



Configuration Guide for Cisco Unified Videoconferencing 5200 Series MCU Release 7.1

January 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000

Text Part Number: OL-21730-01

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynx, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

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

Configuration Guide for Cisco Unified Videoconferencing 5200 Series MCU Release 7.1
© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1**Accessing the Cisco Unified Videoconferencing 5200 Series MCU Interface 1-1**

CHAPTER 2**Viewing Cisco Unified Videoconferencing 5200 Series MCU Status Information 2-1**

- Viewing the Number of Current Conferences 2-1
- Viewing the Number of Conference Participants 2-2
- Viewing Board Status 2-2
- Viewing Gatekeeper Connection Status 2-2
- Viewing SIP Server Connection Status 2-3
- Viewing Ethernet Connection Status 2-3
- Viewing Fan Operation Status 2-3
- Viewing Chassis Temperature Status 2-4
- Viewing Chassis Power Supply Status 2-4
- Viewing Cisco Unified Videoconferencing 5200 Series MCU Resource Usage 2-4
- Viewing Current Users 2-5
- Viewing System Version Information 2-5

CHAPTER 3**Configuring the Cisco Unified Videoconferencing 5200 Series MCU Environment 3-1**

- Setting the User Interface Language 3-1
- Setting the Product Identifier 3-2
- Setting the Time and Date on the Cisco Unified Videoconferencing 5200 Series MCU 3-2
- Changing Address Settings 3-3
- Configuring Security for the Cisco Unified Videoconferencing 5200 Series MCU 3-4
- Creating and Importing a Web Server Certificate 3-4
- How to Manage SNMP Trap Servers 3-5
 - Viewing SNMP Trap Servers 3-5
 - Configuring SNMP Trap Servers 3-5
 - Modifying SNMP Trap Servers 3-6
 - Deleting SNMP Trap Servers 3-6
- Configuring and Viewing Quality of Service 3-6

CHAPTER 4**Configuring Protocols for the Cisco Unified Videoconferencing 5200 Series MCU 4-1**

- Configuring H.323 Gatekeeper Protocol Settings 4-1
- Configuring SIP Proxy Settings 4-2

Configuring the DTMF Signaling Method 4-3

CHAPTER 5

Configuring Conference Management Settings for the Cisco Unified Videoconferencing 5200 Series MCU 5-1

- Viewing and Updating License Information 5-1
- Dialing Directly to the Cisco Unified Videoconferencing 5200 Series MCU 5-2
- Defining Conference Creation Options 5-2
- Defining Ad Hoc Conference Termination Options 5-3
- Configuring Dynamic Cisco Unified Videoconferencing 5200 Series MCU Layouts 5-3
- How to Manage Services on the Cisco Unified Videoconferencing 5200 Series MCU 5-4
 - Services Overview 5-4
 - Creating a New Service 5-5
 - Configuring the Auto Attendant Service 5-5
 - Deleting a Service 5-6
- How to Customize Services 5-6
 - Configuring the Default Layout 5-6
 - Enabling Personal Layouts 5-7
 - Displaying Participant Names 5-7
 - Configuring Presentation View 5-8
 - Configuring Encryption Support 5-8
 - Muting Participants on Joining a Conference 5-9
 - Automatically Reconnecting Conference Participants 5-10
 - Configuring PIN Settings 5-10

CHAPTER 6

Configuring Interactive Response Messages for the Cisco Unified Videoconferencing 5200 Series MCU 6-1

- Setting a Text Overlay Language 6-1
- How to Manage Audio Messages 6-1
 - Saving All Audio Messages 6-2
 - Uploading Individual Audio Messages 6-2
 - Uploading Audio Messages 6-3
- Available Cisco Unified Videoconferencing 5200 Series MCU Messages 6-3

CHAPTER 7

Managing Cisco Unified Videoconferencing 5200 Series MCU Events 7-1

- Available Cisco Unified Videoconferencing 5200 Series MCU Events 7-1
- Viewing the Events Log 7-6
- Viewing the Alarms Log 7-6
- Viewing Security Events 7-6
- Setting Event Security Levels 7-6

[Sending a Trap on a Specified Event](#) 7-7

[Viewing Event Descriptions](#) 7-7

[Viewing Alarm History](#) 7-8

[Using the Event Display Filter](#) 7-8

CHAPTER 8

Managing Cisco Unified Videoconferencing 5200 Series MCU User Profiles 8-1

[Cisco Unified Videoconferencing 5200 Series MCU User Types](#) 8-1

[Viewing User Profiles](#) 8-2

[Adding a User Profile](#) 8-2

[Modifying a User Profile](#) 8-3

[Enabling a User Profile](#) 8-3

[Removing a User Profile](#) 8-3

CHAPTER 9

Configuring Advanced Maintenance Settings for the Cisco Unified Videoconferencing 5200 Series MCU 9-1

[Backing Up Your Cisco Unified Videoconferencing 5200 Series MCU Configuration](#) 9-1

[Restoring Your Cisco Unified Videoconferencing 5200 Series MCU Configuration](#) 9-2

[Restoring Factory Default Settings](#) 9-2

[How to Work with Advanced Commands for the Cisco Unified Videoconferencing 5200 Series MCU](#) 9-3

[Viewing Available Advanced Commands](#) 9-3

[Modifying Advanced Commands](#) 9-6

[Sending Advanced Commands](#) 9-7

[How to Manage Cisco Unified Videoconferencing 5200 Series MCU Software](#) 9-7

[Upgrading Cisco Unified Videoconferencing 5200 Series MCU Software](#) 9-7

[Restoring a Previous Software Version](#) 9-8

[Restarting the Cisco Unified Videoconferencing 5200 Series MCU](#) 9-8

[Contacting Customer Support](#) 9-8

[Viewing Active Conferences](#) 9-9

[Creating a New Conference](#) 9-9



CHAPTER 1

Accessing the Cisco Unified Videoconferencing 5200 Series MCU Interface

Procedure

-
- Step 1** Launch your browser and enter the IP address or the name of the Cisco Unified Videoconferencing 5200 Series MCU.
- Step 2** Enter the Administrator user name and password in the appropriate fields and select **Go**.
The default global user name is admin. The default password is password.



Note If you try to sign in as an Administrator and another Administrator is currently signed in, the Cisco Unified Videoconferencing 5200 Series MCU signs you in as a Read only user. The words “Read Only” appear at the top of the window and a pop-up displays the IP address of the Administrator already signed in. Read only users cannot edit Cisco Unified Videoconferencing 5200 Series MCU settings.



CHAPTER 2

Viewing Cisco Unified Videoconferencing 5200 Series MCU Status Information

- [Viewing the Number of Current Conferences, page 2-1](#)
- [Viewing the Number of Conference Participants, page 2-2](#)
- [Viewing Board Status, page 2-2](#)
- [Viewing Gatekeeper Connection Status, page 2-2](#)
- [Viewing SIP Server Connection Status, page 2-3](#)
- [Viewing Ethernet Connection Status, page 2-3](#)
- [Viewing Fan Operation Status, page 2-3](#)
- [Viewing Chassis Temperature Status, page 2-4](#)
- [Viewing Chassis Power Supply Status, page 2-4](#)
- [Viewing Cisco Unified Videoconferencing 5200 Series MCU Resource Usage, page 2-4](#)
- [Viewing Current Users, page 2-5](#)
- [Viewing System Version Information, page 2-5](#)

Viewing the Number of Current Conferences

Procedure

Step 1 Select **Status**.

Step 2 Locate the Utilization section.

The Conferences box displays the number of conferences currently hosted on the Cisco Unified Videoconferencing 5200 Series MCU.

Viewing the Number of Conference Participants

Procedure

Step 1 Select **Status**.

Step 2 Locate the Utilization section.

The Participants box displays the current number of calls on the Cisco Unified Videoconferencing 5200 Series MCU.

