Configuration Guide for Cisco Unified Videoconferencing 5000 MCU Release 7.0

August 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-19862-01

Configuration Guide for Cisco Unified Videoconferencing 5000 MCU Release 7.0

CONTENTS

CHAPTER 1

Accessing the MCU Interface

Procedure

Step 1 Launch your browser and enter the IP address or the name of the MCU followed.

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 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 MCU settings.

CHAPTER 2

Viewing Cisco Unified Videoconferencing 5000 MCU Status Information

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 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 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 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 MCU is registered to a gatekeeper.

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

Viewing SIP Sever 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 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 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 MCU Resource Usage

Procedure

Step 1 Select **Status**.

Step 2 Locate the Status Map section.

The CPU box indicates the percentage of 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 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 5000 MCU Environment

Setting the User Interface Language

You can configure the language that the MCU supports. Table 3-1 lists the languages that the 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 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 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" section on page 6-1.

Setting the Cisco Unified Videoconferencing 5000 MCU Identifier

You can set the MCU identifier. This identifies the MCU in the following situations:

- During gatekeeper/SIP registration.
- When inviting endpoints into a conference.
- In the text overlay for the cascaded 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 **MCU 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 5000 MCU

Procedure

Step 1 Select **Configuration**.

Step 2 Click **Setup**.

Step 3 Locate the Basics section.

Step 4 (Optional) Select **Set manually** in the Date and time section.

Step 5 Click **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 Click **Apply**.

Changing Address Settings

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

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 MCU in the **Primary IP address** and **Secondary IP address** fields.
- **b.** Enter the IP address of the router you want either MCU to use in the **Router IP** field.
- **c.** Enter the subnet mask you want either 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 MCU in the **DNS suffix** field.

b. Enter the IP address of the primary DNS server that you want the MCU to use in the **DNS server1** field.

c. Enter the IP address of the back-up DNS server that you want the MCU to use in the **DNS server2** field.

Step 6 Select Ethernet port and duplex speed value you want to set in the **Port settings** field.

Note We recommend that you set the Port settings option to "Auto".

Step 7 Select **Apply**.

Configuring Security for the Cisco Unified Videoconferencing 5000 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 Select **Configuration**.

Step 2 Select **Setup**.

Step 3 Locate the Security section.

Step 4 Select the access level you want the MCU to support from the **Security mode** field.

- 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 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 a web server certificate with the wizard, select **Import** to import an existing certificate, or select **Export** to save an existing certificate to a file.

Step 5 Select **Enable HTTPS**.

Step 6 Select **Apply**.

How to Manage SNMP Trap Servers

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 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 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 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 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 Select **Enable QoS support**.

Step 5 Set the required DiffServ Code Point value for each media type by selecting one of these options:

- Auto attendant service—The system assigns the default DiffServ Code Point value for each media type. The default settings represent Cisco recommendations.
- Custom—The system assigns your own DiffServ Code Point value for each media type.

Step 6 (Optional, if you selected Custom) Do the following:

- Enter a whole number from 0 to 63 in the Voice priority field of the Video calls section to set the DiffServ Code Point value of voice packets that the MCU sends out. The default value is 34.
- Enter a whole number from 0 to 63 in the Video priority field of the Video calls section to set the DiffServ Code Point value of video packets that the MCU sends out. The default value is 34.
- Enter a whole number from 0 to 63 in the Voice priority field of the Audio calls section to set the DiffServ Code Point value of voice packets that the MCU sends out. The default value is 46.

Step 7 Select **Apply**.

CHAPTER 4

Configuring Protocols for the Cisco Unified Videoconferencing 5000 MCU

Configuring H.323 Gatekeeper Protocol Settings

You can configure the protocol settings of an H.323 gatekeeper to set how the MCU and the gatekeeper interact.

Note

- Changing gatekeeper settings does not reset the MCU, but might disconnect active calls.
- You do need to reset the 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 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 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 MCU communication with the SIP proxy.

