
- Step 6** In the Retries field of the Registration section, enter a value setting the number of times you want the MCU to attempt to register with the Cisco Unified CallManager.
- Step 7** In the Initial timeout (sec) field, enter a value in seconds setting the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on the first attempt to register.
- Step 8** In the Consequent timeout (sec) field, enter a value in seconds setting the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on subsequent attempt to register.
- Step 9** In the Retries field of the Keep Alive section, enter a value setting the number of times you want the MCU to send the Keep Alive message to the Cisco Unified CallManager before acknowledging that the connection has failed.
- Step 10** In the Timeout (sec) field, enter a value in seconds setting the interval at which the MCU sends Keep Alive messages.
- Step 11** In the Recovery mode field, choose the mode with which you want the MCU to terminate calls when the connection to the Cisco Unified CallManager fails:
- gracefully—Allow completion of current calls.
 - immediately—Terminate conference immediately.
 - timeout—Allow all conferences to continue for the interval specified in the Recovery timeout (sec) field.
- Step 12** If you select timeout in the Recovery mode field, enter a value in seconds in the Recovery timeout (sec) field to set the length of time the MCU allows calls to continue after the connection with the Cisco Unified CallManager fails.
- Step 13** Click **OK** to save your changes.
- Step 14** Click **Cancel** to close the Advanced SCCP Settings dialog box without saving changes.
-



Cisco Unified Videoconferencing 3515 MCU Services

This section introduces services, describes how to work with them, and includes the following topics:

- [About Services, page 5-1](#)
- [Working with Services on the 3515 MCU, page 5-2](#)
- [Configuring Advanced Management and Security for the 3515 MCU, page 5-11](#)

About Services

A service can be regarded as a conference template. A service is the mechanism that defines the qualities and capabilities of a conference. A service is identified by its prefix. The service prefix number is incorporated into the conference ID to specify the service for the conference. A description of the service indicates the main attributes of the service or the target use for the service.

The MCU comes with four predefined services for audio and video conferencing, for use with the SCCP protocol and for use with Cisco Unified MeetingPlace. The predefined services are factory tuned to be suitable in most cases for audio and video calls. We recommend starting with these services and modifying them as necessary to suit your needs.

When using an SCCP service the following limitations apply:

- No support for presentation view (Duo Video and H.239)
- No support for T.120 data collaboration
- No support for H.235 encryption
- Maximum resolution supported is CIF
- Maximum call rate supported is 768 Kbps
- The G.722.1 and G.723 audio codecs are not available
- No support for conference PINs
- No support for dial out

Working with Services on the 3515 MCU

This section describes how to create new services and how to configure your own services settings.

- [Creating a New Service, page 5-2](#)
- [Creating a New SCCP Service, page 5-3](#)
- [Customizing Services, page 5-3](#)

Creating a New Service

You create a new service from the Services tab. The new service will have default settings which are suitable for most conferences and usually no further configuration is needed.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Services** tab.

Step 3 Click **Add**.

The Automatic Service Definition dialog box appears.

Step 4 In the Service prefix field, enter a prefix for the service.



Note The service prefix is used as part of the dialing plan of your enterprise. Ensure that the prefix does not conflict with other prefixes used in your network.

Step 5 In the Service description field, enter a description of the service in free text.

Step 6 Select one of the following options from the Service type field:

- Audio Only—Forces the conference to be audio-only.
- Standard Rate Video—Supports transcoding at bandwidth rates of up to 384 Kbps.
- High Rate Video—Supports transcoding at bandwidth rates of up to 2 Mbps.
- High Definition Video—Supports switched High Definition video at rates of up to 2 Mbps.

Step 7 Click **Upload**.

Creating a New SCCP Service

You create a new SCCP service from the Services tab. The new service will have default settings which are suitable for most conferences and usually no further configuration is needed.



Note

Data collaboration and encryption configuration options are not available for SCCP services.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Services** tab.
- Step 3** Click **Add**.
- The Automatic Service Definition dialog box appears.
- Step 4** In the Service prefix field, enter a prefix for the service.
- Step 5** Check **SCCP service**.
- Step 6** In the Service description field, enter a description of the service in free text.
- Step 7** Click **Upload**.
-

Customizing Services

You customize a service by first creating a new default service and then configuring your own settings in the Automatic Service Definition dialog box.

- [Configuring the Maximum Call Rate, page 5-4](#)
- [Configuring the Maximum Layout, page 5-4](#)
- [Configuring Standard Definition Advanced Video Settings, page 5-4](#)
- [Configuring High Definition Advanced Video Settings, page 5-6](#)
- [Configuring Advanced Audio Settings, page 5-7](#)
- [Configuring Data Collaboration Support, page 5-8](#)
- [Configuring Presentation View, page 5-9](#)
- [Configuring Encryption Support, page 5-10](#)
- [Configuring Advanced Management and Security for the 3515 MCU, page 5-11](#)

Configuring the Maximum Call Rate

You can configure the maximum call rate for audio and video. This is the maximum bit rate available for this service. This value represents the total bit rate of the voice, video and data streams combined, up to a maximum of 2 Mbps per call.

Procedure

-
- Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
 - Step 2 Click the **Services** tab.
 - Step 3 Click **Add**.
The Automatic Service Definition dialog box appears.
 - Step 4 In the Max call rate field, select the maximum call rate for the voice, video and data streams combined.
 - Step 5 Click **Upload**.
-

Configuring the Maximum Layout

The Max Layout field indicates the video layout displaying the maximum number of participants to which the conference view expands.

The choice of layouts for the service depends on the type of processing mode. The default layout is 1+7 participants.