Viewing Board Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

A green tick next to the slot number indicates that the Cisco Unified Videoconferencing 5200 Series MCU board in the specified chassis slot is correctly installed and operational.

A red cross next to the slot number indicates that an installation or operational error has occurred for the board in the specified chassis slot.

Viewing Gatekeeper Connection Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

A green arrow next to the Gatekeeper box indicates that the Cisco Unified Videoconferencing 5200 Series MCU is registered to a gatekeeper.

A red cross next to the Gatekeeper box indicates a gatekeeper registration error.

Viewing SIP Server Connection Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

A green arrow next to the SIP Server box indicates that the Cisco Unified Videoconferencing 5200 Series MCU is registered to a SIP server.

A red cross next to the SIP Server box indicates a SIP server registration error.

A dotted line to the SIP Server box without a tick or a cross indicates that the Cisco Unified Videoconferencing 5200 Series MCU has not attempted to register to a SIP server.

Viewing Ethernet Connection Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

The Ethernet box indicates the status of the Ethernet connection.

The Ethernet connection speed is displayed below the Ethernet box.

Viewing Fan Operation Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

The Fan box indicates the operational status of the fan.

A green tick indicates normal operation.

A red cross indicates that one or more fans have failed. The Fan problem SNMP trap lists the specific fan affected.

The average speed for all fans is displayed below the Fan box.

Viewing Chassis Temperature Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

The Temperature box indicates the temperature status of the chassis.

A green tick indicates normal operation.

A red cross indicates the ambient chassis temperature has risen above the high temperature threshold.

The chassis temperature is displayed below the Temperature box.

Viewing Chassis Power Supply Status

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

The PSU box indicates the operational status of the chassis power supply unit.

A green tick indicates normal operation.

A red cross indicates an error in at least one of the power supply units.

Viewing Cisco Unified Videoconferencing 5200 Series MCU Resource Usage

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

The CPU box indicates the percentage of Cisco Unified Videoconferencing 5200 Series MCU resources currently occupied.

We recommend that this value does not exceed 90 percent.

Viewing Current Users

Procedure

-
- Step 1** Select **Status**.
- Step 2** Locate the Logged users section.
- A list displays all of the users currently logged in to the Cisco Unified Videoconferencing 5200 Series MCU.
-

Viewing System Version Information

Procedure

-
- Step 1** Select **Status**.
- Step 2** Locate the Product Information section to view software and serial number version information.
-



CHAPTER 3

Configuring the Cisco Unified Videoconferencing 5200 Series MCU Environment

- [Setting the User Interface Language, page 3-1](#)
- [Setting the Product Identifier, page 3-2](#)
- [Setting the Time and Date on the Cisco Unified Videoconferencing 5200 Series MCU, page 3-2](#)
- [Changing Address Settings, page 3-3](#)
- [Configuring Security for the Cisco Unified Videoconferencing 5200 Series MCU, page 3-4](#)
- [Creating and Importing a Web Server Certificate, page 3-4](#)
- [How to Manage SNMP Trap Servers, page 3-5](#)
- [Configuring and Viewing Quality of Service, page 3-6](#)

Setting the User Interface Language

You can configure the language that the Cisco Unified Videoconferencing 5200 Series MCU supports. [Table 3-1](#) lists the languages that the Cisco Unified Videoconferencing 5200 Series MCU supports.



Note

To view Chinese or Japanese fonts properly in the Administrator interface, the computer on which the web browser is running must support the relevant languages. On a Microsoft Windows operating system, you can set the default language in Control Panel > Regional and Language Options.

Table 3-1 *Supported Languages in the Cisco Unified Videoconferencing 5200 Series MCU Interface*

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

Procedure

-
- Step 1** Select **Configuration** in the Cisco Unified Videoconferencing 5200 Series MCU user interface.
- Step 2** Select **Setup**.
- Step 3** Locate the Basics section.
- Step 4** Select a language in the Default user interface language field.
- Step 5** Select **Apply**.



Note You set the text overlay language at Configuration > Customization. For more information, see the [Setting a Text Overlay Language, page 6-1](#).

Setting the Product Identifier

You can set the Product Identifier to identify the Cisco Unified Videoconferencing 5200 Series MCU in the following situations:

- During gatekeeper/SIP registration.
- When inviting endpoints into a conference.
- In the text overlay for the cascaded Cisco Unified Videoconferencing 5200 Series MCU in cascaded conferences.

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Setup**.
- Step 3** Locate the Basics section.
- Step 4** Enter an identifier in the **Product Identifier** field (up to a maximum of 32 characters). For example, "London office."
- Step 5** Select **Apply**.
-

Setting the Time and Date on the Cisco Unified Videoconferencing 5200 Series MCU

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Setup**.

- Step 3** Locate the Basics section.
 - Step 4** (Optional) Select **Set manually** in the Date and time section.
 - Step 5** Select **Get local time** or click the calendar icon and set the required time settings.
 - Step 6** (Optional) Select **Set NTP server** to synchronize the time with a network server clock.
 - Step 7** Enter the IP address of the required NTP server.
 - Step 8** Select a time zone.
 - Step 9** Select **Apply**.
-

Changing Address Settings

You can change IP address information, DNS information and Ethernet port speed and duplex settings for .

Procedure

- Step 1** Select **Configuration**.
- Step 2** Select **Setup**.
- Step 3** Locate the **Network** section.
- Step 4** Perform any of these steps to change an IP address setting:
 - a. Enter the IP addresses you want to assign to either Cisco Unified Videoconferencing 5200 Series MCU in the **Primary IP address** and **Secondary IP address** fields.
 - b. Enter the IP address of the router you want either Cisco Unified Videoconferencing 5200 Series MCU to use in the **Router IP** field.
 - c. Enter the subnet mask you want to either Cisco Unified Videoconferencing 5200 Series MCU to use in the **Subnet Mask** field.
- Step 5** To change or add DNS information, do the following steps:
 - a. Enter the alias you want to assign to the current Cisco Unified Videoconferencing 5200 Series MCU in the **DNS suffix** field.
 - b. Enter the IP address of the primary DNS server that you want the Cisco Unified Videoconferencing 5200 Series MCU to use in the **DNS server1** field.
 - c. Enter the IP address of the back-up DNS server that you want the Cisco Unified Videoconferencing 5200 Series MCU to use in the **DNS server2** field.
- Step 6** Select the ethernet port and duplex speed value you want to set in the **Port settings** field.



Note We recommend to set the **Port settings** option to **Auto**. Make sure the directly connected switch is configured with the same settings.

- Step 7** Select **Apply**.
-

Configuring Security for the Cisco Unified Videoconferencing 5200 Series MCU

You can configure the access that external programs have to the Cisco Unified Videoconferencing 5200 Series 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 | Select Configuration . |
| Step 2 | Select Setup . |
| Step 3 | Locate the Security section. |
| Step 4 | Select the access level you want the Cisco Unified Videoconferencing 5200 Series MCU to support from the Security mode field. <ul style="list-style-type: none">• Standard—Allows SNMP, Telnet, FTP, and ICMP to access the Cisco Unified Videoconferencing 5200 Series MCU.• High (no Telnet or FTP)—Allows access to the Cisco Unified Videoconferencing 5200 Series MCU only through SNMP and ICMP.• Maximum (no Telnet, FTP, SNMP, or ICMP)—Disallows external programs to access the Cisco Unified Videoconferencing 5200 Series MCU. |
| Step 5 | Select Apply . |
-

Creating and Importing a Web Server Certificate

Procedure

-
- | | |
|---------------|--|
| Step 1 | Select Configuration . |
| Step 2 | Select Setup . |
| Step 3 | Locate the Security section. |
| Step 4 | Select Manage to create certificate request. <ul style="list-style-type: none">a. Enter the required information to specify the details of the certificate.
The Cisco Unified Videoconferencing 5200 Series MCU issues a certificate request (CSR).b. Submit the CSR to the certification authority server.
The certification authority server returns an authenticated certificate. |
- or-

- Step 5** Select **Import** to import the new certificate or an existing one.
- or-
- Step 6** Select **Export** to save an existing certificate to a file
- Step 7** Select **Enable HTTPS**.
- Step 8** Select **Apply**.
-

How to Manage SNMP Trap Servers

- [Viewing SNMP Trap Servers, page 3-5](#)
- [Configuring SNMP Trap Servers, page 3-5](#)
- [Modifying SNMP Trap Servers, page 3-6](#)
- [Deleting SNMP Trap Servers, page 3-6](#)

Viewing SNMP Trap Servers

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Setup**.
- Step 3** Locate the Trap servers section to view all configured SNMP trap servers to which the Cisco Unified Videoconferencing 5200 Series MCU sends SNMP traps.
-

Configuring SNMP Trap Servers

You can specify the IP address and port number for multiple SNMP trap servers to which the Cisco Unified Videoconferencing 5200 Series MCU sends SNMP traps.