Step 5 Enter the SIP domain of the 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 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.
- 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 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 MCU communicates with the SIP proxy.

The default is 5060.

Step 11 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 12 Enter the MCU user name and password.

The user name and password must match the name and password defined on the SIP proxy server.

Step 13 Select **Use registrar digest authentication** to enable 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.

Step 14 Select **Use 'Empty Invite' when sending Invite messages to endpoints** to enable the remote endpoint to indicate preferred audio and video channels.

Step 15 Select **Using Microsoft OCS** to enable the MCU to work with Microsoft Office Communications Server (OCS).

Step 16 Select **Apply**.

CHAPTER 5

Configuring Conference Management Settings for the Cisco Unified Videoconferencing 5000 MCU

Dialing Directly to the Cisco Unified Videoconferencing 5000 MCU

You can allow users to dial directly to the MCU IP address using 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 using the MCU IVR.

If the 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 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 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 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 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 5000 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 using the Change link.

Step 6 Select **Apply**.

How to Manage Services on the Cisco Unified Videoconferencing 5000 MCU

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 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.722.1 and G.723 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 (Optional) Enter the string $ID to display the conference ID in the welcome screen.

Step 11 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

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:

a. Select **Dynamically adjusted**.

b. Select the maximum number of participants to which the conference layout expands from the **Max displayed streams** field.

c. Select **OK**.

Step 7 Perform these steps to define a fixed layout for the conference:

a. Select **Static** to define a fixed layout for the conference.

b. Select **Select**.

c. Select the required layout and select **OK**.

d. 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 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 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 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 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 MCU to automatically call disconnected terminals to attempt a reconnection.

The 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 5000 MCU

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

You can save all audio messages currently in use on the 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 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 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 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 MCU Messages

Table 6-1 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)
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

Message Name	Recorded Message	Displayed Message	Played for …	Played when …
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
Success indication	Tone		Single participant	a DTMF command has succeeded
Enter party number	To dial out, please dial the number of the party you wish to invite to the meeting, followed by the pound sign.		Single participant	you are in invite mode (after dialing *8 using DTMF) and you do not dial any number for a period of time
Error indication	Tone		Single participant	a DTMF command has failed
Moderator privileges required	This action requires moderator privileges.		Single participant	you perform a DTMF command that requires moderator privileges without first becoming a moderator
Another moderator exists	Another participant is already moderating the meeting.		Single participant	you try to become the moderator using DTMF, but there is already another moderator for the meeting

Message Name	Recorded Message	Displayed Message	Played for …	Played when …
Meeting control menu	To return to the meeting – press pound. To become the moderator – press 1. To mute or unmute your line – press 2. To control the volume of your line – press 3. To show or hide participants' names - press 4.		Single participant	you are in DTMF command mode (after dialing * or ** using DTMF) and you do not enter any command for a period of time
Meeting control menu (personal layout disabled)	To return to the meeting - press pound. To become the moderator - 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 ** using DTMF) and you do not enter any command for a period of time
Enter moderator PIN	Enter the moderator PIN followed by the pound sign.		Single participant	you try to become the moderator using DTMF and a moderator PIN is defined
Moderator menu	To return to the meeting - press pound. To stop moderating - press 1. To mute or unmute your line - press 2. To control the volume of your line - press 3. To show or hide participants' names - press 4. To terminate the meeting - press 5. To change the main video layout - press 6. To block admission to the meeting - press 7. To dial out - press 8. To mute/unmute all lines except yourself - press 9.		Single participant	you are in DTMF moderator mode (i.e. after becoming the moderator using DTMF) and you do not enter any command for a period of time
Moderator menu (blocked meeting)	To return to the meeting - press pound. To stop moderating - press 1. To mute or unmute your line - press 2. To control the volume of your line - press 3. To show or hide participants' names - press 4. To terminate the meeting - press 5. To change the main video layout - press 6. To allow admission to the meeting - press 7. To dial out - press 8. To mute/unmute all lines except yourself - press 9.		Single participant	you are in DTMF moderator mode (i.e. after becoming the moderator using DTMF) in a meeting whose admission is blocked and you do not enter any command for a period of time
Join sub-conference	You have joined a sub-conference.		Single participant	a participant joins a sub-conference