Procedure

-
- Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
 - Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
 - Step 3 In the Max Layout field, a picture of the current maximum layout appears. Click the **Change** button to choose a new layout.
 - Step 4 Click **OK**.
-

Configuring Standard Definition Advanced Video Settings

In the Advanced Video Settings dialog box you can configure the video codec, video image size, participant layout options, theme and additional layouts for a particular service.

Procedure

-
- Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
 - Step 2 Click the **Services** tab.

- Step 3** Click **Add**.
The Automatic Service Definition dialog box appears.
- Step 4** Click the **Advanced Video Settings** button.
The Advanced Video Settings dialog box appears.
- Step 5** The Video Codecs and Image Size section displays the choice of codecs that you prefer and the supported image size. The codecs are listed in declining order of preference with the most preferred codec listed first. Setting the codec priorities notifies the MCU and remote endpoints of your preferred video codecs. This is useful when more than one codec is supported by both sides. To select or change the codec priorities, follow these steps:
- To add a codec to the Available field, click it in the Selected field and then click **Add**. To remove a codec from the Available field, click it and then click **Remove**.
 - To move a codec up the priority list, click it and then click the **Up** button. To move a codec down the priority list, click it and then click the **Down** button.
- Step 6** In the Support image size up to field, choose the maximum incoming picture format supported in conferences using this service.
- Step 7** In the Main (Participant) Layout section select the layout options you wish to define for this service.
- Step 8** To display a welcome screen to user when that user connects to a conference, select **Display welcome screen**. For information on modifying the welcome screen, see the “[Configuring Welcome Screen Settings](#)” section on page 5-6.
- Step 9** To configure automatic switching, select **Enable auto switch** and enter the interval in seconds. Auto switching allows participant images in the video layout periodically to change and display other conference participants according to the interval set.
- Step 10** Select **Dynamically change layout as participants join or leave** to dynamically enlarge or reduce the displayed number of subframes.
- Step 11** To configure removal of the self image, select **Enable ‘No Self See’**.
- Step 12** Select an option from the Display participants names field to show a participant’s name at the bottom of each sub-frame.
- Step 13** Select **Slightly reduce image size for optimal TV display** to change the display from PC screen mode to TV screen mode.
- Step 14** From the Themes to use field, select a theme. Basic is the default.
- Step 15** (Optional) In the Additional Layouts section, select **Enable custom layouts** to define custom layouts to maintain backward compatibility with previous product versions.
- Step 16** (Optional) Click **Settings** to define the layout options in the Custom Layout Settings dialog box.



Note If you select **Support presentation view (Duo Video and H.239)**, one of the customized layouts must be Presentation layout.

Related Topics

[Configuring Welcome Screen Settings, page 5-6](#)

- [Configuring 3G Layout Settings, page 5-7](#)
- [Configuring Presentation View, page 5-9](#)

Configuring High Definition Advanced Video Settings

In the Advanced Video Settings dialog box you can configure the video codec, video image size, participant layout options, theme and additional layouts for a particular service.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Services** tab.
- Step 3** Select **High Definition Video** in the Service type field.
- Step 4** Click **Add**.
- The Automatic Service Definition dialog box appears.
- Step 5** Click the **Advanced Video Settings** button.
- The High Definition Service dialog box appears.
- The maximum call rate set in the Max call rate field of the Automatic Service Definition dialog box is displayed.
- Step 6** Set a value in the **Allow call rate drop down to** option.
- This option enables you to configure the minimum bandwidth to which the MCU lowers a conference to enable additional endpoints to join. This form of “downspeeding” contributes to a higher percentage of call completion on the network. Endpoints are prevented from joining a conference at a bandwidth rate below the value set in this option.
- After downspeeding occurs, the MCU automatically raises the conference bandwidth rate when the endpoints participating at the lowest bandwidth rate leave the conference. For example, in a conference of endpoints communicating at 768 Kbps and a value of 512 Kbps configured in the Allow call rate drop to option, the MCU lowers the conference to 512 Kbps when an endpoint attempts to join the conference at 512 Kbps. If that endpoint later disconnects from the conference, leaving two endpoints capable of communicating at 768 Kbps, the MCU automatically increases the bandwidth of the conference back to 768 Kbps.
- Step 7** Select a codec from the **Codec** field.
- Step 8** To configure removal of the self image, select **Enable ‘No Self See’**.
- Step 9** Click **OK**.
-

Configuring Welcome Screen Settings

In the Main (participant) layout section of the Advanced Video Settings dialog box you can modify the appearance of the welcome screen.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Services** tab. Select the service you wish to configure and click **Add**.
- The Automatic Service Definition dialog box appears.

- Step 3** Click the **Advanced Video Settings** button.
An Advanced Video Settings dialog box appears.
- Step 4** Select **Display welcome screen** and click **Settings**.
- Step 5** Select the text color and background color settings that you require.
- Step 6** Enter your required welcome text in the Welcome text field.
- Step 7** Set the length of time for which the welcome screen will display in the Display duration field.
- Step 8** Click **OK**.
-

Configuring 3G Layout Settings

In the Additional Layouts section of the Advanced Video Settings dialog box you can configure the layout options for 3G videophone users.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click **Services**. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Click **Advanced Video Settings**.
An Advanced Video Settings dialog box appears.
- Step 4** In the Additional Layouts section, select **Enable 3G videophone layout** to limit the layout for 3G videophone users.
- Step 5** Click **Settings** to select the layout in the 3G Layout Settings dialog box.
- Step 6** Click **OK** to return to the Automatic Service Definition dialog box.
-

Configuring Advanced Audio Settings

Transcoding between audio protocols enables the Cisco Unified Videoconferencing 3515 MCU to support communication between endpoints with different audio codecs. You configure service audio transcoding in the Audio Settings dialog box.