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Setup**.
- Step 3** Locate the Trap servers section.
- Step 4** Select **Add new server...**
- Step 5** Enter the IP address and port for the SNMP trap server.
- The default port for SNMP servers is 162.
- Step 6** Select **Apply** to save your settings.
-

Modifying SNMP Trap Servers

Procedure

-
- | | |
|---------------|---|
| Step 1 | Select Configuration . |
| Step 2 | Select Setup . |
| Step 3 | Locate the Trap servers section. |
| Step 4 | Select the button in the Review column for the server you want to modify. |
| Step 5 | Modify the required settings. |
| Step 6 | Select Apply to save your settings. |
-

Deleting SNMP Trap Servers

Procedure

-
- | | |
|---------------|---|
| Step 1 | Select Configuration . |
| Step 2 | Select Setup . |
| Step 3 | Locate the Trap servers section. |
| Step 4 | Select the button in the Review column for the server you want to delete. |
| Step 5 | Select Delete . |
| Step 6 | Select Yes to confirm the deletion. |
-

Configuring and Viewing Quality of Service

You can assign a Quality of Service (QoS) priority level to video and voice calls using either pre-configured system settings or by creating your own settings.

QoS settings involve configuring the Cisco Unified Videoconferencing 5200 Series MCU to add a QoS DiffServ Code Point value in the IP header of outbound packets. Routers on the network that support QoS can give preferential treatment for bandwidth, latency and jitter to such coded packets and facilitate the efficient transmission of packets. You can set QoS parameters on the Cisco Unified Videoconferencing 5200 Series MCU for voice calls, video calls or both.

Procedure

-
- | | |
|---------------|--------------------------------|
| Step 1 | Select Configuration . |
| Step 2 | Select Setup . |
| Step 3 | Locate the QoS section. |

- Step 4** Set the required priority value for each media type by selecting one of these options:
- **Default**—The system assigns the recommended default priority values for each media type.
 - **Custom**—The system assigns specified values for each media type.
 - **None**—The system disables QoS.
- Step 5** If you select **Custom**, set the values manually, where a higher number represents a higher priority. The maximum value is 63. The fields can be customized as follows:
- Enter an integer in the **Control** field of the **Control** section, to represent the priority given to signalling packets such as SIP or H323. Change this value to influence handshakes at the start of a call while a connection is established.
 - Enter an integer in the **Voice priority** field of the **Video calls** section, to represent the priority given to audio signals of video calls.
 - Enter an integer in the **Video priority** field of the **Video calls** section, to represent the priority given to the video image signals of video calls.
 - Enter an integer in the **Data priority** field of the **Video calls** section, to represent the priority given to the other data transmitted during video calls, such as chat or presentations.
 - Enter an integer in the **Voice priority** field of the **Audio calls** section, to represent the priority given to the audio signals during calls with no video.
- Step 6** Select **Apply**.
-



CHAPTER 4

Configuring Protocols for the Cisco Unified Videoconferencing 5200 Series MCU

- [Configuring H.323 Gatekeeper Protocol Settings, page 4-1](#)
- [Configuring SIP Proxy Settings, page 4-2](#)
- [Configuring the DTMF Signaling Method, page 4-3](#)

Configuring H.323 Gatekeeper Protocol Settings

You can configure the protocol settings of an H.323 gatekeeper to set how the Cisco Unified Videoconferencing 5200 Series MCU and the gatekeeper interact.



Note

- Changing gatekeeper settings does not reset the Cisco Unified Videoconferencing 5200 Series MCU, but might disconnect active calls.
 - You do need to reset the Cisco Unified Videoconferencing 5200 Series MCU to disable support for the H.323 protocol.
-

Procedure

- Step 1** Select **Configuration**.
- Step 2** Select **Protocols**.
- Step 3** Locate the H.323 section.
- Step 4** Select **H.323** to enable the Cisco Unified Videoconferencing 5200 Series MCU to operate with the H.323 protocol.
- Step 5** Enter the IP address and port number for the gatekeeper.
The default port is 1719.
- Step 6** Select **Apply**.
-

Configuring SIP Proxy Settings

You can configure settings for SIP registrar profiles which set how the Cisco Unified Videoconferencing 5200 Series MCU and the registrar interact.

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Protocols**.
- Step 3** Locate the SIP section.
- Step 4** Select **SIP** to enable Cisco Unified Videoconferencing 5200 Series MCU communication with the SIP proxy.
- Step 5** Enter the SIP domain of the Cisco Unified Videoconferencing 5200 Series MCU in the **Default SIP domain** field as defined in the SIP server.
- An example of a SIP domain is company.com.
- Step 6** Select **Locate automatically** to instruct the Cisco Unified Videoconferencing 5200 Series MCU to automatically locate one of the SIP proxy servers that are present in the domain,
- or
- Select **Specify** and enter the following:
- An IP address or host name of the SIP proxy, for example proxy.company.com. Make sure that in Cisco Unified Communications Manager, the DTMF Signaling Method is set to "No Preference" for the SIP trunk used in this deployment. See the [“Configuring the DTMF Signaling Method” section on page 4-3](#).
 - The communication port number of the SIP proxy address. The default port is 5060.
 - 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.
-  **Note** The Locate automatically option works only if you have configured a valid IP address at Configuration > Setup > Network > DNS server1 or DNS server2.
-
- Step 7** Select **Use registrar** to instruct the Cisco Unified Videoconferencing 5200 Series MCU to register with a SIP registrar and to send service information to the registrar.
- Step 8** Enter the following information:
- The IP address or the host name of the SIP registrar in the **IP address** field.
- This field is mandatory.
- The communication port number of the SIP registrar address.
 - 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 9** Select **More**.