Message Name	Recorded Message	Displayed Message	Played for …	Played when …
Leave sub-conference	You have left the sub-conference.		Single participant	a participant leaves a sub-conference
Join not allowed	For security reasons, please join from the MeetingPlace web conferencing interface. Goodbye.			Reserved for Cisco Unified MeetingPlace
No video resources	All video resources are currently in use. Please try again later.			Reserved for Cisco Unified MeetingPlace
Meeting terminating	The meeting is about to terminate.		All participants	a meeting is about to terminate
Organizer not yet joined	Please wait for the meeting moderator.		Single participant	you join a meeting in a waiting room mode before the moderator has joined
Organizer joined, meeting starts	The meeting will now begin.		All participants	the moderator joins a meeting in waiting room mode
Organizer left, meeting paused	You have been moved to the waiting room, please wait.		All participants	the moderator leaves a meeting in waiting room mode
Organizer back, meeting resumed	The meeting will now resume.		All participants	the moderator returns to a meeting in waiting room mode
Wrong moderator PIN	You have entered an incorrect moderator PIN.		Single participant	you have entered the wrong moderator PIN
You are the moderator	You are now the moderator.		Single participant	you have become the moderator of the meeting using DTMF
Muted	Muted		Single participant	you mute yourself using DTMF
Unmuted	Unmuted		Single participant	you unmute yourself using DTMF
Volume control menu	To decrease the volume, press zero. To increase, press one.		Single participant	you are in volume control mode (after dialing *3 using DTMF) and you do not enter any command for a period of time

Message Name	Recorded Message	Displayed Message	Played for …	Played when …
Meeting admission blocked	Admission to the meeting is now blocked.		Single participant	you block admission to the meeting using DTMF
Meeting admission allowed	Admission to the meeting is now allowed.		Single participant	you allow admission to the meeting using DTMF
Dialing	Dialing.		Single participant	you invite a participant using DTMF
Invalid input	Invalid input.		Single participant	you press an invalid key during a DTMF command
Stopped moderating	You are no longer the meeting moderator.		Single participant	you have stopped moderating the meeting using DTMF
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 using DTMF) and you do not enter any command for a period of time
Mute/Unmute All menu	To mute all participants except yourself, press zero. To un-mute all participants, press 1.		Single participant	you are in mute/unmute all mode (after dialing *9 using DTMF) and you do not enter any command for a period of time
All muted	All participants are now muted.		Single participant	you mute all participants using DTMF
All unmuted	All participants are now unmuted.		Single participant	you unmute all participants using DTMF
Silent				
Meeting selection	Thank you for calling. To create a new meeting or join by ID, press nine. To select a meeting from the list, press the entry number.		Single participant	you dial the MCU Auto Attendant (with video)
Enter meeting ID	Enter the meeting ID followed by the pound sign.	Enter meeting ID	Single participant	you choose to create or join a meeting by ID during an Auto Attendant session, or when you dial the MCU Auto Attendant with audio only