For a service, you can configure conference audio codec support and transcoding priorities. The MCU supports the following audio codecs:

- G.711 A/μ law—Toll quality at 64 Kbps (A-Law/mu-Law).
- G.722—High-quality audio at 64 Kbps.
- G.722.1—High quality audio at 24 Kbps or 32 Kbps using a digital sampling rate ranging from 50 Hz up to 7 kHz.
- G.723.1—Voice quality audio at 5.3 Kbps or 6.4 Kbps.

- G.728—Near toll quality audio at 16 Kbps.
- G.729A—Audio at 8 Kbps.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click **Services**. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Click **Advanced Audio Settings** to modify audio settings.
The Audio Settings dialog box appears.
- Step 4** The Audio codec settings section displays the choice of codecs that you prefer for audio transcoding. The codecs are listed in declining order of preference with the most preferred codec listed first. Setting these priorities notifies the MCU and remote endpoints of your preferred audio codecs. This is useful when more than one codec is supported by both sides. To change these priorities, follow these steps:
- To add a codec to the Available field, click it in the Selected field and then click **Add**. To remove a codec from the Available field, click it and then click **Remove**.
 - To move a codec up the priority list, click it and then click **Up**. To move a codec down the priority list, click it and then click **Down**.
- Step 5** In the Audio packet size field, enter the minimum audio packet size.
- Step 6** In the Number of speakers to mix concurrently field, enter the maximum number of speakers in a conference who can be heard at the same time. The value you enter is the number of loudest speakers for whom the audio stream is mixed and sent to all conference participants. For example, if you enter 4, the MCU mixes the audio stream of the four loudest speakers in the conference.
- Step 7** In the Speaking duration to become ‘Active Speaker’ field, enter the interval (in milliseconds) before the voice-activated video-switching mechanism displays a new active speaker in the video image. The default setting is 3000 milliseconds.
- Step 8** Select **Automatically mute participants who join the conference** to have the MCU initially mute all participants joining the conference. Once the conference begins, the conference Chair Control can unmute selected participants. This is useful for lectures.
- Step 9** If you performed step 8, you can select **Do not mute first conference participant** to have the MCU mute all conference participants except the participant that joined the conference first.
- Step 10** Click **OK**.
-

Configuring Data Collaboration Support

In the Data Collaboration section of the Automatic Services Definition dialog box you can configure the service to support T.120 data collaboration when the MCU works with a T.120 server.



Note

Data collaboration configuration options are not available for SCCP services.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
 - Step 2** Click the **Services** tab. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
 - Step 3** Select **Support T.120 data conferencing**.
 - Step 4** If you performed step 3, you can select **Allow access to data conferencing from MCU conference control**.
 - Step 5** Click **Upload**.
-

Configuring Presentation View

In the Data Collaboration section of the Automatic Services Definition dialog box you can configure the service to support presentation view (DuoVideo and H.239).

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Services** tab. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Check Support presentation view (Duo Video and H.239) and click the **Settings** button.
The Presentation View Settings dialog box appears.
- Step 4** For a Standard Definition service type, choose a codec from the Presentation Video Codec field.
For a High Definition service type, the Presentation Video Codec field is a read-only field displaying the codec selected in the High Definition Service dialog box.



Note A video codec that is not selected in the Video Codecs and Image Size section of the Advanced Video Settings dialog box is disabled in the Presentation Video Codec field.

- Step 5** In the Presentation Image Size field, choose the required image size.
 - Step 6** In the Presentation Frame Rate field, choose the required frame rate.
 - Step 7** Click **OK**.
-

Configuring Encryption Support

The Cisco Unified Videoconferencing 3515 MCU supports encrypted calls over IP networks. You can configure the service to be encrypted and the type of encryption required.



Note

Encryption configuration options are not available for SCCP services.

About H.235 Encryption for H.323 Calls

The encryption conforms to the H.235 standard and supports the following encryption algorithms:

- DES: with an encryption key of 56 bits
- AES: with an encryption key of 128 bits

Encryption on the MCU can operate in one of the following modes:

- Disabled—No encryption. The supported capability for this mode is Priority 1: no encryption.
- Best effort—This mode implements a “best effort” encryption algorithm. If an endpoint supports encryption, it connects in an encrypted way. If not, it connects without encryption. The supported capabilities for this mode are:
 - Priority 1: AES 128
 - Priority 2: DES 56
 - Priority 3: No encryption
- Encryption required—This mode only connects encrypted calls. Encryption is either AES 128 or DES 56. Non-encrypted calls are not allowed to connect. The supported capabilities for this mode are:
 - Priority 1: AES 128
 - Priority 2: DES 56
- Strong encryption required—This mode only allows AES 128 encrypted calls. Endpoints that do not support AES 128 are not allowed to connect. The supported capability for this mode is Priority 1: AES 128.

The following channels support encryption:

- Audio channel
- Video channel
- Far End Camera Control (FECC)



Note

All channels (audio, video, FECC, incoming, and outgoing) on the same call must have the same encryption levels. If the encryption on all channels cannot be achieved, the call disconnects.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click the **Services** tab. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.

- Step 3** In the Management and Security section, select **Support encryption** to enable encryption.
- Step 4** From the Encryption mode field, select the type of encryption:
- Best effort
 - Encryption required
 - Strong encryption required
- Step 5** Click **Upload**.
-

Configuring Advanced Management and Security for the 3515 MCU

In the Advanced Management and Security interface, you can configure policies for PIN settings, auto-reconnect and auto-redial, audio indications and invite authorizations, port reservations and limits, and Far End Camera Control (FECC).