- Step 10** Enter the number of the signaling port on which the Cisco Unified Videoconferencing 5200 Series MCU communicates with the SIP proxy.
The default is 5060.
- Step 11** Select **Use proxy digest authentication** to enable Cisco Unified Videoconferencing 5200 Series 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.
Enter the Cisco Unified Videoconferencing 5200 Series MCU user name and password. They must match those defined on the SIP proxy server.
- Step 12** Select **Use registrar digest authentication** to enable Cisco Unified Videoconferencing 5200 Series MCU authentication with a SIP registrar using user name and password.
Authentication is performed as defined in RFC 2617. This field is disabled by default.
Enter the Cisco Unified Videoconferencing 5200 Series MCU user name and password. They must match those defined on the SIP proxy server.
- Step 13** Select **Use 'Empty Invite' when sending Invite messages to endpoints** to enable the remote endpoint to indicate preferred audio and video channels.
- Step 14** Select **Apply**.
-

Configuring the DTMF Signaling Method

Procedure

-
- Step 1** Sign in to Cisco Unified Communications Manager Administration.
- Step 2** Select **Device > Trunk**.
- Step 3** Select the SIP trunk added for this deployment.
- Step 4** Under SIP Information, set the DTMF Dialing Method to **No Preference**.
- Step 5** Save and apply the new configuration to the SIP trunk.
-



CHAPTER 5

Configuring Conference Management Settings for the Cisco Unified Videoconferencing 5200 Series MCU

- [Viewing and Updating License Information, page 5-1](#)
- [Dialing Directly to the Cisco Unified Videoconferencing 5200 Series MCU, page 5-2](#)
- [Defining Conference Creation Options, page 5-2](#)
- [Defining Ad Hoc Conference Termination Options, page 5-3](#)
- [Configuring Dynamic Cisco Unified Videoconferencing 5200 Series MCU Layouts, page 5-3](#)
- [How to Manage Services on the Cisco Unified Videoconferencing 5200 Series MCU, page 5-4](#)
- [How to Customize Services, page 5-6](#)

Viewing and Updating License Information

Procedure

- Step 1** Select the  icon.
- Step 2** Select **Licensing and Registration**.
The licensing information is displayed.
- Step 3** To update your license, enter the new license key in the **Update license key** field and click **Update**.
-

Dialing Directly to the Cisco Unified Videoconferencing 5200 Series MCU

You can allow users to dial directly to the Cisco Unified Videoconferencing 5200 Series MCU IP address via the “auto-attendant” mechanism without the need to register to an H.323 gatekeeper or SIP registrar.

Users specify the conference they want to create or join via the Cisco Unified Videoconferencing 5200 Series MCU IVR.

If the Cisco Unified Videoconferencing 5200 Series MCU is already registered to an H.323 gatekeeper or SIP registrar, you can still allow users to access the auto-attendant mechanism by specifying an auto-attendant number which is registered with the appropriate H.323 gatekeeper or SIP registrar. Any call that the Cisco Unified Videoconferencing 5200 Series MCU cannot route to a valid conference is sent to the auto-attendant.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Select Configuration . |
| Step 2 | Select Conferences . |
| Step 3 | Locate the Conference Control section. |
| Step 4 | Select Enable auto attendant. |
| Step 5 | Enter an auto-attendant number. |
- Use this option if the Cisco Unified Videoconferencing 5200 Series MCU is already registered to an H.323 gatekeeper or SIP registrar.
- | | |
|---------------|---|
| Step 6 | (Optional) Select Prompt for conference PIN during conference creation if you want the Cisco Unified Videoconferencing 5200 Series MCU to prompt users for a PIN when accessing a conference using this auto-attendant number. |
| Step 7 | Select Apply . |
-

Defining Conference Creation Options

You can determine how participants are allowed to create a conference.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Select Configuration . |
| Step 2 | Select Conferences . |
| Step 3 | Locate the Conference Control section. |
| Step 4 | Select More . |

- Step 5** Select a method by which users can create conferences in the **Users can create conference using** field.
- 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 Cisco Unified Videoconferencing 5200 Series MCU API.
 - Scheduler, Web and Control API and Dial-in (default)—Enables all the conference creation methods listed above, as well as dial-in for ad-hoc conference creation.
- Step 6** Select **Apply**.
-

Defining Ad Hoc Conference Termination Options

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Conferences**.
- Step 3** Locate the Conference Control section.
- Step 4** Select **More**.
- Step 5** Select a method through which dial-in (ad hoc) conferences terminate in the **Terminate ad hoc conference when** field.
- 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 6** Select **Apply**.
-

Configuring Dynamic Cisco Unified Videoconferencing 5200 Series MCU Layouts

You can define dynamic meeting layouts for video callers. A dynamic meeting layout changes automatically as participants join or leave the meeting.

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Conferences**.
- Step 3** Locate the Conference Control section.
- Step 4** Select **More**.

- Step 5** Select a set of dynamic layouts from the **Select a set of dynamic layouts for all services** field.
- Enlarged main view—Selects a set of layouts in which the main video frame is the largest frame in the display.
 - Same-sized view—Selects a set of layouts in which all video frames are the same size.
 - Customized set—Enables you to create your own set from the available layouts.
- You can change the layouts included in your customized set via the Change link.
- Step 6** Select **Apply**.
-

How to Manage Services on the Cisco Unified Videoconferencing 5200 Series MCU

- [Services Overview, page 5-4](#)
- [Creating a New Service, page 5-5](#)
- [Configuring the Auto Attendant Service, page 5-5](#)
- [Deleting a Service, page 5-6](#)

Services Overview

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 Cisco Unified Videoconferencing 5200 Series MCU comes with several predefined services: one service for the SCCP protocol, one service for Cisco Unified MeetingPlace, and the remainder for audio and video conferencing. 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 (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.722.1C, G.722.1 and AAC audio codecs are not available
- No support for conference PINs
- No support for dial out

Creating a New Service

A new service has default settings which are suitable for most conferences and usually no further configuration is needed.

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.
 - Step 3** Locate the **Services** list section.
 - Step 4** Select **Add new service**.
 - Step 5** Enter a prefix for the service and a description of the service in free text.



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 6** (Optional) Select **Audio only** to force the conference to be audio-only.
 - Step 7** (Optional) Select **SCCP service** to enable the conference to support the SCCP protocol.
 - Step 8** (Optional) Select **Display welcome screen** and enter your text in the welcome screen window.
 - Step 9** (Optional) Enter the string \$DESC to display the conference description in the welcome screen.
You define the conference description in the **Conference Control** web user interface at Create Conference > Conference Description.
If you do not define a conference description, the \$DESC string displays the conference ID by default.
 - Step 10** Select the **Max call rate** (default is 2048 Kbps).
 - Step 11** Select **Switched Video** to bypass signal processing, resulting in the display of a single endpoint only. This option requires both ends to be using the same resolution and codec.
 - Step 12** (Optional) Enter the string \$ID to display the conference ID in the welcome screen.
 - Step 13** Select **Apply**.
-

Configuring the Auto Attendant Service

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.
 - Step 3** Locate the Services list section.
 - Step 4** Select **Review** for the service you want to use as the Auto attendant service.

- Step 5** Select the **Set as Auto attendant service** link.
- Step 6** Select **OK**.
-

Deleting a Service

Procedure

- Step 1** Select **Configuration**.
- Step 2** Select **Conferences**.
- Step 3** Locate the Services list section.
- Step 4** Select the arrow in the Review column for the service that you want to delete.
- Step 5** Select **Delete**.
- Step 6** Select **Yes** in the message that appears.
- The service is removed from the services list.
-

How to Customize Services

- [Configuring the Default Layout, page 5-6](#)
- [Enabling Personal Layouts, page 5-7](#)
- [Displaying Participant Names, page 5-7](#)
- [Configuring Presentation View, page 5-8](#)
- [Configuring Encryption Support, page 5-8](#)
- [Muting Participants on Joining a Conference, page 5-9](#)
- [Automatically Reconnecting Conference Participants, page 5-10](#)
- [Configuring PIN Settings, page 5-10](#)

Configuring the Default Layout

Procedure

- Step 1** Select **Configuration**.
- Step 2** Select **Conferences**.
- Step 3** Locate the Services list section.
- Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
- Step 5** Select **More**.

- Step 6** Perform these steps to enable the conference layout to change automatically as participants join or leave:
- Select **Dynamically adjusted**.
 - Select the maximum number of participants to which the conference layout expands from the **Max displayed streams** field.
 - Select **OK**.
- Step 7** Perform these steps to define a fixed layout for the conference:
- Select **Static** to define a fixed layout for the conference.
 - Select **Select**.
 - Select the required layout and select **OK**.
 - Select **OK** again.
- Step 8** Select **Apply**.
-

Enabling Personal Layouts

System administrators can enable conference participants to create a personalized layout during a conference. Personalized layouts do not affect the layouts of any other conference participant. When this feature is disabled, neither the operator nor the participant can create or control personal layouts in conferences that use this service.