Message Name	Recorded Message	Displayed Message	Played for …	Played when …
Invalid meeting ID	You have entered an incorrect meeting ID.	The meeting ID is invalid.	Single participant	you enter an invalid meeting ID during an Auto Attendant session
Create meeting PIN	To create a PIN code to protect this meeting, enter a PIN code followed by the pound sign. Enter only the pound sign if you do not want PIN protection.	Creating a new meeting Enter PIN code (optional)	Single participant	you choose to create a new meeting during an Auto Attendant session
Create meeting failed	Failed to create a meeting.	Failed to create a meeting –[reason]. To join an existing meeting enter meeting ID Reason is one of: • No resources • Not allowed • Other When the reason is "other", no reason is displayed.	Single participant	during Auto Attendant session, when meeting creation fails. Possible reasons: **No resources**—MCU is out of resources **Not allowed**—MCU is configured to disallow meeting creation by dial-in.
Create meeting – invalid PIN code	You have entered an invalid PIN. Enter a valid PIN using digits only followed by the pound sign.	The PIN code is invalid. Enter valid PIN code.	Single participant	during Auto Attendant session, when creating a new meeting and entering an invalid meeting PIN code (PIN code should be digits only)
Failed to connect to the meeting	Failed to connect to the meeting. Disconnecting.	Failed to connect to the meeting –[reason]. Reason is one of: • No endpoint support • Other When the reason is "other", no reason is displayed.	Single participant	during Auto Attendant session, after user has selected a meeting, when the transfer to the selected meeting fails
Invalid meeting ID - try again	You have entered an incorrect meeting ID. Please enter your meeting ID followed by the pound sign.		Single participant	during Auto Attendant session, after user has entered an invalid meeting ID

Message Name	Recorded Message	Displayed Message	Played for …	Played when …
Create meeting failed - reenter meeting	Failed to create a meeting. To join an existing meeting, enter your meeting ID followed by the pound sign.		Single participant	during Auto Attendant session, after meeting creation has failed (audio only caller)
Meeting ends in 10 min	The meeting is about to end in less than ten minutes.			
Meeting ends in 5 min	The meeting is about to end in less than five minutes.			
Meeting ends in 2 min	The meeting is about to end in less than two minutes.			
Meeting end in 1 min	The meeting is about to end in less than one minute.			
Disconnecting	Disconnecting			
No Input from user	I did not hear your entry.			
No video resources, connected as audio only	You are connected with audio only due to resource limitations. Please contact your system administrator if needed.			there are no video resources and the participant connected using audio only
Termination due to failure	The meeting is about to terminate due to a temporary failure. Please redial the meeting ID and report the incident to your system administrator.			
Meeting extended automatically	The meeting has been automatically extended.			
Meeting extended by moderator	The meeting has been extended by the moderator.			
Please hold	Thank you, please hold.			

CHAPTER 7

Managing Cisco Unified Videoconferencing 5000 MCU Events

Available SNMP Events

Table 7-1 lists trap event indications by category.

Table 7-2 lists trap event indications by ID number.

Table 7-1 MCU Trap Events by Category

Category	ID	Type	Trap is sent when...
Info	1	Power up	The MCU has begun operation.
Info	2	Power down	The 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 MCU has been reset using the Administrator interface.
Info	8	Cold start	The 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 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 MCU.
Info	18	Incompatible sw burn attempt	An attempt to burn a version of the MCU software onto incompatible hardware occurs.
Info	19	MP registration blocked	The media processor registration to the MCU failed.
Info	27	TFTP connection failed	The MCU fails to connect to a Cisco TFTP server.
Info	33	Low memory	Memory usage reaches the 90 percent threshold set in the MCU.
Alarm	5	Gatekeeper registration state change	A change occurs in the registration status of the 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 5230 chassis under power or inserted into the Cisco Unified Videoconferencing 5230 chassis under power.

Category	ID	Type	Trap is sent when...
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.
Security	14	Service table changed	The service table has been modified.
Security	20	User logged in	A user successfully logs in to the system using the web interface.
Security	21	User logged out	A user logs out of the system using 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 using the web interface.
Security	25	Configuration import	Configuration is imported using 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 using 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 using the  icon.
Security	30	Default configuration restored	A user selects the Restore factory defaults option using the  icon.