- [Configuring PIN Settings, page 5-11](#)
- [Configuring Service Dial-out Policies, page 5-12](#)
- [Configuring Service Indication Settings, page 5-12](#)
- [Configuring Port Reservations and Limits, page 5-13](#)
- [Configuring Support for Far End Camera Control, page 5-14](#)

Configuring PIN Settings

In the PIN Settings tab you can define a policy for the use of PINs for accessing a conference.

Procedure

- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click **Services** tab. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Click **Advanced Management and Security**.
The Management and Security interface appears.
- Step 4** Click **PIN Settings**.
- Step 5** Select **Force conference PIN protection** if you want user to enter a PIN when creating or entering a conference using this service.
- Step 6** Select **Do not to ask for conference PIN when dialing-out to invitees** if you want only dial-in participants to enter the conference PIN.
- Step 7** Click **OK**.
-

Configuring Service Dial-out Policies

In the Dial-out tab of the Management and Security interface, for a service, you can define policies for invitation rights and auto reconnect and auto redial.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click **Services**. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Click **Advanced Management and Security**.
The Management and Security interface appears.
- Step 4** Click **Dial-out**.
- Step 5** In the Invitation rights section, select one of the options to define whether anyone can invite or only the chair-controller can invite participants to the conference:
- Select **Anyone can invite...** if you want any user to be able to invite participants into the conference.
 - Select **Only the chair can invite...** if you only want users with Chair Control-level access to invite participants into the conference.
- Step 6** In the Re-dial and reconnect section, to define redial and reconnect policies follow these steps:
- Select **Automatically redial invited participants...** for the MCU to redial endpoints that fail to respond to conference invites.
 - In the Number of redial attempts field, enter the number of redial attempts.
 - In the Delay between retries (seconds) field, enter a number representing the number of seconds between each redial attempt.
 - Select **Automatically reconnect participants...** for the MCU to automatically call disconnected terminals to attempt a reconnection. The MCU attempts reconnection three times.
- Step 7** Click **OK**.
-

Configuring Service Indication Settings

In the Indications tab of the Management and Security interface, for a service, you can configure audio indications played to conference participants.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click **Services**. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Click **Advanced Management and Security**.
The Management and Security interface appears.

- Step 4 Click **Indications**.
 - Step 5 Select **First participant entry** if you want a message played to the first participant entering a conference, informing the participant that they are the first one to enter.
 - Step 6 Select **Participant entry** if you want an audio indication played when any additional participant enters a conference.
 - Step 7 Select **Participant exit** if you want an audio indication played when any participant exits a conference.
 - Step 8 Select **Conference termination** if you want an audio indication played when a conference ends.
 - Step 9 Click **OK**.
-

Configuring Port Reservations and Limits

In the Port Reservation & Limits tab of the Management and Security interface, for a service, you can configure the number of ports to reserve when a conference starts.

Procedure

- Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2 Click **Services**. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3 Click **Advanced Management and Security**.
The Management and Security interface appears.
- Step 4 Click **Port Reservation & Limits**.
- Step 5 Select **Number of ports guaranteed (reserved) when a conference starts**. Enter the number of ports to reserve. The minimum value allowed is one port.



Note Enter a number no larger than the maximum number of ports the platform can support.

- Step 6 Select **Allow conference to grow over guaranteed value** if you want the to allow the conference to grow dynamically beyond the number of ports you have defined in the Number of ports guaranteed (reserved) when a conference starts check box.
 - Step 7 Click **OK**.
-

Configuring Support for Far End Camera Control

In the FECC tab of the Management and Security interface, for a service, you can configure Far End Camera Control (FECC) data for managing the camera of endpoints at other locations.

Procedure

-
- Step 1** In the Administrator interface, on the sidebar, click **MCU** (if not already selected).
- Step 2** Click **Services**. Select the service you wish to configure and click **Add**.
The Automatic Service Definition dialog box appears.
- Step 3** Click **Advanced Management and Security**.
The Management and Security interface appears.
- Step 4** Click **FECC**.
- Step 5** Select the check box to enable FECC support.
- Step 6** Click **OK**.
-



Using the Cisco Audio Message Utility

This section describes the following topics:

- [Introduction, page 6-1](#)
- [Launching the Cisco Audio Message Utility, page 6-2](#)
- [Playing a Message, page 6-2](#)
- [Recording a Message, page 6-6](#)
- [Replacing a Message, page 6-7](#)
- [Uploading a Message to a Device, page 6-8](#)
- [Viewing Message Details, page 6-8](#)
- [Exiting the Utility, page 6-9](#)
- [About Express Setup, page 6-9](#)
- [Using Express Setup, page 6-9](#)

Introduction

The Cisco Audio Message Utility is an interactive GUI that enables you to record and replace messages and upload new messages to the call routing mechanisms in Cisco devices.

Default built-in audio messages are in English. The Cisco Audio Message Utility allows you to record new messages in a different language or with different content to suit your requirements. The Cisco Audio Message Utility also enables you to replace and upload new messages to the target Cisco device.

There are two ways of using the Cisco Audio Message Utility. The standard utility functions enable you to play, record or replace messages. The Express Setup guides you through the recording, replacing and upload procedure for each of the voice messages.

Before You Begin

Before you can record, play and upload messages to the target Cisco device, you must

- Save recorded messages as WAV files.
- Know the IP address of the target device.

Launching the Cisco Audio Message Utility

This section describes how to install and launch the Cisco Audio Message Utility.

Procedure

- Step 1** Copy the Audio Message Utility folder from the Cisco Unified Videoconferencing Software CD-ROM to your local computer.