Procedure

-
- Step 1** Select **Configuration**.
- Step 2** Select **Conferences**.
- Step 3** Locate the Services list section.
- Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
- Step 5** Select **More**.
- Step 6** Select **Enable personal layout**.
- Step 7** Select **OK**.
- Step 8** Select **Apply**.
-

Displaying Participant Names

System administrators can enable conference participants with Moderator-level access to display a participant's name at the bottom of each sub-frame when the conference starts.

This feature is enabled by default.

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.
 - Step 3** Locate the Services list section.
 - Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
 - Step 5** Select **More**.
 - Step 6** Select **Display participants names**.
 - Step 7** (Optional) Select **Constantly** to display the participant name continuously.
 - Step 8** (Optional) Select **On location changes for** and an interval in seconds to continue to display the participant name after the location of the participant video frame changes during a conference.
 - Step 9** Select **OK**.
 - Step 10** Select **Apply**.
-

Configuring Presentation View

You can configure a service to support presentation view (H.239).

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.
 - Step 3** Locate the Services list section.
 - Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
 - Step 5** Select **More**.
 - Step 6** Select **Enable presentation view** and a presentation video codec.
 - Step 7** Select **OK**.
 - Step 8** Select **Apply**.
-

Configuring Encryption Support

Restrictions

The Cisco Unified Videoconferencing 5200 Series MCU supports encrypted calls over IP networks. You can configure the service to be encrypted and the encryption mode required.

Encryption configuration options are not available for SCCP services.

The encryption conforms to the H.235 standard and supports the AES encryption algorithm with an encryption key of 128 bits.

Encryption on the Cisco Unified Videoconferencing 5200 Series 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 with encryption. If not, it connects without encryption. The supported capabilities for this mode are AES 128 keys of lengths 512 bits or 1024 bits:
 - Priority 1: AES 128
 - Priority 2: No encryption
- 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 AES 128 keys of 1024 bits.

These 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** Select **Configuration**.
 - Step 2** Select **Conferences**.
 - Step 3** Locate the Services list section.
 - Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
 - Step 5** Select **More**.
 - Step 6** Select **Encryption**.
 - Step 7** Select the type of encryption from the Encryption mode field.
 - Best effort
 - Strong encryption required
 - Step 8** Select **OK**.
 - Step 9** Select **Apply**.
-

Muting Participants on Joining a Conference

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.

- Step 3** Locate the Services list section.
 - Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
 - Step 5** Select **More**.
 - Step 6** Select **Auto mute joining participant** to instruct the Cisco Unified Videoconferencing 5200 Series MCU to initially mute all participants joining the conference.

Once the conference begins, the conference Moderator can unmute selected participants. This is useful for lectures.
 - Step 7** (Optional) Deselect **Auto mute first joining participant** to instruct the Cisco Unified Videoconferencing 5200 Series MCU to initially mute all conference participants except the first participant that joins the conference.
 - Step 8** Select **OK**.
 - Step 9** Select **Apply**.
-

Automatically Reconnecting Conference Participants

You can instruct the Cisco Unified Videoconferencing 5200 Series MCU to automatically call disconnected terminals to attempt a reconnection.

The Cisco Unified Videoconferencing 5200 Series MCU attempts reconnection three times.

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.
 - Step 3** Locate the Services list section.
 - Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
 - Step 5** Select **More**.
 - Step 6** Select **Automatically reconnect dropped participants**.
 - Step 7** Select **OK**.
 - Step 8** Select **Apply**.
-

Configuring PIN Settings

You can define a policy for the use of PINs for accessing a conference.

PINs can contain up to 32 characters.

Procedure

-
- Step 1** Select **Configuration**.
 - Step 2** Select **Conferences**.

- Step 3** Locate the Services list section.
 - Step 4** Locate the service that you want to modify in the Services list section or select **Add new service**.
 - Step 5** Select **More**.
 - Step 6** Select **Force conference PIN protection** if you want the user to enter a PIN when creating or entering a conference using this service.
 - Step 7** Select **Ask for conference PIN on invite** if you want invitees to enter a PIN when they join a conference.
Leave deselected if you want only dial-in participants to enter the conference PIN.
 - Step 8** Select **OK**.
 - Step 9** Select **Apply**.
-



CHAPTER 6

Configuring Interactive Response Messages for the Cisco Unified Videoconferencing 5200 Series MCU

- [Setting a Text Overlay Language, page 6-1](#)
- [How to Manage Audio Messages, page 6-1](#)

Setting a Text Overlay Language

Procedure

- Step 1** Select **Configuration**.
 - Step 2** Select **Customization**.
 - Step 3** Locate the Video display messages section.
 - Step 4** Select the required language.
Set to English by default.
 - Step 5** Select **Apply**.
-

How to Manage Audio Messages

- [Saving All Audio Messages, page 6-2](#)
- [Uploading Individual Audio Messages, page 6-2](#)
- [Uploading Audio Messages, page 6-3](#)
- [Available Cisco Unified Videoconferencing 5200 Series MCU Messages, page 6-3](#)

Saving All Audio Messages

You can save all audio messages currently in use on the Cisco Unified Videoconferencing 5200 Series MCU and download them to your computer in a single zip file.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Select Configuration . |
| Step 2 | Select Customization . |
| Step 3 | Locate the Audio messages section. |
| Step 4 | Select Save next to the Save messages pack file field to save the zip file containing the audio messages to a specified location on your computer. |
-

Uploading Individual Audio Messages

You can upload individual audio messages from your computer to the Cisco Unified Videoconferencing 5200 Series MCU.

Files must be in the following formats:

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

Procedure

-
- | | |
|---------------|---|
| Step 1 | Select Configuration . |
| Step 2 | Select Customization . |
| Step 3 | Locate the Audio messages section. |
| Step 4 | Locate the Message files section. |
| Step 5 | Locate the audio message that you want to save. |
| Step 6 | Select the arrow in the Review column. |
| Step 7 | Select Browse . |
| Step 8 | Navigate to the file that you want to save and select Save . |
| Step 9 | Select Apply . |
-

Uploading Audio Messages

You can upload audio message packs from your computer to the Cisco Unified Videoconferencing 5200 Series MCU.

Files must be in the following formats:

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



Note The maximum file size is 3Mb.

Procedure

- Step 1** Select **Configuration**.
- Step 2** Select **Customization**.
- Step 3** Locate the Audio messages section.
- Step 4** Locate the Messages pack section.
- Step 5** Select **Browse** in the Update messages pack file field and navigate to the message pack file that you want to upload.
- Step 6** Select **Open**.
- Step 7** Select **Apply**.

Available Cisco Unified Videoconferencing 5200 Series MCU Messages

Table 6-1 *Cisco Unified Videoconferencing 5200 Series MCU Audio Messages*

Message Name	Recorded Message	Displayed Message	Played for...	Played when...
Connected indication	Sound		Single participant	a participant first connects to a meeting
Enter meeting PIN	Thank you for attending the meeting. Enter the meeting PIN followed by the pound sign.	Enter PIN code	Single participant	a participant connects to a PIN-protected meeting (played after the Connected indication sound)

Message Name	Recorded Message	Displayed Message	Played for...	Played when...
Wrong PIN, disconnecting	Incorrect PIN. Disconnecting.	Incorrect PIN code. Disconnecting ...	Single participant	a participant tries to join a PIN-protected meeting after entering the wrong PIN three times in a row
Wrong PIN, enter a valid one.	Incorrect PIN. Enter the correct PIN followed by the pound sign.	Incorrect PIN code. Enter PIN code.	Single participant	a participant tries to join a PIN-protected meeting after entering the wrong PIN (less than three times in a row)
First participant in meeting	Thank you for attending the meeting. You are the first participant. Please hold.		Single participant	the first participant joins the meeting (after the Connected Indication and the Enter meeting PIN messages)
First participant and moderator	Thank you for attending the meeting. You are the first participant. You have moderation privileges.		Single participant	the first participant joined the meeting using the moderator PIN instead of the meeting PIN
New participant joined	Tone		All participants	a new participant has joined the meeting
Participant left	Tone		All participants	a participant has left the meeting



CHAPTER 7

Managing Cisco Unified Videoconferencing 5200 Series MCU Events

- [Available Cisco Unified Videoconferencing 5200 Series MCU Events, page 7-1](#)
- [Viewing the Events Log, page 7-6](#)
- [Viewing the Alarms Log, page 7-6](#)
- [Viewing Security Events, page 7-6](#)
- [Setting Event Security Levels, page 7-6](#)
- [Sending a Trap on a Specified Event, page 7-7](#)
- [Viewing Event Descriptions, page 7-7](#)
- [Viewing Alarm History, page 7-8](#)
- [Using the Event Display Filter, page 7-8](#)

Available Cisco Unified Videoconferencing 5200 Series MCU Events

[Table 7-1](#) lists trap event indications by category.