Table 7-2 MCU Trap Events by ID

Category	ID	Type	Trap is sent when...
Info	1	Power up	The MCU has begun operation.
Info	2	Power down	The 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 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 MCU has been reset using the Administrator interface.
Info	8	Cold start	The 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 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 5230 chassis under power or inserted into the Cisco Unified Videoconferencing 5230 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.

Category	ID	Type	Trap is sent when...
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 MCU.
Info	18	Incompatible sw burn attempt	An attempt to burn a version of the MCU software onto incompatible hardware occurs.
Info	19	MP registration blocked	The media processor registration to the MCU failed.
Security	20	User logged in	A user successfully logs in to the system using the web interface.
Security	21	User logged out	A user logs out of the system using 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 using the web interface.
Security	25	Configuration import	Configuration is imported using the web interface.
Security	26	User account locked	A user account is disabled.
Info	27	TFTP connection failed	The MCU fails to connect to a Cisco TFTP server.
Security	28	Audio prompts uploaded	A user uploads a new set of audio messages using 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 using the  icon.
Security	30	Default configuration restored	A user selects the Restore factory defaults option using the  icon.

Category	ID	Type	Trap is sent when...
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 MCU.

Viewing the Events Log

The 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 5000 MCU User Profiles

Cisco Unified Videoconferencing 5000 MCU User Types

Users must have authorization to access the MCU.

Users are either Administrators or Operators. Table 8-1 describes each access level.

Table 8-1 MCU Access Levels

Access Level	Privileges
Administrator	• Full access to the MCU Administrator interface. • Full Operator-level access to the Conference Control interface. • Telnet access to the MCU. • You can assign Administrator authorization to up to ten users.

Access Level	Privileges
Operator	• Access to the Conference Control interface using the Create Conference window. • Access to view details of all conferences hosted on the MCU and to cascaded conferences hosted on participating 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 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

Restrictions

You cannot delete an administrator 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 5000 MCU

Backing Up Your Cisco Unified Videoconferencing 5000 MCU Configuration

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.

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 5000 MCU Configuration

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.

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 you want to import.

The file must have an .ini extension.

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 5000 MCU

You can send text-based commands used for the enhanced control of the 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

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 enable	Enabled
Minimal new speaker interval	minnewspeakerinterval	Sets the minimum length of time (in milliseconds) an attendee must wait before becoming the active speaker.		3000

Command	String	Description	Parameters	Default
Enable DTMF conference control	dtmfconferencecontrolenable		disable enable	Enabled
Register conference ID	mcuregisterconfname	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.		

Command	String	Description	Parameters	Default
H.239 Live Mode	h239livemode		disable enable	Enabled
H.239 Duo Video	h239duovideo		disable enable	Disabled
Unit Notify Level	notifylevel	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
Waiting Room Indication Timeout	setwaitingroomindtimeout	Indicates the length of time (in milliseconds) between waiting room announcements.		
Display Cascaded Endpoint Name	cascadedisplayendpointname	When enabled, the text overlay on the subframe from the slave conference is the endpoint name.	disable enable	Enabled
Handle DTMF After Notification	handledtmfafternotification	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.	

Command	String	Description	Parameters	Default
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 5000 MCU Software

Upgrading Cisco Unified Videoconferencing 5000 MCU Software

Procedure

Step 1 Select the  icon.

Step 2 Select **Update software**.

Step 3 Select **Browse** and navigate to required 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 MCU reboots and reloads with the new software version.

Restoring a Previous Software Version

Procedure

Step 1 Select the  icon.

Step 2 Select **Update software**.

Step 3 Select **Roll back**.

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

All active conferences are disconnected.

Step 4 Select **Continue**.

Step 5 As soon as the update process has finished, the MCU reboots and reloads with the new software version.

Restarting the Cisco Unified Videoconferencing 5000 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 MCU activity and is approximately 10 MB in size. The snapshot file contains the following information about the 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

INDEX

R

S

T

U

W