Note You cannot run the Audio Message Utility from the Cisco Unified Videoconferencing Software CD-ROM.

- Step 2** To run the utility, double-click the *IvrRecordingUtility.exe* file.

Playing a Message

This section describes how to play an audio message. Available messages depend upon the device selected in the Target Type field.

- [MCU Messages, page 6-2](#)



Note The devices available in the Target Type drop-down list vary according to the Cisco devices included in your installation.

MCU Messages

The following MCU messages are available:

Table 6-1 *MCU Messages*

ID	Message Name	Recorded Message	Played for ...	Played when ...
0	Connected indication	Audio signal	single participant	a participant first connects to a conference
1	Enter conference PIN	“Thank you for attending the conference. Please enter the conference PIN code followed by the pound sign now.”	single participant	a participant connects to a PIN-protected conference (played after the Connected indication message)
2	Wrong PIN, disconnecting	“You have entered an invalid PIN code. Please check with the conference organizer and try again.”	single participant	a participant tries to join a PIN-protected conference after entering the wrong PIN three times in a row

Table 6-1 MCU Messages (continued)

ID	Message Name	Recorded Message	Played for ...	Played when ...
3	Wrong PIN, enter a valid one	“You have entered an invalid PIN code. Please enter a valid PIN code followed by the pound sign now.”	single participant	a participant tries to join a PIN-protected conference after entering the wrong PIN (less than three times in a row)
4	Reserved	N/A		reserved for future use
5	First participant in conference	“Thank you for attending the conference. You are the first participant. Please hold.”	single participant	the first participant joins the conference (after the Connected indication and the Enter conference PIN messages)
6	New participant joined conference	Audio signal	all participants	a new participant has joined the conference
7	Participant left conference	Audio signal	all participants	a participant has left the conference
8	Success indication	Audio signal	single participant	a DTMF command has succeeded
9	Enter party number	“To dial out, please dial the number of the party you wish to invite to the conference, followed by the pound sign.”	single participant	you are in invite mode (after dialing *8 via DTMF) and you do not dial any number for a period of time
10	Reserved	N/A		for future use
11	Error indication	Audio signal	single participant	a DTMF command has failed
12	Reserved	N/A		for future use
13	Chair privileges required	“This action requires chair privileges. Please take the chair and try again.”	single participant	you perform a DTMF command that requires chair privileges without first taking the chair
14	Chair already taken	“Chair already taken.”	single participant	you try to take the chair via DTMF, but someone else has already taken the chair
15	Reserved	N/A		for future use
16	Initial menu	“The following conference commands are available— To return to the conference, press pound. To take chair, press 1. To mute or unmute your line, press 2. To control the volume of your line press 3.”	single participant	you are in DTMF command mode (after dialing * or ** via DTMF) and you do not enter any command for a period of time

Table 6-1 MCU Messages (continued)

ID	Message Name	Recorded Message	Played for ...	Played when ...
17	Enter chair PIN	“Please enter the chair PIN code followed by the pound sign.”	single participant	you try to take the chair via DTMF and a chair PIN is defined
18	Chair menu	“The following conference commands are available—To return to the conference, press pound. To release chair, press 1. To mute or unmute your line, press 2. To control the volume of your line, press 3. To change the video layout, press 6. To block admission to the conference, press 7. To dial out, press 8. To mute/unmute all lines except you, press 9.”	single participant	you are in DTMF chair mode (i.e. after taking the chair via DTMF) and you do not enter any command for a period of time
19	Join sub-conference	“You have currently joined a sub-conference.”	single participant	a participant joins a sub-conference
20	Leave sub-conference	“You have just left the sub-conference.”	single participant	a participant leaves a sub-conference
21	Reserved	N/A		for future use
22	Join not allowed	“For security reasons, please join from the MeetingPlace web conferencing interface. Goodbye.”		Reserved for Cisco Unified MeetingPlace
23	No video resources	“All video resources are currently in use. Please try again later.”		Reserved for Cisco Unified MeetingPlace
24	Reserved	N/A		for future use
25	Conference terminating	“Please note, the conference is about to terminate.”	all participants	a conference is about to terminate
26	Organizer not yet joined, please wait	“Please wait until the conference organizer joins the conference.”	single participant	you join a conference in waiting room mode before the organizer has joined
27	Organizer joined, conference starts	“The conference will now begin.”	all participants	the organizer joins a conference in waiting room mode
28	Organizer left, conference waiting	“You have been moved to the waiting room, please wait.”	all participants	the organizer leaves a conference in waiting room mode
29	Organizer back, conference resume	“The conference will now resume.”	all participants	the organizer returns to a conference in waiting room mode
30	Wrong chair PIN	“You have entered an invalid chair PIN code.”	single participant	you have entered the wrong chair PIN

Table 6-1 MCU Messages (continued)

ID	Message Name	Recorded Message	Played for ...	Played when ...
31	You are the chair	"You are now the chair person."	single participant	you have taken the chair via DTMF
32	Muted	"All participants are now muted."	single participant	you mute yourself via DTMF
33	Unmuted	"All participants are now unmuted."	single participant	you unmute yourself via DTMF
34	Volume control menu	"Volume control. Press 0 to decrease and 1 to increase the volume."	single participant	you are in volume control mode (after dialing *3 via DTMF) and you do not enter any command for a period of time
35	Conference admission blocked	"Admission to the conference is now blocked."	single participant	you block admission to the conference via DTMF
36	Conference admission allowed	"Admission to the conference is now allowed."	single participant	you allow admission to the conference via DTMF
37	Dialing	"Dialing."	single participant	you invite a participant via DTMF
38	Invalid input	"You have entered invalid input".	single participant	you press an invalid key during a DTMF command
39	Chair released	"You are no longer the conference chair."	single participant	you release the chair via DTMF
40	Change layout menu	"Change layout. Please enter the number of participants to be seen on the screen or press zero for automatic layout."	single participant	you are in change layout mode (after dialing *6 via DTMF) and you do not enter any command for a period of time
41	Mute/Unmute All menu	"Press 0 to mute all participants except yourself. Press 1 to unmute all participants."	single participant	you are in mute/unmute all mode (after dialing *9 via DTMF) and you do not enter any command for a period of time
42	All muted	"All participants are now muted."	single participant	you mute all participants via DTMF