[Table 7-2](#) lists trap event indications by ID number.

Table 7-1 *Cisco Unified Videoconferencing 5200 Series MCU Events by Category*

Category	ID	Type	Trap is sent when...
Info	1	Power up	The Cisco Unified Videoconferencing 5200 Series MCU has begun operation.
Info	2	Power down	The Cisco Unified Videoconferencing 5200 Series MCU is shutting down.
Info	3	Link down	Standard SNMP MIB trap indicating that the network connection is down with details about the cause and time of connection loss.
Info	4	Link up	Standard SNMP MIB trap indicating that the network connection has been reestablished.

Category	ID	Type	Trap is sent when...
Info	7	Warm start	The Cisco Unified Videoconferencing 5200 Series MCU has been reset via the Administrator interface.
Info	8	Cold start	The Cisco Unified Videoconferencing 5200 Series MCU has been reset using the button on the front panel.
Info	10	CPU usage	CPU usage reaches the 90 percent threshold set in the Cisco Unified Videoconferencing 5200 Series MCU.
Info	13	Abnormal disconnection	A call disconnects for a reason other than normal, busy, or no answer.
Info	16	General alarm	A system failure is detected.
Info	17	Corrupt web data	Corrupt web files are present in the Cisco Unified Videoconferencing 5200 Series MCU.
Info	18	Incompatible sw burn attempt	An attempt to burn a version of the Cisco Unified Videoconferencing 5200 Series MCU software onto incompatible hardware occurs.
Info	19	MP registration blocked	The media processor registration to the Cisco Unified Videoconferencing 5200 Series MCU failed.
Info	27	TFTP connection failed	The Cisco Unified Videoconferencing 5200 Series MCU fails to connect to a Cisco TFTP server.
Info	33	Low memory	Memory usage reaches the 90 percent threshold set in the Cisco Unified Videoconferencing 5200 Series MCU.
Alarm	5	Gatekeeper registration state change	A change occurs in the registration status of the Cisco Unified Videoconferencing 5200 Series MCU with the gatekeeper.
Alarm	6	Ethernet state change	The network returns after going down. Indicates the time at which the network was restored.
Alarm	9	MP connection	Communication with a registered media processor has broken.
Alarm	11	Network problem	A problem occurs on the network.
Alarm	12	Hot swap	A blade has been removed from the Cisco Unified Videoconferencing 5200 Series chassis under power or inserted into the Cisco Unified Videoconferencing 5200 Series chassis under power.
Alarm	15	Over heating	The configured temperature thresholds for the device are exceeded. Overheating can cause serious damage to the functioning of the device.
Alarm	31	Fan problem	A problem occurs with one of the chassis fans.
Alarm	32	Power supply problem	A problem occurs with one of the power supply units.

Category	ID	Type	Trap is sent when...
Security	14	Service table changed	The service table has been modified.
Security	20	User logged in	A user successfully logs in to the system via the web interface.
Security	21	User logged out	A user logs out of the system via the web interface.
Security	22	Authentication failed	A user tries to log in to the web interface and authentication fails.
Security	23	Configuration changed	A configuration change is uploaded from the web interface.
Security	24	Configuration export	Configuration is exported via the web interface.
Security	25	Configuration import	Configuration is imported via the web interface.
Security	26	User account locked	A user account is disabled.
Security	28	Audio prompts uploaded	A user uploads a new set of audio messages via configuration > Customization > Audio messages > Update messages pack file, or a user modifies an existing message file.
Security	29	Version update	A user selects the Update software option via the  icon.
Security	30	Default configuration restored	A user selects the Restore factory defaults option via the  icon.

Table 7-2 Cisco Unified Videoconferencing 5200 Series MCU Events by ID

Category	ID	Type	Trap is sent when...
Info	1	Power up	The Cisco Unified Videoconferencing 5200 Series MCU has begun operation.
Info	2	Power down	The Cisco Unified Videoconferencing 5200 Series MCU is shutting down.
Info	3	Link down	Standard SNMP MIB trap indicating that the network connection is down with details about the cause and time of connection loss.
Info	4	Link up	Standard SNMP MIB trap indicating that the network connection has been reestablished.
Alarm	5	Gatekeeper registration state change	A change occurs in the registration status of the Cisco Unified Videoconferencing 5200 Series MCU with the gatekeeper.
Alarm	6	Ethernet state change	The network returns after going down. Indicates the time at which the network was restored.
Info	7	Warm start	The Cisco Unified Videoconferencing 5200 Series MCU has been reset via the Administrator interface.
Info	8	Cold start	The Cisco Unified Videoconferencing 5200 Series MCU has been reset using the button on the front panel.
Alarm	9	MP connection	Communication with a registered media processor has broken.
Info	10	Cpu usage	CPU usage reaches the 90 percent threshold set in the Cisco Unified Videoconferencing 5200 Series MCU.
Alarm	11	Network problem	A problem occurs on the network.
Alarm	12	Hot swap	A blade has been removed from the Cisco Unified Videoconferencing 5200 Series chassis under power or inserted into the Cisco Unified Videoconferencing 5200 Series chassis under power.
Info	13	Abnormal disconnection	A call disconnects for a reason other than normal, busy, or no answer.
Security	14	Service table changed	The service table has been modified.
Alarm	15	Over heating	The configured temperature thresholds for the device are exceeded. Overheating can cause serious damage to the functioning of the device.
Info	16	General alarm	A system failure is detected.
Info	17	Corrupt web data	Corrupt web files are present in the Cisco Unified Videoconferencing 5200 Series MCU.
Info	18	Incompatible sw burn attempt	An attempt to burn a version of the Cisco Unified Videoconferencing 5200 Series MCU software onto incompatible hardware occurs.

Category	ID	Type	Trap is sent when...
Info	19	MP registration blocked	The media processor registration to the Cisco Unified Videoconferencing 5200 Series MCU failed.
Security	20	User logged in	A user successfully logs in to the system via the web interface.
Security	21	User logged out	A user logs out of the system via the web interface.
Security	22	Authentication failed	A user tries to log in to the web interface and authentication fails.
Security	23	Configuration changed	A configuration change is uploaded from the web interface.
Security	24	Configuration export	Configuration is exported via the web interface.
Security	25	Configuration import	Configuration is imported via the web interface.
Security	26	User account locked	A user account is disabled.
Info	27	TFTP connection failed	The Cisco Unified Videoconferencing 5200 Series MCU fails to connect to a Cisco TFTP server.
Security	28	Audio prompts uploaded	A user uploads a new set of audio messages via configuration > Customization > Audio messages > Update messages pack file, or a user modifies an existing message file.
Security	29	Version update	A user selects the Update software option via the  icon.
Security	30	Default configuration restored	A user selects the Restore factory defaults option via the  icon.
Alarm	31	Fan problem	A problem occurs with one of the chassis fans.
Alarm	32	Power supply problem	A problem occurs with one of the power supply units.
Info	33	Low memory	Memory usage reaches the 90 percent threshold set in the Cisco Unified Videoconferencing 5200 Series MCU.