Table 6-1 MCU Messages (continued)

ID	Message Name	Recorded Message	Played for ...	Played when ...
43	All unmuted	“All participants are now unmuted.”	single participant	you unmute all participants via DTMF
44	Chair blocked menu	“The following conference commands are available—To return to the conference, press 1. To release chair, press 1. To mute or unmute your line, press 2. To control the volume of your line, press 3. To change the video layout, press 6. To allow admission to the conference, press 7. To mute/unmute all lines except you, press 9.”	single participant	you are in DTMF chair mode (i.e. after taking the chair via DTMF) in a conference whose admission is blocked and you do not enter any command for a period of time

Procedure

- Step 1** In the Target Type field, choose the device that uses the message you want to play.



Note The options available in the Target Type drop-down list vary according to the Cisco devices included in your installation.

The **Audio Recordings** window displays the messages currently uploaded to the target device.

- Step 2** Ensure the message type you wish to play is enabled in the **Audio Recordings** window.
- Step 3** Click on the message type you wish to play in the **Audio Recordings** window.
- Step 4** From the Message menu, select **Play Message**.

The **Play Recording** dialog box appears. You can stop or replay the message you have selected to play.

Recording a Message

This section describes how to record a new audio message.

Procedure

- Step 1** From the Message menu, select **New Recording**.

The **New Recording** confirmation box appears and the MSound recording utility is invoked.



Note MSound is invoked by default. You can use any recording software that supports the WAV format.

The new message must be recorded in the following formats:

- WAV file
- G.711 (CCITT)
- μ -Law
- 8-bit
- Sampling rate 8kHz

- Step 2** Use the recording software, to record a new message and save it to the Cisco Audio Message Utility directory.
-

Replacing a Message

This section describes how to replace an audio message.

Procedure

- Step 1** In the Target Type field, choose the device that uses the message you want to replace.



Note The options available in the Target Type drop-down list vary according to the Cisco devices included in your installation.

- Step 2** The Audio Recordings window displays the messages currently uploaded to the target device. Click the message type in the Audio Recordings window you wish to replace.
- Step 3** From the Message menu, select **Properties**.
The Properties dialog box appears showing the name of the message you selected in the Message Type field.
- Step 4** (Optional) Enter the text that you want to appear in the Message Type field in the **Audio Recordings** window.
- Step 5** Click Browse to choose the new message you wish to use.
The Replace Recording dialog box appears.
- Step 6** Select the file with which you wish to replace the current message and click **Open** to confirm your selection.
- Step 7** Click **OK** in the Properties dialog box.
- Step 8** The new message appears in the Audio Recordings window.
-

Uploading a Message to a Device

This section describes how to upload audio messages from the Audio Message Utility to a target device.

Procedure

- Step 1** From the Actions menu, select **Upload Messages To Target**.
The Upload dialog box appears.
- Step 2** In the General Information section, enter the IP address of the target device.
- Step 3** In the Login Information section, enter the user name and password of the target device, as configured in the device network configuration settings.
- Step 4** (Optional) Modify the read and write community settings for the target device as follows:
- Click **Customize SNMP Settings**.
The Customize SNMP Settings dialog box displays.
 - Enter the required read community and write community values and click **OK**.
- Step 5** Click **Upload Messages**.
The Upload in progress window appears, and the message files are uploaded and burned onto the target device.
-

Viewing Message Details

You can view the file name and length of the audio messages listed in the **Audio Recordings** window.

Procedure

- Step 1** Click the **Target Type** drop-down list.
- Step 2** Choose the device that uses the message you want to replace.



Note The options available in the Target Type drop-down list vary according to the Cisco devices included in your installation.

The names of audio message files currently uploaded to the target device appear in the Recorded Message field of the Audio Recordings window.

The lengths of audio message files currently uploaded to the target device appear in the Message Length (sec) field of the Audio Recordings window.

Exiting the Utility

This section describes how to exit the Audio Message Utility.

Procedure

- Step 1 Open the Actions menu.
 - Step 2 Select **Exit**.
-

About Express Setup

The Express Setup is an alternative way of recording, replacing and uploading messages. The Express Setup guides you through the recording, replacing and uploading procedure for each audio message.

You proceed through the Express Setup sequentially for each message type. You are alternately prompted to select to record a new message and to navigate a path to a new message file with which you wish to replace a current file.

As you proceed through the Express Setup, the dialog box displays the name the current message type and the associated message file.



Note

You can skip the recording and replacing sequence for each message by clicking **Next** at each step in the Express Setup. You can return to any step in the procedure to change the setup for a particular message by clicking **Back**.

Using Express Setup

This section describes how to use the Express Setup.

Procedure

- Step 1 Click **Express Setup** in the **Tools** menu.
The Express Setup dialog box is displayed informing you of the name of the first message file in the selection and provides a check box for indicating whether you wish to create a new recording for the message.
- Step 2 Check **Create a new recording** and click **Next**.
The Express Setup dialog box displays the required format settings for the new message and the MSsound recorder is displayed. Use the MSsound recorder or other recording software to record the new message and save it to the Audio Message Utility directory.
- Step 3 When you have finished recording a new message, click **Next**.
The Express Setup dialog box displays the path of the current file for the specified message type and the Replace button.
- Step 4 Click **Replace**.