Viewing the Events Log

The Cisco Unified Videoconferencing 5200 Series MCU displays up to 100 events.

Procedure

- Step 1

Select **Events**.
- Step 2

Select **All**.

Viewing the Alarms Log

Procedure

- Step 1

Select **Events**.
- Step 2

Select **Alarms**.

Viewing Security Events

Procedure

- Step 1

Select **Events**.
- Step 2

Select **Security**.

Setting Event Security Levels

Procedure

- Step 1

Select **Events**.
- Step 2

Select **All**, **Alarms** or **Security**and select the link in the Type column for the event that you want to configure,

or

Select **All** and select the  icon.
- Step 3

Select the arrow in the Review column for the event that you want to modify.

- Step 4** Select an option from the list in the Severity column.
- Cleared—One or more previously reported alarms have been cleared.
 - Info—Notification of a non-erroneous event.
 - Critical—A service-affecting event has occurred and requires immediate corrective action.
 - Major—A service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.
 - Minor—A non-service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.
 - Warning—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.
- Step 5** Select **Apply**.
- Step 6** Select **Close**.
-

Sending a Trap on a Specified Event

Procedure

-
- Step 1** Select **Events**.
- Step 2** Select **All**, **Alarms** or **Security**.
- Step 3** Select the link in the Type column for the event that you want to configure or select the  icon.
- Step 4** Select the arrow in the Review column for the event that you want to modify.
- Step 5** Select the box in the Trapped column.
- Step 6** Select **Apply**.
- Step 7** Select **Close**.
-

Viewing Event Descriptions

Procedure

-
- Step 1** Select **Events**.
- Step 2** Select **All**, **Alarms** or **Security**.
- Step 3** Select the icon in the Info column for the event description that you want.
-

Viewing Alarm History

Procedure

Step 1 Select **Events**.

Step 2 Select **Alarms**.

Step 3 Select the **Show history** box.

When Show history is selected, the Alarms tab displays all alarm events.

When Show history is deselected, the Alarms tab displays only alarm events that are still current.

Using the Event Display Filter

Procedure

Step 1 Select **Events**.

Step 2 Select **All**.

Step 3 Select **Filter settings**.

Step 4 Select the information that you want to display on the events log.

Step 5 Select **Apply**.



CHAPTER 8

Managing Cisco Unified Videoconferencing 5200 Series MCU User Profiles

- [Cisco Unified Videoconferencing 5200 Series MCU User Types, page 8-1](#)
- [Viewing User Profiles, page 8-2](#)
- [Adding a User Profile, page 8-2](#)
- [Modifying a User Profile, page 8-3](#)
- [Enabling a User Profile, page 8-3](#)
- [Removing a User Profile, page 8-3](#)

Cisco Unified Videoconferencing 5200 Series MCU User Types

Users must have authorization to access the Cisco Unified Videoconferencing 5200 Series MCU. Users are either Administrators or Operators. [Table 8-1](#) describes each access level.

Table 8-1 *Cisco Unified Videoconferencing 5200 Series MCU Access Levels*

Access Level	Privileges
Administrator	• Full access to the Cisco Unified Videoconferencing 5200 Series MCU Administrator interface. • Full Operator-level access to the Conference Control interface. • Telnet access to the Cisco Unified Videoconferencing 5200 Series MCU. • You can assign Administrator authorization to up to ten users.
Operator	• Access to the Conference Control interface using the Create Conference window. • Access to view details of all conferences hosted on the Cisco Unified Videoconferencing 5200 Series MCU and to cascaded conferences hosted on participating Cisco Unified Videoconferencing 5200 Series MCU. • Ability to create a new conference from the Conference Control access window, the Create Conference window, or the Conference Control interface. • Moderator-level access to all conferences while moderator controls are simultaneously held by other users. • Ability to invite other participants to a conference. • You can assign Operator authorization to up to 50 users.

Viewing User Profiles

Procedure

-
- Step 1** Select **Users**.
- Step 2** Select the arrow in the Review column for the user profile you want to view.
-

Adding a User Profile

Procedure

-
- Step 1** Select **Users**.
- Step 2** Select **Add new user**.
- Step 3** Select an authority level for the new user—Administrator or Operator.
- Step 4** Enter a password and confirm it.
- Step 5** Select **Apply**.
-

Modifying a User Profile

Procedure

-
- Step 1** Select **Users**.
 - Step 2** Select the arrow in the Review column for the user profile you want to modify.
 - Step 3** Modify the required settings.
 - Step 4** Select **Apply**.
-

Enabling a User Profile

You must enable a user profile before that user can access the Cisco Unified Videoconferencing 5200 Series MCU web user interface.

Procedure

-
- Step 1** Select **Users**.
 - Step 2** Select the Active box for the user profile you want to enable.
 - Step 3** Select **Apply**.
-

Removing a User Profile

Procedure

-
- Step 1** Select **Users**.
 - Step 2** Select the arrow in the Review column for the user profile you want to remove.
 - Step 3** Select **Delete**.
 - Step 4** Select **Yes** in the message that appears.
- The user profile is removed from the authorized users list.
-



CHAPTER 9

Configuring Advanced Maintenance Settings for the Cisco Unified Videoconferencing 5200 Series MCU

- [Backing Up Your Cisco Unified Videoconferencing 5200 Series MCU Configuration, page 9-1](#)
- [Restoring Your Cisco Unified Videoconferencing 5200 Series MCU Configuration, page 9-2](#)
- [Restoring Factory Default Settings, page 9-2](#)
- [How to Work with Advanced Commands for the Cisco Unified Videoconferencing 5200 Series MCU, page 9-3](#)
- [How to Manage Cisco Unified Videoconferencing 5200 Series MCU Software, page 9-7](#)
- [Restarting the Cisco Unified Videoconferencing 5200 Series MCU, page 9-8](#)
- [Contacting Customer Support, page 9-8](#)
- [Viewing Active Conferences, page 9-9](#)
- [Creating a New Conference, page 9-9](#)

Backing Up Your Cisco Unified Videoconferencing 5200 Series MCU Configuration

You can save Cisco Unified Videoconferencing 5200 Series 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 Cisco Unified Videoconferencing 5200 Series MCU or to configure a similar Cisco Unified Videoconferencing 5200 Series MCU.

The exported file is a .zip file that includes a .val file and a .xml file.

Procedure

-
- Step 1** Select the  icon.
- Step 2** Select **Backup configuration**.
- Step 3** Save the configuration settings file to your chosen location.
The .zip extension is automatically appended to the file name.
-

Restoring Your Cisco Unified Videoconferencing 5200 Series MCU Configuration

You can import the settings of a saved Cisco Unified Videoconferencing 5200 Series MCU configuration file from a storage device on your network. You can use the saved configuration file to restore the settings to the current Cisco Unified Videoconferencing 5200 Series MCU or to configure another Cisco Unified Videoconferencing 5200 Series MCU.

The imported file is a .zip file that includes a .val file and a .xml file.

Procedure

-
- Step 1** Select the  icon.
- Step 2** Select **Restore configuration**.
- Step 3** Select **Browse**.
- Step 4** Navigate to and select the configuration file (.zip) you want to import.
- Step 5** Select **Restore**.
- Step 6** Select **Continue** to upload the new configuration settings.
The restore procedure causes all current configuration to be permanently lost.
The system shuts down for a few minutes and then restarts automatically.
All active conferences are disconnected.
- Step 7** Select **OK** to complete the restore procedure.
-

Restoring Factory Default Settings

Procedure

-
- Step 1** Select the  icon.
- Step 2** Select **Restore factory defaults**.