The Replace Recording window appears showing the directory containing the current sound files for the device.

- Step 5** Select the required file and click **Open** to replace this file with the current message file for the specified message.

When you have completed the recording and replacement procedure, the Express Setup dialog box displays the new list of message types and message files associated with each type.

- Step 6** Click **Upload**.

The Upload dialog box appears.

- Step 7** Enter the IP address of the target device.

- Step 8** Enter the user name and password as defined in the network configuration settings of the Cisco device.

- Step 9** Click **Upload Messages** to complete the upload procedure.

The Upload in progress window displays. The message files are uploaded and burned onto the target device.



Numerics

3G layout settings [5-7](#)

A

active speaker [5-8](#)

address information [1-8](#)

 DNS [1-8](#)

 Ethernet [1-8](#)

 IP address [1-8](#)

Addressing tab [1-8](#)

address settings

 changing [1-9](#)

administrator

 add [1-3](#)

 authorization level [1-3, 1-4](#)

 edit [1-4](#)

Administrator interface

 about configuring [1-1](#)

 addressing tab [1-8](#)

 Board Basic tab [1-5](#)

 elements [1-2](#)

 Event Log tab [1-2](#)

 Media Processing tab [1-1](#)

 Protocols tab [1-1](#)

 Security tab [1-10](#)

 Services tab [1-2](#)

 Settings tab [1-1](#)

 Status tab [1-1](#)

 Users tab [1-3, 1-4](#)

 Web tab [1-9](#)

advanced commands

 list of [3-4](#)

 sending [3-6](#)

Advanced Commands dialog box [3-6](#)

Advanced H.323 Setting dialog box [4-2](#)

Advanced Management and Security interface [5-11](#)

Advanced SCCP Settings dialog box [4-11](#)

Advanced SIP Setting dialog box [4-4](#)

advanced video settings (High Definition) [5-6](#)

advanced video settings (Standard Definition) [5-4](#)

Advanced Video Settings dialog box [5-5, 5-7](#)

alert indications [2-7](#)

 about [2-7](#)

 event types [2-7](#)

audio

 advanced settings [5-7](#)

 codecs [5-7](#)

 indications [5-12](#)

 packet size [5-8](#)

 transcoder priorities [5-8](#)

audio announcement interval [3-4](#)

audio messages available [6-2](#)

Audio Message Utility procedures

 exit [6-9](#)

 install and launch utility [6-2](#)

 play message [6-6](#)

 record message [6-6](#)

 replace message [6-7](#)

 upload message [6-8](#)

 use Express Setup [6-9](#)

 view message details [6-8](#)

Audio Settings dialog box [5-7, 5-8](#)

authorization level [1-3, 1-4](#)

 administrator [1-3, 1-4](#)

operator 1-3, 1-4
 authorization policy 3-2
 Automatic Service Definition dialog box 5-3, 5-4, 5-5, 5-6,
 5-7, 5-8, 5-9, 5-10, 5-11, 5-12, 5-13, 5-14
 auto reconnect 5-12
 auto redial 5-12
 auto switch 5-5

C

call rate
 maximum 5-4
 Change Time dialog box 1-7
 Chinese 2-2
 Choose file dialog box 2-12
 codecs
 audio 5-7
 video 5-5
 cold start 2-8
 communications (ICMP) failure 3-3
 concurrent speakers 5-8
 configuration procedures
 add administrators and operators 1-3
 add Cisco Unified Call Manager 4-10
 configure 3G videophone layout options 5-6, 5-7
 configure advanced audio settings 5-8
 configure advanced H.323 gatekeeper settings 4-2
 configure advanced SCCP protocol settings 4-11
 configure advanced SIP Proxy settings 4-4
 configure advanced video settings 5-4, 5-6
 configure as separate SIP domain 4-7
 configure as UAC 4-6
 configure authorization policy 3-2
 configure data collaboration support 5-9
 configure dynamic layouts 2-6
 configure H.323 gatekeeper settings 4-1
 configure maximum call rate 5-4
 configure maximum layout 5-4
 configure PIN settings 5-11
 configure quality of service 2-6
 configure SCCP support 4-9
 configure service dial-out policies 5-12
 configure service indication settings 5-12
 configure SIP Proxy settings 4-3
 configure SNMP trap servers 2-9
 configure TFTP server 4-9
 configure themes 2-4
 create a new SCCP service 5-3
 create new services 5-2
 delete administrators and operators 1-5
 delete SNMP trap servers 2-10
 delimiters 3-2
 disconnect on communications (ICMP) failure 3-3
 edit administrators and operators 1-4
 edit SNMP trap servers 2-9
 enable DTMF 2-4
 enable H.243 2-4
 import settings 2-12
 methods for creating conferences 3-1
 open a Telnet terminal 3-7
 password 3-2
 register conference ID 3-1
 save settings 2-11
 select language 2-2
 send advanced commands 3-6
 set alert indications 2-8
 set conference joining methods 3-2
 set invite delimiters 3-2
 set operator number 2-3
 set port reservations and limits 5-13
 set unit identifier 2-3
 support encryption 5-10
 support FECC 5-14
 terminate ad hoc 3-2
 transcoder priorities 5-8
 view SCCP protocol configurations 4-8
 custom layouts 5-5