- Step 3

Select **Continue** to upload the new configuration settings, or select **Cancel** to abort the restore procedure.

The restore procedure causes all current configuration to be permanently lost.

The system shuts down for a few minutes and then restarts automatically.

All active conferences are disconnected.
- Step 4

Select **OK** to complete the restore procedure.

How to Work with Advanced Commands for the Cisco Unified Videoconferencing 5200 Series MCU

You can send text-based commands used for the enhanced control of the Cisco Unified Videoconferencing 5200 Series MCU.



Note

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

- [Viewing Available Advanced Commands, page 9-3](#)
- [Modifying Advanced Commands, page 9-6](#)
- [Sending Advanced Commands, page 9-7](#)

Viewing Available Advanced Commands

Table 9-1 lists all available advanced commands.

Procedure

- Step 1

Select the  icon.
- Step 2

Select **Advanced** parameters.

Table 9-1		List of Available Advanced Commands		
Command	String	Description	Parameters	Default
H323 RAS port number	h323rasport	Sets the H.323 RAS port number.		1719
H323 SIG port number	h323sigport	Sets the H.323 Signaling port number.		1720
Registration mode	h323gkregmode			
SIP support video fast update	sipsupportvfu		disable	Enabled
			enable	

Command	String	Description	Parameters	Default
Minimal new speaker interval	minnewspeakerinterval	Sets the minimum length of time (in milliseconds) an attendee must wait before becoming the active speaker.		3000
Enable DTMF conference control	dtmfconferencecontrol		disable enable	Enabled
Register conference ID	mcuregisterconference ID	Registers conference ID (on the Gatekeeper or SIP server).	disable enable	Enabled
Participants join conference policy	mcujoinpolicy		All Invite Only	All
External conference policy authorization	externalconferenceauthorization		None Notify Authorize	None
Unit location	boardlocation	Indicates where the unit is physically located.	String	None
SNMP read password	snmpreadpassword	SNMP read community	String	RVGET2
SNMP write password	snmpwritepassword	SNMP write community	String	RVSET2
H.323 status show	h323statusshow	Prints a snapshot of H.323 stack-related information.		
H.323 stack show	h323stackshow	Enables H.323 stack prints.		H.323 stack printing is disabled by default.
H.323 stack hide	h323stackhide	Disables H.323 stack prints.		
SIP status show	sipstatusshow	Prints a snapshot of SIP stack-related information.		
SIP stack show	sipstackshow	Enables SIP stack prints.		SIP stack printing is disabled by default.
SIP stack hide	sipstackhide	Disables SIP stack prints.		
H.239 Live Mode	h239livemode		disable enable	Enabled
H.239 Duo Video	h239duovideo		disable enable	Disabled

Command	String	Description	Parameters	Default
Unit Notify Level	notifylevel	Sets the Cisco Unified Videoconferencing 5200 Series MCU log notify level filter	Fatal—Cisco Unified Videoconferencing 5200 Series 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 Cisco Unified Videoconferencing 5200 Series 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
Waiting Room Indication Timeout	setwaitingroomin dtimeout	Indicates the length of time (in milliseconds) between waiting room announcements.		
Display Cascaded Endpoint Name	cascadedisplayen dpointname	When enabled, the text overlay on the subframe from the slave conference is the endpoint name.	disable enable	Enabled

Command	String	Description	Parameters	Default
Handle DTMF After Notification	handledtmfafternotification	Instructs the Cisco Unified Videoconferencing 5200 Series MCU to send DTMF signals to an external server and other specified destinations.	no—Cisco Unified Videoconferencing 5200 Series MCU sends DTMF signals to the external server only. yes—Cisco Unified Videoconferencing 5200 Series MCU sends DTMF signals to the external server and to the destination set by the DTMF forwarding advanced command.	
DTMF Forwarding Target	dtmfforwardto	Indicates the target of DTMF forwarding.	to all—All endpoints in the conference. to gateways—To gateways only. to none—DTMF is disabled.	None
DTMF Detection Before Authentication	dtmfalwaysopen		disable enable	Enabled
CS Logging	cslog	Display Customer Support-relevant logs.	start stop status	

Modifying Advanced Commands

Procedure

- Step 1** Select the  icon.
- Step 2** Select **Advanced parameters**.
- Step 3** Select the arrow in the Review column for the advanced command that you want to modify.
- Step 4** Modify the value for the parameter in the **Value** field.
- Step 5** Select **Apply**.

Sending Advanced Commands

Procedure

-
- | | |
|---------------|--|
| Step 1 | Select the  icon. |
| Step 2 | Select Advanced parameters . |
| Step 3 | Locate the CLI section and select More . |
| Step 4 | Enter a command in the Command field. |
| Step 5 | Enter a parameter value for the command (where applicable) in the Parameter field. |
| Step 6 | Enter a value for the parameter (where applicable) in the Value field. |
| Step 7 | Select Execute . |
-

How to Manage Cisco Unified Videoconferencing 5200 Series MCU Software

- [Upgrading Cisco Unified Videoconferencing 5200 Series MCU Software, page 9-7](#)
- [Restoring a Previous Software Version, page 9-8](#)

Upgrading Cisco Unified Videoconferencing 5200 Series MCU Software

Procedure

-
- | | |
|---------------|--|
| Step 1 | Select the  icon. |
| Step 2 | Select Update software . |
| Step 3 | Select Browse and navigate to required Cisco Unified Videoconferencing 5200 Series MCU upgrade package. |
| Step 4 | Select Update .

The system shuts down for a few minutes and then restarts automatically.

All active conferences are disconnected. |
| Step 5 | Select Continue . |
| Step 6 | As soon as the update process has finished, the Cisco Unified Videoconferencing 5200 Series MCU reboots and reloads with the new software version. |
-

Restoring a Previous Software Version

Procedure

Step 1 (Recommended) Save the current MCU custom configuration by performing these steps:

a. In the web MCU web user interface, select the maintenance icon .

b. Select Backup configuration and save the generated .zip file.

Step 2 In the web MCU web user interface, select the maintenance icon .

Step 3 Select **Rollback software**.

Step 4 After reset, the previous release is installed on the MCU.

The downgrade process returns the the MCU configuration back to the previous version—with the values used prior to the last upgrade.



Note

Do not import the saved configuration to the MCU, after the downgrade. An older version of the MCU configuration might not support the new configuration values.

Restarting the Cisco Unified Videoconferencing 5200 Series MCU

Procedure

Step 1 Select the  icon.

Step 2 Select **Restart unit**.

The system shuts down for a few minutes and then restarts automatically.

All conferences are disconnected.

Step 3 Select **Continue**.

Contacting Customer Support

Procedure

Step 1 Select the  icon.

Step 2 Select **Contact Customer Support**.

The Contacting Customer Support window displays the Customer Support contact details.

Step 3 (Optional) Select **Create** to create a snapshot file of bundled logs and configuration files which you can send to Cisco Customer Support for debugging purposes.

The snapshot file contains the last 24 hours of Cisco Unified Videoconferencing 5200 Series MCU activity and is approximately 10 MB in size, depending on the amount of traffic. The snapshot file contains the following information about the Cisco Unified Videoconferencing 5200 Series MCU system:

- Inventory file
 - Configuration files
 - Log files for the previous 24 hours
 - All initialization log files
 - All exception log files
 - Events and alarms logs
-

Viewing Active Conferences

Procedure

Step 1 Select **Manage Conferences**.

Step 2 Select the link in the Conference ID column for the conference you want to view.

Creating a New Conference

Procedure

Step 1 Select **Manage Conferences**.

Step 2 Select the  icon.

Step 3 Follow the procedure described in the [“Create a New Meeting” section in the User Guide for Cisco Unified Videoconferencing 5000 Series MCU](#).