D

data collaboration
 configuring 5-9
 support T.120 data collaboration 5-8

delimiters 3-2

dial-out policies 5-12

Dial-out tab 5-12

dial plan
 SIP 4-3, 4-5

DTMF 2-3
 enable in-band DTMF (RFC 2833) 3-6
 forwarding 3-4
 handle after XML 3-5

Duo Video 5-5, 5-9

dynamic layouts 2-6

E

encryption
 H.235 5-10
 support 5-10

English 2-2

Ethernet
 view information 1-8

event log 2-10

Event Log tab 2-7, 2-10

Express Setup 6-9

external programs 1-10

F

Far End Camera Control (FECC) 5-14

FECC tab 5-14

File Download dialog box 2-11

font align 3-4

frame rate
 presentation 5-9

FTP 1-3, 1-10

G

G.728 mode 3-4

H

H.235 5-10

H.239 5-5, 5-9

H.243 2-4

H.323 advanced commands
 hide stack 3-5
 show stack 3-5
 show status 3-5

H.323 gatekeepers
 advanced settings 4-2
 conference registration 3-1
 settings 4-1

H.323 Protocol Configurations dialog box 4-1, 4-2

High Definition 5-2

High Definition Service dialog box 5-6

I

ICMP 1-10

image size
 maximum 5-5
 presentation 5-9

importing configuration settings 2-12

Indications tab 5-12

invitation rights 5-12

invite
 delimiters 3-2

IP address
 address information 1-8

J

Japanese 2-2

L

language support [2-2](#)

layouts

3G [5-7](#)

custom [5-5](#)

maximum participant [5-4](#)

participant [5-5](#)

LED Monitoring tab [1-5](#)

Licensing and Registration dialog box [1-6](#)

link down [2-8](#)

link up [2-8](#)

login name [1-3](#)

log notify level filter [3-5](#)

M

management and security, advanced [5-11](#)

maximum layout [5-4](#)

Media Processing tab [2-10](#)

media processor [2-10](#)

registration failure [2-7](#)

type [2-10](#)

mute

automatic [5-8](#)

do not [5-8](#)

N

Netscape Navigator [1-11](#)

NTP synchronization period [3-5](#)

number of conferences and calls [2-1](#)

O

online help [1-10](#)

Netscape Navigator [1-11](#)

operational status [2-1](#)

operator

add [1-3](#)

authorization level [1-3, 1-4](#)

edit [1-4](#)

number [2-3](#)

P

packet size

audio [5-8](#)

maximum across network [3-6](#)

participant

layout [5-5](#)

password [3-2](#)

PIN

delimiters [3-2](#)

settings [5-11](#)

PIN Settings tab [5-11](#)

port

reservations and limits [5-13](#)

Port 80 [1-9](#)

Port Reservation & Limits tab [5-13](#)

Portuguese [2-2](#)

presentation

frame rate [5-9](#)

image size [5-9](#)

support presentation view [5-5, 5-9](#)

video codec [5-9](#)

view [5-9](#)

Presentation View Settings dialog box [5-9](#)

protocol settings [4-1 to 4-7](#)

Protocols tab [4-1](#)

Q

Quality of Service (QoS) [2-5](#)

QualiVision

hide settings [3-6](#)

show settings 3-6

R

resources 2-1

Russian 2-2

S

saving configuration settings 2-11

SCCP

advanced protocol settings 4-10

SCCP advanced commands

hide stack 3-6

show status 3-6

SCCP Protocol Configurations dialog box 4-8, 4-9, 4-10

Security tab 1-10

services configuration 5-1 to 5-14

Services tab 5-2

settings configuration 2-2 to 3-7

SIP

as separate SIP domain 4-7

dial plan 4-3, 4-5

incoming calls 4-6

outgoing calls 4-6

SIP Protocol Configurations dialog box 4-3, 4-4, 4-7

SIP Proxy

advanced settings 4-4

settings 4-3

Skinny Client Control Protocol (SCCP) 4-8

SNMP 1-10

configuring trap servers 2-9

deleting trap servers 2-10

editing trap servers 2-9

standard SNMP trap event types 2-8

SNMP Trap Servers Properties dialog box 2-9

Spanish 2-2

speaker mix 5-8

Status tab 2-1

system procedures

change address settings 1-9

change default web server port 1-9

configure external program access 1-10

configure security 1-10

set date and time 1-7

set location 1-8

update license 1-6

view expanded software version information 1-7

T

Telnet 1-3, 1-10, 3-7

terminal baud rate 3-6

text-based commands See advanced commands

themes 2-4, 5-5

transcoder priority 5-8

Trivial File Transfer Protocol (TFTP) server 4-8

Type of Service (ToS) 2-5

U

UAC 4-5

configuring as UAC 4-6

unit identifier 2-3

user interface language 2-2

Users tab 1-3, 1-4

access level 1-3

login name 1-3

Telnet/FTP 1-3

V

Version Details dialog box 1-7

video

advanced settings (High Definition) 5-6

advanced settings (Standard Definition) 5-4

codec [5-5](#)
image size [5-5](#)
video processor [2-10](#)
viewing
 access levels [1-3](#)
 address information [1-8](#)
 advanced SCCP protocol settings [4-10](#)
 audio message details [6-8](#)
 board information [1-5](#)
 Ethernet information [1-8](#)
 event log [2-10](#)
 general information [1-5](#)
 H.323 gatekeeper settings [4-1](#)
 LED information [1-5](#)
 media processors [2-10](#)
 registered users [1-3](#)
 resource usage and performance [2-1](#)
 SCCP protocol configurations [4-8](#)
 users access levels [1-3, 1-4](#)

W

warm start [2-8](#)
web refresh interval [3-4](#)
Web tab [1-9](#)
welcome screen [5-5, 5-6](#)

X

XML [3-5](#)